



Digita Facile

Campania



GUIDA AL DIGITALE FACILE

PROGETTO “DIGITA FACILE CAMPANIA” BANDO “DRITTI AL PUNTO”
è un progetto selezionato e sostenuto
dal Fondo per la Repubblica Digitale Impresa Sociale

SOMMARIO

Premessa.....	25
tema a lavoro e sviluppo produttivo.....	29
A chi è rivolto questo capitolo.....	30
Essere cittadini digitali: da dove si comincia	30
Il digitale non è solo un'App.....	30
I vantaggi concreti: tempo, autonomia, inclusione.....	31
La bussola digitale: il quadro DigComp 2.2.....	31
Il Curriculum Vitae: la chiave per il successo professionale.....	32
Obiettivi del modulo.....	32
Cos'è un curriculum vitae	32
Perché il curriculum vitae è così importante.....	32
La differenza tra curriculum vitae e lettera di presentazione	33
Struttura del CV e errori da evitare.....	34
Obiettivi del modulo.....	34
Gli errori più comuni: come riconoscerli e correggerli	36
Il tuo CV, un vestito su misura	39
Obiettivi del modulo.....	39
Cosa sono gli ATS e perché devi conoscerli	39
Fatti notare: la tecnologia al tuo fianco.....	41
Obiettivi del modulo.....	41
Gli strumenti per creare il curriculum vitae.....	41

Le piattaforme per cercare lavoro.....	42
Dal curriculum vitae al colloquio: come prepararsi.....	43
Il colloquio comincia dal curriculum	43
Le domande più frequenti e come rispondervi	44
L'immagine conta: come presentarsi.....	44
La tua identità digitale: reputazione online e privacy	45
Cosa cercano i selezionatori online	45
Come controllare e migliorare la propria presenza online	45
La privacy dei dati nel processo di candidatura.....	46
Riepilogo e punti chiave.....	46
Autovalutazione delle competenze DigComp.....	47
Glossario essenziale	48
tema a lavoro e sviluppo produttivo.....	50
A chi è rivolto questo capitolo.....	51
Il digitale come strumento di cittadinanza attiva.....	51
Esercitare i propri diritti nell'era digitale	51
Perché questo percorso è importante per te.....	52
La trasformazione digitale del lavoro.....	53
Obiettivi del modulo.....	53
Dal valore fisico al valore intangibile: la Workforce Transformation	53
L'impatto sui settori tradizionali: trasformazione, non sostituzione	53
Il Digital Skill Gap: il divario che frena.....	54

Upskilling e Reskilling: le due strategie di risposta	55
Le Politiche Attive del Lavoro: la risposta istituzionale	55
Le piattaforme istituzionali: orientarsi tra i portali.....	57
Obiettivi del modulo.....	57
Il Ministero del Lavoro e ClicLavoro.....	57
Il SILF Campania: l'interfaccia unica regionale.....	57
La Scheda Anagrafica Professionale: il tuo profilo ufficiale.....	58
Garanzia Giovani: il programma europeo per i NEET	58
Come i servizi per l'impiego ti prendono in carico.....	60
Obiettivi del modulo.....	60
La Dichiarazione di Immediata Disponibilità: il primo passo ufficiale.....	60
La profilazione quantitativa: come il sistema ti valuta	61
Le classi di occupabilità: cosa significano.....	61
Il Patto di Servizio Personalizzato: un accordo su misura	62
Lifelong Learning: imparare per tutta la vita	63
Obiettivi del modulo.....	63
Il Lifelong Learning: imparare non finisce mai	63
Identificare il proprio Skill Gap	63
Le fonti digitali per la formazione: come scegliere	64
Le principali tipologie di risorse formative	65
Il Centro per l'Impiego: cosa può fare per te	66
Un servizio spesso sconosciuto, ma prezioso	66

I servizi offerti dal CPI	66
Come prepararsi al meglio a un appuntamento al CPI	67
Navigare sicuri: attenzione alle truffe nel digitale del lavoro	67
Un rischio reale, da non sottovalutare	67
Le forme più comuni di truffa lavorativa online	67
Come proteggersi.....	68
Riepilogo dei concetti fondamentali	69
Scheda di autovalutazione DigComp.....	70
Glossario essenziale	70
tema a lavoro e sviluppo produttivo.....	73
A chi è rivolto questo capitolo.....	74
Il digitale come chiave per il mercato del lavoro	74
Diventare cittadini digitali autonomi	74
I vantaggi concreti del digitale nella ricerca del lavoro	75
Il mercato del lavoro: tendenze e opportunità del territorio	76
Obiettivi del modulo.....	76
Le tendenze che trasformano il mercato del lavoro	76
Opportunità specifiche nel territorio campano	77
Le competenze più richieste	77
Scrivere per convincere: CV e lettera di presentazione	79
Obiettivi del modulo.....	79
Tecniche per un curriculum vitae che funziona	79

La lettera di presentazione: raccontare il perché	80
Il colloquio e il networking: costruire relazioni che aprono porte	81
Obiettivi del modulo.....	81
Prepararsi al colloquio: più che rispondere a domande.....	81
Il metodo STAR: rispondere con chiarezza e concretezza	81
Il networking: costruire relazioni che creano opportunità	82
Le piattaforme online: dove e come cercare lavoro	83
Obiettivi del modulo.....	83
LinkedIn: molto più di un curriculum online	83
ClicLavoro e i portali istituzionali	83
Costruire un profilo professionale attraente	84
Le soft skills: le competenze che fanno la differenza	85
Obiettivi del modulo.....	85
Cosa sono le soft skills e perché contano.....	85
Le principali soft skills e come svilupparle	85
Come comunicare le soft skills in un colloquio	86
Autovalutazione e piano d'azione per la propria carriera.....	88
Obiettivi del modulo.....	88
L'autovalutazione: il punto di partenza	88
Gli obiettivi SMART: trasformare i sogni in piani	88
Il piano d'azione: dai propositi ai passi concreti	89

Le domande più frequenti: risposte concrete	90
Devo per forza cercare lavoro solo tra le professioni più richieste nella mia zona?	90
Perché non posso inviare lo stesso CV a tutte le aziende per fare prima? ..	90
Cosa rispondo alla domanda “parlami di te” se non ho mai lavorato?	91
Come fisso un obiettivo professionale se non so ancora che lavoro voglio fare?	91
Ho un obiettivo grande ma mi sembra irraggiungibile. Da dove inizio?	91
Gli errori più comuni nella ricerca del lavoro: come evitarli	91
Candidarsi a tutto senza un criterio	92
Trascurare il follow-up	92
Non aggiornare i profili digitali	92
Concentrarsi solo sulle offerte online	92
Smettere di formarsi mentre si cerca lavoro	92
Riepilogo dei concetti fondamentali	93
Scheda di autovalutazione	94
Glossario essenziale	95
tema a lavoro e sviluppo produttivo	97
A chi è rivolto questo capitolo	98
Perché le opportunità del territorio riguardano tutti	98
Essere cittadini digitali autonomi: il punto di partenza	98
Il valore del digitale per chi cerca lavoro o vuole crearlo	99
Analisi del Mercato Locale: Dinamiche Economiche e Occupazionali	100
Obiettivi del modulo	100

Cos'è l'analisi del mercato del lavoro locale	100
Obiettivi e contenuti dell'analisi	100
Gli strumenti di analisi e statistica	101
Come interpretare i dati ISTAT.....	102
Mappatura delle Risorse Locali: Naturali, Umane e Digitali	104
Obiettivi del modulo.....	104
Perché mappare le risorse del territorio	104
Le risorse naturali.....	104
Le risorse umane	105
Gli strumenti GIS per la mappatura del territorio.....	105
Settori Produttivi Emergenti: le Opportunità del Futuro.....	107
Obiettivi del modulo.....	107
Le innovazioni tecnologiche che stanno ridisegnando il lavoro	107
Turismo sostenibile ed esperienziale.....	107
Agricoltura biologica e di precisione	108
Tecnologie ecologiche (Green Tech)	109
Le Opportunità del Tuo Territorio	110
Un modulo personalizzato per ogni luogo.....	110
Come fare un'analisi delle opportunità del proprio territorio.....	110
Ideazione e Creazione di Start-up	112
Obiettivi del modulo.....	112
Cosa è una start-up e perché è diversa da un'impresa tradizionale	112

Le fasi del processo di creazione	112
L'imprenditoria nelle aree interne: sfide e opportunità specifiche	114
Riepilogo dei concetti fondamentali	115
Test di autovalutazione.....	116
Autovalutazione delle competenze DigComp 2.2	117
Glossario essenziale	117
Risorse utili	119
tema b sicurezza e uso consapevole	121
Presentazione del capitolo	122
La rete non è un mondo parallelo: è il nostro mondo	122
Il digitale come spazio di vita, non solo di svago.....	122
Il digitale come estensione della responsabilità.....	123
Cos'è il cyberbullismo: caratteristiche, reati e meccanismi psicologici	124
Obiettivi del modulo.....	124
Dal bullismo al cyberbullismo: cosa cambia.....	124
Quando il comportamento online diventa reato.....	125
Le forme di aggressione online: riconoscerle per contrastarle	125
I meccanismi psicologici: perché le persone diventano aggressive online ..	126
Gli attori, i fattori di rischio e le conseguenze.....	128
Obiettivi del modulo.....	128
Gli attori: molto più di bullo e vittima	128
Il potere degli spettatori: da testimoni a protagonisti	128

I fattori di rischio	129
Le conseguenze: il peso invisibile.....	130
Uso etico della rete: netiquette, privacy e pensiero critico	131
Obiettivi del modulo.....	131
La netiquette: il galateo della rete	131
L'impronta digitale: cosa lasci di te online	131
La cultura del consenso	132
Privacy e sicurezza: proteggersi attivamente	132
Il pensiero critico: l'antivirus contro i bias	132
Come rispondere: protocollo S.O.S., strumenti e quadro legale.....	134
Obiettivi del modulo.....	134
Il protocollo S.O.S.: cosa fare quando succede.....	134
Gli strumenti tecnologici di protezione.....	135
Il quadro normativo: la Legge 71/2017 e i reati digitali.....	135
La cultura dell'inclusione: da spettatori ad alleati	137
Obiettivi del modulo.....	137
L'empatia digitale: vedersi nell'altro	137
La responsabilità collettiva: il cyberbullismo si vince con la cultura	137
Il toolkit: le cinque regole d'oro.....	138
Il ruolo degli adulti: genitori, educatori e comunità.....	139
Perché il dialogo è più efficace del controllo.....	139
Come parlare di cyberbullismo con i giovani	139

Il ruolo della scuola: oltre la Legge 71/2017	140
La comunità come rete di protezione	140
Imparare dai casi: scenari e riflessioni	141
Scenario 1: il gruppo di classe	141
Scenario 2: l'ex partner	141
Scenario 3: lo spettatore	142
Scenario 4: l'adulto e la truffa digitale.....	142
Riepilogo dei concetti fondamentali	143
Test di autovalutazione.....	144
Glossario essenziale	144
Risorse e contatti utili.....	146
tema b sicurezza e uso consapevole	147
Presentazione del capitolo	148
La rete come opportunità: navigare con consapevolezza.....	148
Il digitale è ovunque: saper navigare è saper vivere	148
I rischi reali di una navigazione inconsapevole.....	149
Fondamentali della Navigazione Digitale	150
Obiettivi del modulo.....	150
Gli strumenti per navigare: i browser.....	150
Anatomia di un browser: gli strumenti essenziali.....	151
Come funziona un motore di ricerca	152
Verificare la sicurezza di un sito web	153

Fondamentali della Comunicazione Digitale.....	155
Obiettivi del modulo.....	155
COMUNICAZIONE ASINCRONA: L'EMAIL	155
Molto più di un semplice messaggio.....	155
A, CC e CCN: privacy nella comunicazione di gruppo	155
Regole di etichetta e sicurezza nell'uso dell'email.....	156
COMUNICAZIONE SINCRONA: APP DI MESSAGGISTICA	156
Comunicare in tempo reale	156
AGORÀ VIRTUALI: I SOCIAL NETWORK	157
Social network e forum: spazi diversi per scopi diversi.....	157
RISCHI E VANTAGGI DELL'INFORMAZIONE DIGITALE	158
Le dinamiche cognitive dei social network.....	158
Creatività Digitale	160
Condividere in sicurezza: la gestione dei permessi.....	160
Diritto d'autore e licenze Creative Commons.....	161
Difendere i propri account: password e autenticazione	162
La password: prima linea di difesa	162
L'autenticazione a due fattori	162
I dati personali: cosa proteggere e come	162
Le truffe online: riconoscerle e difendersi.....	164
Il panorama delle truffe digitali	164
Il phishing nelle sue forme moderne	164

Le truffe sugli acquisti online	164
Le truffe romantiche	164
Cosa fare se si è vittime di una truffa.....	165
Intelligenza Artificiale e informazione: le nuove sfide.....	166
L'AI nella vita quotidiana: già presente, spesso invisibile	166
I deepfake: quando vedere non è più credere	166
Le allucinazioni dei modelli linguistici	166
Usare l'AI con consapevolezza.....	167
Identità digitale e reputazione online	168
La tua presenza online: costruirla o subirla.....	168
L'impronta digitale e le sue conseguenze.....	168
Il diritto all'oblio: come esercitarlo.....	168
Costruire una reputazione digitale positiva	168
Riepilogo dei concetti fondamentali	169
Test di autovalutazione.....	170
Glossario essenziale	170
Risorse utili	172
tema b sicurezza e uso consapevole	173
A chi è rivolto questo capitolo.....	174
Welcome to the Digital Village: perché serve la netiquette	175
Online ci capiamo davvero?	175
Le parole corrono più veloci delle intenzioni	175

Cos'è la netiquette	176
Digital Fair Play: le buone maniere che cambiano tutto.....	177
Obiettivi del modulo.....	177
Il fair play nella comunicazione digitale	177
Le 10 regole d'oro della netiquette.....	177
Comportamenti scorretti: riconoscerli per non perpetuarli	179
Impronte Digitali: tracce, rischi e potere dell'immagine online	180
Obiettivi del modulo.....	180
Identità digitale: cos'è e da cosa è composta	180
L'impronta digitale: volontaria e involontaria.....	180
Gli errori più comuni: oversharing e commenti impulsivi	181
Reputazione online: come si costruisce e come si protegge.....	181
Write Don't Fight: comunicare senza creare conflitti.....	183
Obiettivi del modulo.....	183
L'email: lo strumento più frainteso del web.....	183
Chat e gruppi: le regole del flusso	183
Le cinque trappole comunicative	184
Comunicazione assertiva: la terza via	185
Digital Teampay: collaborare senza caos	186
Obiettivi del modulo.....	186
Il documento condiviso come spazio comune	186
I commenti: strumenti di collaborazione, non di giudizio.....	186

Gli errori più comuni che fanno litigare i team digitali	186
Il patto di collaborazione	187
Conclusione: Il Patto delle Buone Connessioni	188
Riepilogo dei concetti fondamentali	188
Kit Netiquette: strumenti per la vita reale	189
Le 10 regole d'oro della netiquette.....	189
Checklist “Prima di inviare”	190
Mini-guida alla collaborazione digitale.....	190
Identità e reputazione online: cosa tenere a mente	190
Guida tascabile alla Netiquette	190
Test di autovalutazione finale	191
Autovalutazione delle competenze DigComp 2.2	192
Glossario essenziale	192
Gestire i conflitti digitali: dalla teoria alla pratica.....	193
Quando la comunicazione diventa conflitto.....	193
Il protocollo di de-escalation	194
I conflitti nei gruppi: regole specifiche	194
Il benessere digitale	195
tema b sicurezza e uso consapevole	196
A chi è rivolto questo capitolo.....	197
Perché la sicurezza digitale riguarda tutti.....	198
I numeri della cybercriminalità in Italia	198

La cybersicurezza è soprattutto comportamento.....	198
Opportunità della Rete: Web, Smartphone e Cybersicurezza	199
Obiettivi del modulo.....	199
Lo smartphone: la rivoluzione in tre passi	199
I dati: chi ha guadagnato di più dalla rivoluzione smartphone	200
L'evoluzione del Web: da biblioteca a piazza a ecosistema di valore.....	200
La cybersicurezza: perché è diventata urgente	201
Difendere il dispositivo: sistemi di protezione passiva.....	202
Obiettivi del modulo.....	202
L'analogia della casa: proteggere il digitale come la vita reale.....	202
Il Firewall: il muro di cinta digitale.....	202
L'antimalware: dalla lista nera all'analisi comportamentale.....	203
Gli aggiornamenti: chiudere le finestre rotte.....	203
I tipi di malware: conoscere il nemico	204
Filtri Antispam: il sistema di Vigilanza attiva	205
I fattori di sicurezza: password, 2FA e biometria.....	207
Obiettivi del modulo.....	207
I tre fattori di sicurezza	207
Le password: lunghezza batte complessità.....	208
L'autenticazione a due fattori: il doppio lucchetto	209
Il riconoscimento biometrico: come funziona davvero.....	209
La Cassaforte Digitale: backup e protezione dei dati.....	211

Obiettivi del modulo.....	211
Perché il backup è la misura di sicurezza più importante	211
La regola 3-2-1: il gold standard del backup.....	211
I tipi di backup: scegliere quello giusto	212
Riepilogo dei concetti fondamentali	213
Test di autovalutazione.....	214
Autovalutazione delle competenze DigComp 2.2	215
Glossario essenziale	215
tema b sicurezza e uso consapevole	218
A chi è rivolto questo capitolo.....	219
Navigare lascia tracce: cosa succede davvero online	219
Truffe online: fenomeno in crescita	219
I nostri dati sono il “nuovo oro”	220
Cookie, Tracce e Privacy nella Navigazione	221
Obiettivi.....	221
Le tracce invisibili: i cookie. Biscotti dolci o amari?	221
Le tracce invisibili: il Fingerprinting. Come un'impronta.....	222
Le tracce visibili: cronologia e storico delle ricerche	222
La navigazione in incognito: un mantello parziale	223
La VPN: il vero scudo della navigazione.....	224
Permessi delle App.....	225
Active Listening: gli smartphone ci ascoltano?	225

I permessi delle app: come comportarsi	225
ID Pubblicitario: il Santo Graal del marketing.....	226
Social Engineering: la psicologia della truffa.....	228
Cos'è il social engineering.....	228
I tre grimaldelli emotivi	228
I tre canali della truffa digitale	229
Gli Scenari di Truffa: riconoscere e difendersi	230
Il finto pacco – Smishing	230
Lo spear phishing – Il phishing personalizzato	230
La truffa e-commerce – L'affare del secolo.....	231
Il romance scam – Il principe azzurro digitale.....	231
Il tech support scam – Il finto tecnico.....	232
Il phishing bancario – La banca in panico.....	232
Il man in the middle – L'intercettazione sul Wi-Fi	233
I trojan bancari – Le spie in tasca.....	233
E-commerce in sicurezza: comprare online senza sorprese	234
1. Cosa osservare in un sito E-commerce	234
3. Come smascherare truffe dei rivenditori sui Marketplace	235
Buone pratiche per scongiurare una Truffa	235
Comandamenti della Banca online	236
Riepilogo dei concetti fondamentali	237
Test di autovalutazione.....	238

Autovalutazione delle competenze DigComp 2.2	239
Glossario essenziale	239
Contatti utili in caso di truffa	241
tema b sicurezza e uso consapevole	242
A chi è rivolto questo capitolo.....	243
Welcome to the Fake Jungle: la giungla dell'informazione	243
Iris Feed e l'ecosistema informativo digitale	243
Dato, informazione, misinformazione, disinformazione	244
Perché le fake news si diffondono: algoritmi, viralità, camere dell'eco.....	245
Le emozioni come punto di partenza	245
Fake News Anatomy: dentro la macchina della disinformazione	247
Obiettivi del modulo.....	247
Cos'è davvero una fake news.....	247
La struttura di una fake news: gli elementi ricorrenti	247
Fake news vs clickbait: una distinzione importante.....	248
La zona grigia informativa.....	248
I meccanismi psicologici: perché funziona su tutti	249
Fake or Real Tools: verificare fonti e contenuti.....	250
Obiettivi del modulo.....	250
Opinione o informazione verificata?	250
I tre controlli minimi: Fonte, Data, Riscontro	250
1. Verificare la fonte	250

2. Verificare la data	251
3. Verificare il riscontro	251
Strumenti di verifica: il toolkit pratico	252
Le immagini e i video fuori contesto	253
Clickbait e Manipolazione: come non cascare nel tranello.....	254
Obiettivi del modulo.....	254
Cos'è il clickbait e perché funziona.....	254
Le tecniche linguistiche del clickbait	255
Dal clickbait alla manipolazione.....	255
I dark pattern informativi.....	256
Condividere non è neutro	256
Le 5 regole d'oro per la verifica orizzontale	257
Il Kit Anti-Fake: strumenti pratici da portare a casa.....	258
Checklist rapida di verifica.....	258
Segnali di allarme immediati	259
Riepilogo dei concetti fondamentali	259
Test di autovalutazione finale	261
Autovalutazione delle competenze DigComp 2.2	262
Glossario essenziale	262
tema c Accesso ai servizi essenziali.....	265
A chi è rivolto questo capitolo.....	266
L'era digitale non fa la coda	267

La paura del digitale: un ostacolo reale, ma superabile	267
Tre vantaggi concreti dei servizi digitali che cambieranno la tua quotidianità....	268
La nostra bussola: il quadro DigComp 2.2	269
Verso l'autonomia digitale	269
SPID e CIE: due strumenti, una sola identità.....	270
L'attivazione dello SPID	270
Come si attiva la CIE per il suo utilizzo digitale	271
La sicurezza: autenticazione a due fattori.....	272
Le Tre regole d'oro per proteggere le tue credenziali	273
Dalla difficoltà alla familiarità.....	273
La Pubblica Amministrazione digitale: ANPR, INPS e Sinfonia	274
ANPR: il Comune che non chiude mai.....	274
L'autocertificazione: il tuo diritto che in pochi conoscono.....	274
INPS: non solo pensioni.....	275
L'app Sinfonia: la sanità campana in tasca	275
E-mail e PEC: la comunicazione ufficiale con gli enti	276
PagoPA: pagare la PA in modo sicuro e semplice	277
Che cos'è PagoPA e perché è diverso da una banca	277
Come leggere un avviso di pagamento PagoPA	278
I canali di pagamento: libertà di scelta e continuità del sistema	279
L'App IO: un punto di accesso ordinato ai pagamenti pubblici	279
La sicurezza del sistema e la regola anti-phishing.....	280

La ricevuta elettronica: prova del pagamento e strumento di tutela.....	280
Dal pagamento alla gestione ordinata del proprio portafoglio digitale.....	281
Quando qualcosa va storto: problem solving e facilitatori	282
Il primo passo: l'autovalutazione.....	282
I trucchi pratici per i problemi più comuni.....	282
I Punti di Facilitazione Digitale: la tua rete di supporto	283
Come chiedere aiuto in modo efficace	283
Il tuo Kit Digitale: riepilogo del percorso.....	284
Un consiglio finale: pratica, pratica, pratica.....	284
Piccolo glossario dei termini usati nel corso.....	285
tema c Accesso ai servizi essenziali.....	287
A chi è rivolto questo capitolo.....	288
Perché la sanità digitale riguarda tutti noi.....	288
I vantaggi concreti del digitale nella sanità	288
La bussola DigComp 2.2	289
SPID, CIE e CNS: la chiave d'accesso al digitale	290
Cosa significa essere cittadino digitale	290
I tre strumenti di autenticazione: SPID, CIE e CNS	290
Come ottenere SPID: la procedura passo per passo.....	291
Come attivare CIE: pochi passaggi in massima sicurezza	291
L'autenticazione a due fattori: la doppia difesa	292
Password sicure: come crearle e gestirle.....	292

Il logout: chiudere la porta	293
Le trappole del web: phishing e ingegneria sociale	293
Il Fascicolo Sanitario Elettronico (FSE).....	295
Cos'è il FSE e perché cambia tutto	295
Cosa contiene il FSE	295
Il consenso informato: tu sei il titolare dei tuoi dati	296
Come accedere al FSE tramite Sinfonia.....	296
I benefici del FSE per la cura e la sostenibilità	297
Il futuro del FSE: verso l'interoperabilità	297
CUP, Scelta del Medico e PagoPA: Sinfonia al lavoro.....	298
Il portale Sinfonia: lo sportello sanitario in tasca	298
Scegliere e cambiare il medico di base	298
Prenotare una visita specialistica con il CUP Web	298
PagoPA: il pagamento del ticket in sicurezza.....	299
Esenzioni Ticket: conoscere i propri diritti	301
Il ticket sanitario e il principio di equità.....	301
Due tipi di esenzione: patologia e reddito.....	301
Il ruolo del MEF e il rinnovo automatico	302
Come verificare le proprie esenzioni	302
Il futuro della medicina digitale	303
Le nuove frontiere: telemedicina, AI e interoperabilità.....	303
La sostenibilità della sanità digitalizzata	303

I tre impegni del cittadino digitale	304
Test di autovalutazione finale.....	305
Autovalutazione delle competenze DigComp 2.2	306
Glossario essenziale	306
INTERVISTE DAP.....	309

Le presenti dispense sono pensate come uno strumento didattico di accompagnamento allo sviluppo delle competenze digitali. L'obiettivo non è solo fornire indicazioni di funzionamento, ma anche guidare progressivamente il lettore verso un uso più consapevole, autonomo e sicuro del digitale nella vita quotidiana, nel lavoro, nella relazione con la Pubblica Amministrazione e nell'accesso ai servizi essenziali.

Il percorso parte da un presupposto: oggi una grande quantità di azioni ordinarie passano attraverso canali digitali. Cercare lavoro, scrivere e inviare un Curriculum Vitae, consultare un portale istituzionale, accedere con SPID o CIE, prenotare una visita sanitaria, effettuare un pagamento tramite PagoPA, proteggere i propri dati personali, riconoscere una truffa online o verificare l'attendibilità di una notizia sono attività che hanno progressivamente rimodellato la nostra quotidianità.

Per questo motivo, possedere competenze digitali non rappresenta un vantaggio accessorio, ma una condizione necessaria per partecipare in modo attivo alla vita sociale. Questo aspetto assume una rilevanza particolare nel contesto della Regione Campania, caratterizzato da importanti trasformazioni economiche, sociali e tecnologiche. In questa prospettiva, le dispense sono state concepite come uno strumento concreto, pensato per supportare l'impatto reale che le tecnologie hanno sulla capacità delle persone, ad esempio, di utilizzare i servizi disponibili, cogliere le opportunità del territorio e partecipare in modo più consapevole alla vita della comunità.

Ogni sezione di queste dispense affronta un ambito specifico e propone spiegazioni chiare, esempi, indicazioni pratiche, riepiloghi, glossari e attività di autovalutazione. Questa struttura è pensata per consentire al lettore di procedere per gradi, dapprima comprendendo i concetti fondamentali, poi per riconoscere gli strumenti disponibili e, infine, applicare quanto appreso in situazioni concrete. L'intento è rendere il digitale più vicino, più leggibile e meno distante da chi non lo utilizza abitualmente o non ne sfrutta a pieno le potenzialità.

Un riferimento importante del percorso è il quadro europeo DigComp 2.2, che individua le principali aree di competenze digitali necessarie per i cittadini. Le dispense riprendono tali aree in modo pratico, collegandole a bisogni reali, come cercare e valutare informazioni, comunicare e collaborare online, creare contenuti digitali, proteggere dati e dispositivi, risolvere problemi attraverso la tecnologia. Le competenze non vengono presentate come nozioni astratte, ma come capacità utili per orientarsi meglio nei diversi contesti della vita quo-

tidiana permeati dal digitale, mettendolo al servizio della comunità.

Un primo asse tematico riguarda lo sviluppo professionale nel contesto digitale. Le dispense spiegano come costruire un Curriculum Vitae efficace, come distinguerlo da una lettera di presentazione, evitare gli errori più comuni, personalizzare una candidatura e utilizzare strumenti come Europass, LinkedIn e altre piattaforme per la ricerca di lavoro. Questo blocco didattico aiuta il lettore a comprendere che la ricerca di occupazione richiede metodo, chiarezza e capacità di presentare correttamente le proprie esperienze e competenze. La capacità di comunicare con chiarezza le proprie competenze, nel contesto digitale, per risultare competitivi sul mercato del lavoro va allenata con strumenti adeguati e le presenti dispense si pongono questo come uno degli obiettivi principali.

Un secondo nucleo di queste dispense riguarda la cittadinanza digitale e il rapporto con la Pubblica Amministrazione: ANPR, INPS, Fascicolo Sanitario Elettronico, PagoPA, App IO, PEC, SPID, CIE e CNS sono strumenti che permettono di accedere a certificati, comunicazioni, pagamenti, prestazioni e informazioni personali. Conoscerli significa ridurre la dipendenza da intermediari, evitare passaggi che rallentano processi e gestire con maggiore autonomia pratiche che incidono direttamente sui propri diritti.

Una particolare attenzione è dedicata ai servizi digitali che oggi rappresentano punti di accesso fondamentali ai diritti di cittadinanza. Nel contesto campano, strumenti come il Fascicolo Sanitario Elettronico e la piattaforma Sinfonia consentono di consultare documenti sanitari, monitorare il proprio percorso di cura e accedere a servizi che fino a pochi anni fa richiedevano procedure più complesse. Comprendere il funzionamento di questi strumenti significa poter esercitare in modo più efficace il diritto alla salute e interagire con il sistema sanitario regionale in maniera più semplice, trasparente e autonoma.

In questa prospettiva, il digitale viene inquadrato all'interno di un'infrastruttura al servizio di una maggiore trasparenza dei processi. Accedere direttamente ai propri dati, verificare lo stato di una pratica, conservare una ricevuta, controllare un pagamento o consultare documenti personali sono pratiche che consentono al cittadino di avere un ruolo più attivo. La trasparenza, però, diventa realmente utile solo quando le informazioni sono comprese in maniera adeguata. Per questo le dispense insistono sulla necessità di un linguaggio chiaro e si avvalgono di esempi concreti.

Una terza parte di questo elaborato è dedicata alla sicurezza digitale. La diffusione degli strumenti online ha aumentato le opportunità, ma anche i rischi correlati. Le dispense affrontano temi come la necessità di avere password sicure, l'autenticazione a due fattori, altre operazioni come il backup dei dati,

il rischio di dinamiche di cosiddetto phishing, truffe digitali, social engineering, tutela dei dati personali, privacy e reputazione online. Tutti questi sono aspetti concreti che rappresentano pericoli ai quali si può andare incontro in assenza di una consapevolezza adeguata. L'obiettivo didattico è fornire linee guida a sostegno di comportamenti semplici ma efficaci, che permettano di prevenire errori frequenti e di riconoscere situazioni potenzialmente pericolose.

Un ulteriore ambito riguarda l'informazione online. Saper navigare non significa soltanto trovare risultati su un motore di ricerca, ma anche valutare l'affidabilità delle fonti, distinguere notizie verificate da contenuti manipolati, riconoscere fake news, clickbait, immagini fuori contesto e deepfake. Questo aspetto è particolarmente importante perché la qualità delle informazioni influenza decisioni personali, professionali e collettive. Le dispense propongono quindi strumenti di verifica, controlli minimi e buone pratiche per sviluppare un atteggiamento critico verso ciò che circola in rete.

Grande attenzione è riservata anche alla comunicazione digitale e agli strumenti principali attraverso i quali essa avviene. E-mail, chat, social network, forum e documenti condivisi sono ambienti in cui le persone collaborano, discutono, si confrontano e talvolta entrano in conflitto. Per questo il percorso include la netiquette, una consuetudine per il corretto uso della comunicazione con gli utenti, rispettandone l'alterità, preconditione ottenuta grazie a disposizioni come la gestione dei toni, la comunicazione assertiva, il rispetto della privacy altrui e la responsabilità dei contenuti condivisi. Risulta di fondamentale importanza – se si pensa a uno dei principali problemi cui si può andare incontro utilizzando il digitale, il fenomeno del cyberbullismo – tutelare le persone dall'impatto della comunicazione mediata dagli strumenti digitali. Anche in questo caso, l'obiettivo è pratico: aiutare il lettore a comunicare meglio, evitare fraintendimenti e utilizzare gli strumenti digitali in modo corretto e rispettoso.

Il tema dell'inclusione attraversa in maniera carsica tutto il percorso didattico. Le competenze digitali permettono a più persone di accedere a opportunità formative, lavorative e amministrative. Chi sa usare i servizi online può risparmiare tempo, superare alcune barriere fisiche, controllare più facilmente le proprie informazioni e partecipare in modo più attivo alla comunità. Tuttavia, l'inclusione non è una facoltà automatizzata, ma richiede accompagnamento, chiarezza, gradualità e attenzione ai diversi livelli di partenza. Per questo le dispense adottano un'impostazione didattica progressiva, evitando tecnicismi e privilegiando esempi immediatamente applicabili.

Il lettore viene, quindi, accompagnato in un percorso che procede dal semplice al complesso. Seguendo un percorso introduttivo, vengono spiegati i concetti

di base e gli strumenti principali, si spiegano le procedure più ricorrenti e si propongono criteri per agire in modo autonomo. Ogni modulo ha la funzione precisa di orientare, spiegare, consolidare e rendere spendibili le conoscenze acquisite. Le schede di autovalutazione e i glossari finali hanno proprio la funzione di aiutare chi legge a verificare la tenuta di quanto compreso, fissando termini chiave come una bussola per orientarsi nel profluvio di contenuti. L'utilità delle dispense consiste nella possibilità di tornare sui contenuti ogni volta che si presenta un bisogno concreto. In questo senso, il materiale non è pensato per una lettura meramente teorica, ma per un uso pratico e ricorrente ogni volta che si manifesta un bisogno particolare da parte del lettore.

In conclusione, imparare a usare il digitale in modo consapevole significa poter accedere con maggiore sicurezza ai servizi, comprendere meglio le informazioni, tutelare i propri dati, comunicare in modo più efficace e far valere i propri diritti. È questo il risultato formativo principale: creare cittadini più preparati e più capaci di utilizzare il digitale a beneficio proprio e della comunità.

Al tempo stesso, queste dispense rappresentano uno dei risultati più significativi del progetto promosso dalla Fondazione IFEL Campania, costituendo un patrimonio formativo destinato a rimanere disponibile oltre la conclusione delle attività progettuali, offrendo ai cittadini uno strumento organico e accessibile per l'acquisizione delle competenze digitali fondamentali, valorizzandosi, dunque, come strumento di legacy per il territorio. In questo senso, il valore dell'iniziativa non si esaurisce nell'esperienza formativa immediata, ma mira a produrre un impatto duraturo, capace di rafforzare l'autonomia delle persone, favorire l'inclusione digitale e sostenere una partecipazione più attiva alla vita sociale, lavorativa e istituzionale del territorio.

La scelta di mettere a disposizione questo materiale risponde a una visione della formazione come bene comune e leva di sviluppo territoriale. In uno scenario in cui il digitale è pensato per contribuire a ridurre distanze geografiche, favorire nuove opportunità professionali e rafforzare la coesione delle comunità, soprattutto nelle aree interne della regione, la diffusione delle competenze digitali assume una valenza che supera il singolo individuo e coinvolge l'intero tessuto sociale. È in questa prospettiva che la Fondazione IFEL Campania mette a disposizione queste dispense come un patrimonio formativo destinato a rimanere disponibile nel tempo e che mira a generare un impatto concreto, sostenendo l'acquisizione di competenze utili nella vita quotidiana e contribuendo a rendere il digitale uno strumento sempre più accessibile, inclusivo e capace di creare valore per il territorio.

TEMA A

LAVORO E SVILUPPO PRODUTTIVO

 **CREAZIONE E PRESENTAZIONE DI UN CV**



Digita Facile
Campania

A chi è rivolto questo capitolo

Questo capitolo è stato pensato per chi si avvicina per la prima volta – o quasi – al mondo del lavoro digitale e alla scrittura di un documento fondamentale: il curriculum vitae. Non è necessario avere competenze informatiche avanzate per trarne beneficio. Basta la curiosità di imparare e la voglia di mettere in ordine, su carta (o sullo schermo), tutto ciò che si è fatto, studiato e vissuto.

Il materiale che segue accompagna il percorso formativo proposto nell'ambito del progetto “Digita Facile Campania”, promosso dalla Fondazione IFEL Campania con il sostegno del Fondo per la Repubblica Digitale. Si inserisce nel Tema A – Lavoro e Sviluppo Produttivo – e adotta come riferimento teorico il quadro europeo DigComp 2.2, che definisce le competenze digitali necessarie per essere cittadini autonomi e attivi nella società contemporanea.

Il capitolo è articolato in quattro moduli, ognuna delle quali approfondisce un aspetto diverso del curriculum vitae: dalla sua natura e funzione, alla struttura e agli errori da evitare, fino alla personalizzazione per le diverse candidature e all'uso degli strumenti digitali disponibili. Ogni sezione è scritta in un linguaggio semplice e diretto, con esempi concreti e suggerimenti pratici immediatamente applicabili.

Tieni sempre con te questo capitolo quando scrivi o aggiorni il tuo curriculum vitae. Tornarci ogni volta che hai un dubbio è il modo migliore per farla fruttare.

Essere cittadini digitali: da dove si comincia

Il digitale non è solo un'App

Quando si parla di competenze digitali, la prima immagine che viene in mente è spesso quella di uno smartphone da usare o di un'applicazione da scaricare. In realtà, il digitale è qualcosa di molto più ampio e più profondo: è un insieme di strumenti, conoscenze e comportamenti che ci permettono di esercitare i nostri diritti, risparmiare tempo e denaro, accedere a servizi che altrimenti richiederebbero lunghe attese o spostamenti costosi.

Diventare cittadini digitali competenti non significa semplicemente saper usare un computer. Significa acquisire autonomia: la capacità di muoversi nel mondo digitale senza dipendere sempre dall'aiuto degli altri, di riconoscere le opportunità che la rete offre e, allo stesso tempo, di proteggersi dai rischi.

Il digitale è uno strumento di inclusione. Chi lo conosce e lo usa con consapevolezza ha accesso a un numero molto maggiore di opportunità, soprattutto nel

mondo del lavoro. Chi ne è escluso, invece, rischia di restare indietro rispetto a un contesto che cambia rapidamente. Colmare questo divario è esattamente l'obiettivo di questo percorso formativo.

I vantaggi concreti: tempo, autonomia, inclusione

Tre grandi categorie di vantaggi rendono l'acquisizione di competenze digitali un investimento che vale la pena fare, indipendentemente dall'età e dal punto di partenza.

Il primo vantaggio è il risparmio di tempo e denaro. Molte pratiche burocratiche, prenotazioni e ricerche che in passato richiedevano spostamenti fisici oggi possono essere completate comodamente da casa, in pochi minuti, senza spese di trasporto e senza lunghe attese. Questo non riguarda soltanto chi è giovane e abituato alla tecnologia: riguarda tutti.

Il secondo vantaggio è l'autonomia e la trasparenza. Usare i servizi digitali significa avere il controllo diretto sulle proprie informazioni, sui propri documenti, sui propri pagamenti. Non si dipende da intermediari, non si rischia di perdere appuntamenti o scadenze. Le interfacce moderne sono progettate per essere accessibili anche a chi non ha mai usato un computer: il sistema touch, i pulsanti grandi, i messaggi chiari rendono l'esperienza sempre più semplice.

Il terzo vantaggio è l'inclusione. Il digitale non è un lusso per pochi: è sempre più spesso il canale principale attraverso cui si accede a servizi essenziali, si cerca lavoro, si comunica con le istituzioni. Impararlo significa non essere tagliati fuori.

La bussola digitale: il quadro DigComp 2.2

Per orientarsi nel vasto mondo delle competenze digitali, l'Unione Europea ha sviluppato uno strumento chiamato DigComp, giunto alla versione 2.2. Si tratta di un quadro di riferimento che descrive le competenze che ogni cittadino dovrebbe possedere per partecipare attivamente alla società digitale.

DigComp organizza le competenze in cinque grandi aree: la gestione delle informazioni e dei dati, la comunicazione e la collaborazione online, la creazione di contenuti digitali, la sicurezza e la protezione dei dati personali, la capacità di risolvere i problemi con l'aiuto della tecnologia. Questo percorso formativo si muove all'interno di queste aree, con particolare attenzione a quelle più utili nel contesto del lavoro e dello sviluppo professionale.

Non è necessario conoscere DigComp nei dettagli per seguire questo corso. È importante sapere, però, che ogni competenza acquisita è riconosciuta e valorizzata a livello europeo. MODULO 1

IL CURRICULUM VITAE: LA CHIAVE PER IL SUCCESSO PROFESSIONALE

Obiettivi del modulo

Al termine di questo primo modulo saprai spiegare cos'è un curriculum vitae e perché è così importante nel processo di ricerca del lavoro. Sarai in grado di distinguerlo dalla lettera di presentazione e comprenderai qual è il ruolo che ciascuno dei due documenti svolge nella candidatura a un posto di lavoro.

Cos'è un curriculum vitae

L'espressione "curriculum vitae" viene dal latino e significa, letteralmente, "percorso della vita". È un documento scritto in cui una persona racconta, in forma ordinata e sintetica, la propria storia formativa e professionale: gli studi compiuti, le esperienze lavorative maturate, le competenze acquisite e le informazioni necessarie per essere contattata.

Si tratta, in sostanza, del biglietto da visita di chi cerca lavoro. Prima ancora di incontrare di persona un potenziale datore di lavoro, è il curriculum vitae a parlare per noi. Per questo motivo, deve essere curato, aggiornato e adattato al contesto in cui viene presentato.

Il curriculum vitae non è un documento da scrivere una volta e dimenticare in un cassetto. È uno strumento vivo, che va aggiornato ogni volta che si acquista una nuova esperienza, si completa una formazione o si modifica il proprio obiettivo professionale.

Perché il curriculum vitae è così importante

Nel processo di selezione del personale, il curriculum vitae è quasi sempre il primo documento che un selezionatore esamina. In molti casi, la decisione di contattare o meno un candidato viene presa esclusivamente sulla base di questo documento, prima ancora di qualsiasi incontro o colloquio.

Le aziende e le organizzazioni che cercano personale ricevono spesso decine, a volte centinaia, di candidature per una singola posizione. Il tempo che il selezionatore dedica a ciascun curriculum è molto limitato — studi e ricerche nel settore indicano che in media si tratta di circa 7 secondi. In questo breve lasso di tempo, il documento deve riuscire a trasmettere un'immagine chiara, ordinata e positiva del candidato.

Questo non significa che il curriculum vitae debba essere appariscente o creativo a tutti i costi. Significa che deve essere leggibile, logico, completo nei punti essenziali e privo di errori. La cura con cui si redige il curriculum vitae comunica, indirettamente, la cura con cui si affronta il lavoro in generale.

¹ Studio condotto da TheLadders – Eye-Tracking study - 2018

Un curriculum vitae ben fatto non garantisce il lavoro, ma un curriculum vitae trascurato può impedire di arrivare al colloquio. Curarlo è il primo passo concreto verso l'obiettivo.

La differenza tra curriculum vitae e lettera di presentazione

Spesso si sente parlare di questi due documenti come se fossero la stessa cosa, ma svolgono funzioni diverse e si scrivono in modo diverso.

Il curriculum vitae è un documento strutturato in sezioni, che racconta in modo oggettivo e sintetico l'intera storia professionale e formativa del candidato. Non contiene opinioni o considerazioni personali: si limita a riportare fatti, date, titoli, competenze. È un documento che deve essere letto rapidamente e fornire le informazioni essenziali nel minor tempo possibile.

La lettera di presentazione, invece, è un testo più libero e personale, che accompagna il curriculum vitae e spiega al selezionatore perché ci si candida per quella posizione specifica, in quella specifica azienda. È l'occasione per esprimere la propria motivazione, mostrare di conoscere l'organizzazione a cui ci si rivolge e collegare la propria esperienza alle esigenze del ruolo ricercato.

I due documenti si completano a vicenda: il curriculum vitae risponde alla domanda "Chi sei?", la lettera di presentazione risponde alla domanda "Perché dovremmo scegliere te?". In molti contesti lavorativi, specialmente per posizioni più qualificate, viene richiesto entrambi. In altri, è sufficiente il curriculum vitae.

STRUTTURA DEL CV E ERRORI DA EVITARE

Obiettivi del modulo

Al termine di questo modulo conoscerai la struttura ideale di un curriculum vitae e saprai come organizzare ciascuna sezione in modo chiaro ed efficace. Sarai inoltre in grado di riconoscere gli errori più comuni – quelli che portano un curriculum a essere scartato – e di evitarli nella redazione del tuo.

La struttura ideale di un curriculum vitae

Un curriculum vitae ben organizzato segue una struttura logica e riconoscibile. Non esiste un unico formato obbligatorio, ma alcune sezioni sono considerate imprescindibili da qualsiasi selezionatore. Presentarle nell'ordine giusto, con i contenuti appropriati, fa la differenza tra un documento che viene letto con interesse e uno che viene archiviato senza attenzione.

Dati personali e contatti

La sezione iniziale del curriculum vitae raccoglie le informazioni necessarie per identificare il candidato e contattarlo. Nome, cognome, numero di telefono e indirizzo email sono elementi imprescindibili. L'indirizzo di residenza meglio non indicarlo per motivi di privacy, è bene, invece indicare la città di domicilio. È sempre più comune inserire anche il link al proprio profilo LinkedIn, se si dispone di uno.

Attenzione all'indirizzo email: deve essere serio e professionale, composto preferibilmente da nome e cognome (ad esempio: mario.rossi@gmail.com). Indirizzi email con soprannomi, date di nascita o riferimenti informali trasmettono una scarsa cura per i dettagli.

Profilo professionale o riepilogo

Subito dopo i dati personali, molti curriculum vitae moderni includono un breve paragrafo – solitamente tre o quattro righe – che riassume chi si è, quali sono i propri punti di forza e qual è l'obiettivo professionale. Questo “biglietto da visita testuale” permette al selezionatore di avere subito un'idea del candidato, ancora prima di leggere le sezioni più dettagliate.

Un profilo professionale efficace non è generico: fa riferimento al settore specifico in cui si opera o si vuole operare, e mette in evidenza le caratteristiche più rilevanti per il ruolo a cui ci si candida.

Esperienze lavorative

Questa è, per molti selezionatori, la sezione più importante del curriculum vitae. Le esperienze devono essere elencate in ordine anti-cronologico, partendo cioè dalla più recente e risalendo nel tempo. Per ciascuna esperienza vanno

indicati: il nome dell'azienda o dell'organizzazione, il ruolo ricoperto, le date di inizio e fine (o “in corso” se si tratta dell'impiego attuale), e una breve descrizione delle principali responsabilità e dei risultati ottenuti.

Quando si descrivono le esperienze lavorative, è preferibile usare verbi d'azione e, dove possibile, dati quantificabili. Non “Mi occupavo di vendite” ma “Ho gestito un portafoglio di 30 clienti, aumentando il fatturato del 15% in un anno”. I numeri parlano chiaro e rendono le affermazioni credibili.

Istruzione e formazione

Anche questa sezione segue l'ordine anti-cronologico. Si indicano i titoli di studio conseguiti (laurea, diploma, scuola), i corsi di formazione rilevanti, le certificazioni ottenute. È importante riportare l'istituto o l'ente che ha rilasciato il titolo e l'anno di conseguimento.

Chi è all'inizio della carriera o non ha ancora esperienze lavorative significative può dare maggiore spazio a questa sezione, evidenziando materie studiate, progetti scolastici o universitari, tirocini e attività extracurricolari rilevanti.

Competenze

La sezione delle competenze si articola tipicamente in tre sottocategorie. Le competenze linguistiche indicano le lingue conosciute e il livello di padronanza, espresso preferibilmente con il riferimento al Quadro Comune Europeo di Riferimento (QCER): A1, A2, B1, B2, C1, C2. Le competenze informatiche e tecniche – dette anche hard skills – elencano i software, gli strumenti e le tecnologie che si sa usare. Le competenze trasversali – dette soft skills – descrivono le qualità relazionali e organizzative: la capacità di lavorare in team, di gestire il tempo, di risolvere problemi, di comunicare efficacemente.

Informazioni aggiuntive e autorizzazione al trattamento dei dati

In fondo al curriculum vitae si possono inserire hobby e interessi, soprattutto se pertinenti al ruolo ricercato. Volontariato, attività sportive di squadra, impegni culturali o associativi dicono qualcosa della personalità del candidato e arricchiscono il profilo.

La sezione finale, obbligatoria per legge, è l'autorizzazione al trattamento dei dati personali. Senza questa dicitura, il curriculum vitae non può essere utilizzato dall'azienda ricevente, che non è autorizzata a conservare né elaborare i dati del candidato. La formula corretta fa riferimento al Regolamento Generale sulla Protezione dei Dati (GDPR): “Autorizzo il trattamento dei miei dati personali ai sensi del D. Lgs. 196/2003 e del Regolamento UE 2016/679 (GDPR).”

Il formato EUROPASS, disponibile gratuitamente sul sito europass.europa.eu, è il modello standardizzato riconosciuto in tutta l'Unione Europea. È particolarmente indicato per candidature a concorsi pubblici, istituzioni e progetti in ambito europeo. Permette di creare il proprio curriculum in 31 lingue.

Gli errori più comuni: come riconoscerli e correggerli

Un curriculum vitae efficace non è soltanto quello scritto bene: è anche quello privo degli errori che portano, quasi automaticamente, a uno scarto immediato da parte del selezionatore. Conoscere questi errori è il primo passo per evitarli.

Dati personali sbagliati o incompleti

Può sembrare banale, ma uno degli errori più frequenti riguarda proprio i dati di contatto. Un numero di telefono errato, un'email digitata male, o un recapito mancante rendono impossibile contattare il candidato, vanificando tutto il lavoro di preparazione del documento. Prima di inviare un curriculum vitae, è buona norma verificare attentamente che tutti i dati siano corretti, aggiornati e completi.

Consiglio: Controlla il numero di telefono cifra per cifra e assicurati che l'email sia scritta correttamente. Chiedi a qualcuno di fiducia di verificarla, se non sei sicuro.

Errori grammaticali e di battitura

Un curriculum vitae con errori ortografici, refusi o costruzioni grammaticali scorrette trasmette un'immagine di scarsa attenzione e superficialità. Il selezionatore, leggendolo, conclude — spesso inconsciamente — che chi si è candidato non ha dedicato la dovuta cura al documento che avrebbe dovuto rappresentarlo al meglio. Il risultato, nella maggior parte dei casi, è l'esclusione dalla selezione.

Consiglio: Rileggi il curriculum vitae più volte, a distanza di tempo. Chiedilo anche a qualcuno di fiducia: un secondo paio di occhi nota spesso ciò che sfugge all'autore del testo.

Competenze false o esagerate

La tentazione di presentarsi in modo più qualificato di quello reale è comprensibile, ma è un errore che può avere conseguenze serie. I selezionatori esperti fanno domande specifiche durante il colloquio, contattano i precedenti datori di lavoro e verificano le referenze. Attribuirsi competenze che non si possiedono porta quasi inevitabilmente a situazioni imbarazzanti, o peggio, alla perdita del posto ottenuto.

Il curriculum vitae deve riflettere fedelmente ciò che si sa fare. La lingua italiana offre molte espressioni che permettono di descrivere le proprie competenze in modo onesto ma valorizzante: “buona conoscenza di”, “capacità di lavorare in autonomia su”, “esperienza di base con” sono formulazioni precise e credibili.

Consiglio: Scrivi solo ciò che sei davvero in grado di fare. Un profilo modesto ma veritiero vale molto più di uno brillante ma falso.

Curriculum vitae troppo lungo

Salvo casi particolari – profili con molti anni di esperienza in settori altamente specializzati – un curriculum vitae non dovrebbe superare le due pagine. I selezionatori hanno poco tempo e devono scorrere molti documenti: un curriculum lungo e ridondante rischia di non essere letto fino in fondo, o di trasmettere l'idea che il candidato non sia in grado di sintetizzare le informazioni.

Se il documento supera le due pagine, è necessario rileggerlo con spirito critico ed eliminare tutto ciò che non è direttamente rilevante per il ruolo a cui ci si candida. Meno è meglio, purché il contenuto sia di qualità.

Informazioni inutili o fuori contesto

Inserire esperienze o informazioni che non hanno alcun collegamento con il ruolo per cui ci si candida non solo occupa spazio prezioso, ma può far pensare al selezionatore che il candidato non abbia compreso la natura del lavoro. Se ci si candida per un ruolo in ambito commerciale, la prima esperienza come cameriere durante l'estate dei vent'anni probabilmente non aggiunge valore al documento. Un hobby che dimostra spirito di squadra, creatività o disciplina, invece, può essere menzionato con vantaggio.

Esperienze non aggiornate

Un curriculum vitae che presenta “buchi” temporali – periodi non spiegati tra un'esperienza e l'altra – o che non include le esperienze più recenti dà un'impressione di trascuratezza. Aggiornare il curriculum vitae dopo ogni nuova esperienza, corso o certificazione è un'abitudine che vale la pena costruire, anche quando non si è attivamente in cerca di lavoro.

Organizzazione grafica poco chiara

Un curriculum vitae difficile da leggere è un curriculum vitae che non viene letto. La struttura deve essere coerente, con sezioni ben delimitate, font leggibili, spaziatura adeguata e un uso moderato di grassetto e corsivi.

I colori sgargianti, i caratteri fantasiosi e i layout troppo elaborati possono essere appropriati in certi settori creativi, ma sono generalmente sconsigliati per candidature in ambito istituzionale, pubblico o aziendale.

La foto sbagliata

La foto, quando inserita, deve essere professionale: formato tessera, sfondo neutro, abbigliamento appropriato. Non è opportuno usare foto di gruppo, scatti in vacanza, selfie informali o immagini di bassa qualità. La foto sul curriculum vitae è un ulteriore elemento di presentazione: deve restituire un'immagine affidabile e curata.

I profili social inappropriati

Indicare i propri profili social nel curriculum vitae può essere utile, perché molte aziende effettuano ricerche online sui candidati. Tuttavia, questo vale soltanto per i profili che si vuole che i potenziali datori di lavoro vedano. Prima di includere un link, è opportuno controllare che il profilo sia aggiornato, professionale e privo di contenuti che potrebbero risultare inappropriati o contraddire l'immagine che si vuole dare. LinkedIn è il social network di riferimento per il mondo del lavoro.

Dimenticare l'autorizzazione

Come già anticipato nella sezione sulla struttura, l'autorizzazione al trattamento dei dati personali non è un optional: è un obbligo di legge. Senza questa dicitura, il curriculum vitae non può essere legalmente utilizzato dall'azienda ricevente. Verificare che sia presente e formulata correttamente è una delle ultime cose da controllare prima di inviare il documento.

Avere un solo curriculum vitae per tutte le candidature

Questo è probabilmente l'errore più sottovalutato, ma anche uno dei più penalizzanti. Un curriculum vitae efficace non è un documento fisso: è un testo che va adattato, ogni volta, alla posizione specifica per cui ci si candida e all'azienda a cui lo si invia. Non si tratta di modificare le informazioni, ma di selezionare, ordinare e presentare le proprie esperienze in modo da rispondere il più possibile alle esigenze dell'annuncio.

Questa personalizzazione è tanto più importante in un contesto in cui molte aziende utilizzano software automatici – detti ATS, Applicant Tracking System – per pre-selezionare le candidature. Questi programmi analizzano il testo del curriculum alla ricerca di parole chiave specifiche, presenti nell'annuncio di lavoro. Se il curriculum non le contiene, viene scartato automaticamente, prima ancora che un essere umano lo legga.

Consiglio: Prepara più versioni del curriculum vitae, ognuna ottimizzata per un tipo di ruolo o settore. Quando trovi un annuncio interessante, rileggi attentamente il testo e adatta il documento usando le stesse parole chiave dell'annuncio.

IL TUO CV, UN VESTITO SU MISURA

Obiettivi del modulo

Al termine di questo modulo saprai come personalizzare il tuo curriculum vitae per adattarlo a una specifica offerta di lavoro. Conoscerai il funzionamento dei sistemi ATS e capirai come strutturare il documento per superare questo primo filtro automatico e arrivare alla lettura da parte di un selezionatore in carne e ossa.

Cosa sono gli ATS e perché devi conoscerli

Con la crescita esponenziale delle candidature online, molte aziende – soprattutto quelle di dimensioni medio-grandi – hanno adottato software automatici per gestire il primo livello di selezione. Questi programmi, chiamati Applicant Tracking System (ATS), ricevono i curriculum vitae, li analizzano e li classificano in base alla corrispondenza con i requisiti indicati nell'annuncio di lavoro.

Il funzionamento di un ATS è, in apparenza, semplice: il software cerca nel testo del curriculum determinate parole chiave – titoli di studio, competenze, esperienze, strumenti specifici – e assegna un punteggio a ciascuna candidatura. I curriculum che superano una certa soglia vengono presentati al selezionatore umano; gli altri vengono archiviati o scartati automaticamente, spesso senza che nessuno li abbia mai letti.

Questo significa che, per essere davvero efficace, un curriculum vitae moderno deve essere scritto non soltanto per chi lo leggerà, ma anche – e prima ancora – per il software che lo analizzerà. Fortunatamente, le strategie per superare un ATS coincidono in gran parte con quelle per scrivere un buon curriculum vitae: chiarezza, pertinenza, uso del linguaggio dell'annuncio.

Per superare un ATS, usa un formato semplice come Word o PDF, evita tabelle, immagini e caratteri non standard nelle sezioni di testo, e inserisci le parole chiave dell'annuncio in modo naturale all'interno della descrizione delle tue esperienze e competenze.

Come personalizzare il curriculum vitae

La personalizzazione del curriculum vitae per una specifica offerta di lavoro è un processo che richiede attenzione e un po' di tempo, ma che aumenta significativamente le probabilità di essere selezionati. Si articola in alcuni passaggi fondamentali.

Il primo passo è leggere con attenzione l'annuncio di lavoro. Non si tratta di una lettura rapida: bisogna analizzare ogni parola, identificare i requisiti espli-

citamente richiesti, le competenze desiderate, il linguaggio usato dall'azienda per descrivere il ruolo. Questo linguaggio è prezioso: usarlo nel curriculum vitae aumenta la compatibilità con il sistema ATS e dimostra al selezionatore che si è compresa la natura del ruolo.

Il secondo passo è adattare il profilo professionale — le tre o quattro righe iniziali che riassumono chi si è — per farlo rispondere direttamente alle esigenze dell'annuncio. Se l'azienda cerca “un profilo con spiccate capacità di analisi dei dati”, il profilo deve menzionare esattamente questa competenza, se la si possiede.

Il terzo passo riguarda la selezione e l'ordinamento delle esperienze lavorative. Non tutte le esperienze hanno lo stesso peso per tutte le posizioni. Per una candidatura in ambito commerciale, vanno messe in evidenza le esperienze di vendita e gestione clienti; per una posizione in ambito organizzativo, quelle relative alla gestione di progetti e team. Le esperienze meno pertinenti possono essere accennate brevemente o, in alcuni casi, omesse.

Il quarto passo è verificare che le competenze elencate nella sezione apposita corrispondano a quelle richieste dall'annuncio. Se l'annuncio cita uno specifico software o una determinata certificazione, e si è in possesso di quella conoscenza, è essenziale che sia chiaramente indicata nel documento.

Il profilo LinkedIn: un curriculum sempre accessibile

LinkedIn è la principale piattaforma professionale al mondo e si è affermata come lo strumento di riferimento per chi cerca lavoro, per chi lo offre e per chi vuole costruire la propria rete di contatti professionali. Avere un profilo LinkedIn aggiornato e curato è oggi quasi indispensabile, indipendentemente dal settore in cui si opera.

Il profilo LinkedIn non sostituisce il curriculum vitae tradizionale, ma lo completa. Permette di andare oltre le due pagine del documento cartaceo, inserendo referenze, raccomandazioni di colleghi e superiori, esempi di lavoro, articoli pubblicati e molto altro. Molti selezionatori, prima di invitare un candidato a un colloquio, controllano il suo profilo LinkedIn: è quindi importante che sia coerente con il curriculum vitae e trasmetta un'immagine professionale.

La sezione più importante del profilo LinkedIn è probabilmente il “sommario” o “about”: un breve testo di presentazione che spiega chi si è, cosa si fa e cosa si sta cercando. Deve essere scritto in prima persona, essere diretto e specifico, e suscitare interesse. Non è il momento per l'elenco delle esperienze: quello viene dopo, nella sezione dedicata. È invece il momento per catturare l'attenzione con poche frasi significative.

FATTI NOTARE: LA TECNOLOGIA AL TUO FIANCO

Obiettivi del modulo

Al termine di questo modulo conoscerai i principali strumenti digitali disponibili per creare un curriculum vitae professionale. Saprai come utilizzare le piattaforme online più diffuse per la ricerca di lavoro e avrai una panoramica delle risorse disponibili, incluse quelle specifiche per il territorio campano.

Gli strumenti per creare il curriculum vitae

Oggi non è più necessario partire da un foglio bianco per scrivere un curriculum vitae. Esistono numerosi strumenti digitali – gratuiti – che offrono modelli predefiniti, guide passo dopo passo e la possibilità di creare documenti dall'aspetto professionale anche senza competenze avanzate di grafica o informatica. Conoscere questi strumenti e scegliere quello più adatto alle proprie esigenze è la prima competenza pratica di questo modulo.

Microsoft Word

Il programma di elaborazione testi più diffuso al mondo include una serie di modelli predefiniti per la creazione di curriculum vitae. È uno strumento affidabile, compatibile con quasi tutti i computer e riconoscibile da qualsiasi selezionatore. Il file prodotto può essere salvato in formato Word (.docx) o PDF, i due formati più richiesti nelle candidature online.

Google Documenti

Google Documenti è un'alternativa gratuita a Microsoft Word, accessibile direttamente dal browser senza necessità di installare alcun software. Offre modelli per il curriculum vitae e il vantaggio di poter essere utilizzato da qualsiasi dispositivo connesso a internet, con il salvataggio automatico dei dati. È particolarmente utile per chi vuole lavorare sul proprio curriculum da più dispositivi o condividerlo facilmente con altri.

Canva

Canva è una piattaforma di design grafico online che offre una vasta gamma di modelli per curriculum vitae, anche visivamente elaborati. È particolarmente apprezzata da chi opera in settori creativi – comunicazione, grafica, marketing, moda – dove un curriculum dall'aspetto originale può fare la differenza. La versione gratuita offre già molte opzioni. Attenzione: i curriculum creati con Canva, se molto grafici, potrebbero non essere letti correttamente dai sistemi ATS. Vanno quindi usati con giudizio, in base al contesto.

EUROPASS – la scelta consigliata

Il portale EUROPASS (europass.europa.eu) è il sito ufficiale dell'Unione Euro-

pea per la creazione del curriculum vitae europeo standardizzato. È completamente gratuito, disponibile in 31 lingue e produce un documento riconoscibile e apprezzato in tutta Europa. È la scelta consigliata per chi si candida a concorsi pubblici, posizioni istituzionali, programmi europei o lavori in ambito accademico.

Il processo di creazione è guidato, con indicazioni chiare su cosa inserire in ciascuna sezione. Il sito permette anche di creare un profilo digitale che può essere condiviso online tramite un link, rendendolo uno strumento completo e moderno.

Per chi non ha ancora un curriculum vitae e non sa da dove cominciare, EUROPASS è il punto di partenza ideale. La guida è chiara, il risultato è professionale e il documento viene riconosciuto ovunque in Europa.

Le piattaforme per cercare lavoro

Creare un curriculum vitae è il primo passo. Il secondo è sapere dove inviarlo e dove cercare le opportunità giuste. Le piattaforme online per la ricerca di lavoro hanno rivoluzionato questo processo, rendendo accessibili in pochi click migliaia di annunci da tutto il territorio nazionale e internazionale.

LinkedIn

LinkedIn non è soltanto un social network professionale: è anche una delle principali piattaforme di ricerca lavoro al mondo. Permette di candidarsi direttamente agli annunci pubblicati dalle aziende, di essere contattati da selezionatori e recruiter, di seguire le aziende di interesse e di costruire una rete di contatti professionali. Avere un profilo LinkedIn completo e aggiornato aumenta significativamente la visibilità presso chi cerca personale.

Indeed e Monster

Indeed è uno dei maggiori aggregatori di offerte di lavoro al mondo: raccoglie annunci da migliaia di siti diversi e li rende ricercabili in un unico posto. Monster è un'altra piattaforma storica nel settore, con una vasta offerta di posizioni in svariati settori. Entrambi permettono di caricare il proprio curriculum vitae, impostare notifiche per le nuove offerte corrispondenti al proprio profilo e candidarsi direttamente dalla piattaforma.

ClicLavoro Campania

Per chi risiede in Campania e cerca opportunità sul territorio regionale, una risorsa preziosa è il portale ClicLavoro Campania, gestito dalla Regione Campania in collaborazione con il network nazionale. È il punto di incontro ufficiale tra domanda e offerta di lavoro nella regione, con annunci di aziende locali, infor-

mazioni sui centri per l'impiego e risorse di orientamento professionale.

Domande frequenti: il CV anche senza esperienza

Una delle domande più comuni tra chi partecipa a questo tipo di percorso formativo riguarda cosa fare quando non si ha ancora un'esperienza lavorativa da inserire nel curriculum vitae. È una preoccupazione comprensibile, ma non deve diventare un ostacolo.

Chi non ha mai lavorato può comunque costruire un curriculum vitae ricco e significativo valorizzando la propria formazione scolastica o universitaria, i progetti di gruppo realizzati in ambito accademico, le attività di volontariato, i corsi di formazione seguiti, gli hobby e gli interessi che dimostrano competenze trasversali come la disciplina, la creatività o la capacità di collaborare.

L'importante è essere onesti e specifici. Non si tratta di "riempire" il documento con informazioni vaghe, ma di presentare in modo valorizzante ciò che si è davvero fatto e imparato. Un selezionatore che riceve il curriculum di una persona senza esperienza lavorativa non si aspetta un profilo da professionista affermato: si aspetta onestà, chiarezza e la dimostrazione di un atteggiamento attivo e intraprendente.

È anche utile ricordare che avere un curriculum vitae è importante non soltanto quando si cerca attivamente un lavoro. Prepararlo, anche a sedici o diciassette anni, è un esercizio prezioso: aiuta a riflettere su ciò che si è imparato, a identificare le proprie competenze e a prepararsi per le opportunità che arriveranno — stage, lavori estivi, borse di studio, programmi di scambio.

Dal curriculum vitae al colloquio: come prepararsi

Il curriculum vitae è il primo passo, ma non è l'unico. Una volta che il documento ha superato la fase di selezione e il selezionatore ha deciso di contattarti, inizia una nuova fase altrettanto importante: la preparazione al colloquio di lavoro. Conoscere il legame tra ciò che hai scritto nel curriculum e ciò che ti verrà chiesto durante il colloquio è fondamentale per arrivare all'appuntamento con sicurezza.

Il colloquio comincia dal curriculum

Il selezionatore che ti incontra per un colloquio ha quasi sempre il tuo curriculum vitae davanti a sé. Le domande che ti pone nascono direttamente da ciò che hai scritto: le esperienze lavorative, le competenze dichiarate, i risultati che hai citato. Per questo motivo, prima di un colloquio è essenziale rileggere il proprio curriculum vitae da cima a fondo, come se fosse la prima volta, e prepararsi a parlare di ogni punto in modo chiaro e concreto.

Se hai indicato di conoscere un determinato software, devi essere pronto a spiegare in quale contesto lo hai usato e con quale livello di padronanza. Se hai dichiarato di avere esperienza nella gestione di un team, il selezionatore vorrà sentire un esempio specifico. Ogni riga del curriculum vitae è un potenziale argomento di conversazione: trattala come tale.

Le domande più frequenti e come rispondervi

Esistono alcune domande che compaiono in quasi tutti i colloqui di lavoro, indipendentemente dal settore e dal ruolo. Conoscerle in anticipo e prepararsi una risposta personale e autentica è uno dei modi più efficaci per affrontare il colloquio con tranquillità.

“Parlami di te” è spesso la prima domanda. Non è un invito a raccontare la propria vita dall’infanzia: è l’occasione per fare una presentazione professionale di circa due minuti, sintetica e pertinente al ruolo. Una buona struttura è: chi sei oggi, cosa hai fatto di più rilevante, perché sei qui.

“Quali sono i tuoi punti di forza?” richiede esempi concreti, non aggettivi generici. Non basta dire “sono preciso”: occorre aggiungere “e lo dimostro nel fatto che in due anni di lavoro non ho mai consegnato un progetto in ritardo”. I punti di forza devono essere credibili e verificabili.

“Dove ti vedi tra cinque anni?” non è una domanda trabocchetto: il selezionatore vuole capire se hai un progetto professionale, se l’azienda può farne parte e se le tue ambizioni sono compatibili con il ruolo per cui ti candidi. Rispondere con onestà e con una prospettiva di crescita all’interno del settore è sempre la scelta giusta.

“Perché vuoi lavorare da noi?” richiede preparazione: devi conoscere l’azienda, la sua missione, i suoi prodotti o servizi, la sua storia recente. Una risposta generica come “perché è un’azienda importante” non convince nessuno. Una risposta specifica — “perché ho seguito il vostro progetto X e mi ha colpito l’approccio Y” — dimostra interesse reale e capacità di ricerca.

L’immagine conta: come presentarsi

Il colloquio di lavoro è un contesto professionale, e come tale richiede un abbigliamento adeguato. Non esiste una regola unica valida per tutti i settori: ciò che è appropriato per un colloquio in uno studio legale è diverso da ciò che si indosserebbe per un colloquio in una startup creativa. La regola generale è vestirsi in modo curato, pulito e sobrio, leggermente più formale rispetto a come ci si vestirebbe normalmente sul luogo di lavoro.

Anche il linguaggio del corpo comunica: una stretta di mano ferma, il contatto visivo durante la conversazione, una postura eretta ma rilassata trasmettono sicurezza e professionalità. Arrivare puntuale — o meglio, qualche minuto

prima – è un segnale di rispetto e organizzazione che il selezionatore nota sempre.

Consiglio: Fai una prova prima del colloquio: leggi il tuo curriculum vitae ad alta voce e prepara una risposta di due minuti per ognuno dei punti principali. Più ti eserciti, più sarai a tuo agio il giorno dell'appuntamento.

La tua identità digitale: reputazione online e privacy

Nel mondo del lavoro contemporaneo, la ricerca di informazioni sui candidati non si ferma al curriculum vitae. Prima di un colloquio, molti selezionatori e responsabili delle risorse umane cercano il nome del candidato sui motori di ricerca e sui social network. Ciò che trovano – o non trovano – contribuisce a formare un'impressione che può influenzare la decisione finale.

Gestire la propria identità digitale non significa censurare la propria vita privata, ma piuttosto essere consapevoli di ciò che è visibile online e assicurarsi che non contraddica l'immagine professionale che si vuole dare. È una competenza digitale a tutti gli effetti, che rientra pienamente nell'area della sicurezza del quadro DigComp.

Cosa cercano i selezionatori online

Quando un selezionatore cerca il tuo nome su Google o su LinkedIn, vuole verificare alcune cose: che le informazioni che hai fornito nel curriculum siano coerenti con ciò che appare online, che tu abbia una presenza professionale riconoscibile, e che non ci siano contenuti pubblici che potrebbero risultare problematici nel contesto lavorativo.

Non si tratta di uno spiare la vita privata delle persone: è una pratica diffusa e ormai consolidata nel processo di selezione. La buona notizia è che, con un po' di attenzione, è possibile gestire la propria presenza online in modo da trasformarla in un ulteriore punto di forza anziché in un rischio.

Come controllare e migliorare la propria presenza online

Il primo passo è fare una ricerca del proprio nome su un motore di ricerca come Google e osservare cosa appare nei risultati. Se compaiono contenuti inappropriati – foto imbarazzanti, commenti aggressivi, informazioni false – è opportuno intervenire: eliminando i contenuti direttamente, modificando le impostazioni di privacy dei profili social o, se necessario, contattando le piattaforme per richiedere la rimozione.

Il secondo passo è assicurarsi che il profilo LinkedIn sia aggiornato, completo e coerente con il curriculum vitae. Le informazioni principali – titolo professionale, esperienze, formazione – devono corrispondere a quelle del documento cartaceo. Eventuali discrepanze potrebbero sollevare dubbi sulla veridicità delle informazioni fornite.

Il terzo passo riguarda gli altri profili social. Non è necessario eliminarli, ma è consigliabile verificare le impostazioni di privacy e assicurarsi che i contenuti pubblici siano appropriati. Ciò che si posta sui social network in modo pubblico è accessibile a chiunque: selezionatori, colleghi, clienti. Una regola semplice ma efficace è chiedersi, prima di pubblicare qualcosa, se sarebbe dispiaciuto che lo vedesse un potenziale datore di lavoro.

La privacy dei dati nel processo di candidatura

Quando si invia un curriculum vitae, si condividono informazioni personali sensibili: dati anagrafici, recapiti, storia lavorativa. È importante essere consapevoli di come questi dati possono essere utilizzati e sapere che la legge prevede precise tutele in materia.

Il Regolamento Generale sulla Protezione dei Dati (GDPR) stabilisce che i dati personali possono essere trattati solo per le finalità dichiarate e solo per il tempo necessario. L'azienda che riceve un curriculum vitae è tenuta a proteggerli, a non cederli a terzi senza consenso e a eliminarli su richiesta dell'interessato.

Per questo motivo, l'autorizzazione al trattamento dei dati che si inserisce in fondo al curriculum vitae non è una semplice formalità: è la dichiarazione con cui si acconsente in modo informato all'utilizzo dei propri dati nell'ambito della selezione. Leggerla, capirla e aggiornarla ogni volta che si invia il documento è un atto di consapevolezza digitale che fa parte di una cittadinanza digitale matura.

Consiglio: Cerca il tuo nome su Google almeno una volta all'anno. Se trovi contenuti che non vorresti che un selezionatore vedesse, intervieni prima di iniziare una ricerca di lavoro. Prevenire è molto più semplice che correggere.

Riepilogo e punti chiave

Al termine di questo capitolo, hai acquisito le conoscenze e gli strumenti per affrontare uno dei passaggi fondamentali della ricerca di lavoro: la creazione di un curriculum vitae efficace e professionale. Ricapitolando i punti principali. Il curriculum vitae è il tuo biglietto da visita nel mondo del lavoro. È il primo do-

cumento che un selezionatore esamina, spesso in pochi secondi, per decidere se procedere con la tua candidatura. Curarlo non è un optional: è una necessità. La struttura ideale comprende i dati personali e i contatti, un profilo professionale sintetico, le esperienze lavorative in ordine anti-cronologico, la formazione, le competenze linguistiche e informatiche, e l'autorizzazione al trattamento dei dati personali. Ogni sezione ha uno scopo preciso e deve essere compilata con cura.

Gli errori più comuni – dati sbagliati, grammatica trascurata, informazioni false, lunghezza eccessiva, mancanza di aggiornamento – sono tutti evitabili con un po' di attenzione e metodo. Rileggere il curriculum vitae prima di inviarlo, farlo leggere a qualcuno di fiducia, verificare ogni informazione: sono abitudini semplici che fanno una grande differenza.

Il curriculum vitae non è un documento unico e immutabile: va adattato a ogni candidatura, usando il linguaggio e le parole chiave dell'annuncio di lavoro a cui ci si rivolge. Questa personalizzazione è fondamentale anche per superare i sistemi ATS che le aziende usano per la pre-selezione automatica.

Gli strumenti digitali disponibili – da EUROPASS a LinkedIn, da Google Documenti a Canva – rendono la creazione di un curriculum vitae professionale accessibile a tutti, anche senza competenze informatiche avanzate. Scegli quello più adatto al tuo contesto e inizia a usarlo.

Il momento migliore per scrivere o aggiornare il proprio curriculum vitae non è quando si cerca disperatamente un lavoro: è adesso, con calma, senza pressioni. Un curriculum vitae ben fatto, pronto all'uso, è una risorsa che apre porte anche quando non te lo aspetti.

Autovalutazione delle competenze DigComp

Al termine del percorso formativo, ti invitiamo a riflettere su ciò che hai imparato compilando questa scheda di autovalutazione. Per ciascuna area di competenza, indica il tuo livello su una scala da 1 a 5, dove 1 significa “non mi sento ancora in grado” e 5 significa “mi sento completamente autonomo”.

Area di Competenza	Prima del corso	Dopo il corso
Informazione e dati		
Comunicazione e collaborazione		
Creazione di contenuti digitali		
Sicurezza e tutela dei dati		
Risoluzione dei problemi con il digitale		

Glossario essenziale

ATS (Applicant Tracking System): software utilizzato dalle aziende per analizzare automaticamente i curriculum vitae in base a parole chiave e criteri di compatibilità con il ruolo ricercato.

DigComp: Quadro Europeo delle Competenze Digitali per i Cittadini. Uno strumento sviluppato dall'Unione Europea che descrive le competenze digitali necessarie per la piena partecipazione alla società e al mondo del lavoro.

EUROPASS: piattaforma ufficiale dell'Unione Europea (europass.europa.eu) per la creazione di curriculum vitae standardizzati, riconosciuti in 31 paesi europei.

GDPR (General Data Protection Regulation): Regolamento Generale sulla Protezione dei Dati dell'Unione Europea, che disciplina il trattamento dei dati personali. Deve essere citato nell'autorizzazione al trattamento dei dati inserita nel curriculum vitae.

Hard skills: competenze tecniche specifiche, acquisite attraverso formazione e pratica (es. uso di un software, conoscenza di una lingua straniera, gestione di macchinari).

LinkedIn: principale piattaforma di networking professionale al mondo, utilizzata per cercare lavoro, costruire la propria rete di contatti e farsi trovare da selezionatori e aziende.

Ordine anti-cronologico: criterio di organizzazione delle informazioni che prevede di partire dall'esperienza o dalla formazione più recente, risalendo a ritroso nel tempo. È lo standard per curriculum vitae ed esperienze lavorative.

PDF: formato di file (Portable Document Format) che preserva la grafica e l'impaginazione del documento indipendentemente dal dispositivo su cui viene

ne aperto. È uno dei formati più richiesti per l'invio di curriculum vitae.

QCER: Quadro Comune Europeo di Riferimento per le Lingue. Definisce i livelli di conoscenza linguistica su una scala che va da A1 (livello base) a C2 (livello avanzato).

Recruiter/Selezionatore: persona incaricata di gestire il processo di ricerca e selezione del personale per conto di un'azienda o di un'agenzia specializzata.

Soft skills: competenze trasversali di natura relazionale e comportamentale (es. capacità di lavorare in team, comunicazione efficace, gestione dello stress, problem solving).

Per ulteriori informazioni sul progetto e per conoscere il calendario dei prossimi corsi, visita il sito della Fondazione IFEL Campania oppure consulta la pagina dedicata al progetto su ifelcampania.it/eventi.

TEMA A
LAVORO E SVILUPPO PRODUTTIVO
FORMAZIONE E SERVIZI DIGITALI



Digita Facile
Campania

A chi è rivolto questo capitolo

Questo capitolo accompagna il percorso formativo dedicato al tema Formazione e Servizi Digitali, sviluppato nell'ambito del progetto Digita Facile Campania. Si rivolge a cittadine e cittadini che desiderano comprendere come funziona il mercato del lavoro nell'era digitale, quali strumenti istituzionali esistono per trovare o riqualificarsi nel lavoro, e in che modo le competenze digitali siano diventate oggi una condizione essenziale per accedere a queste opportunità.

Il capitolo è articolato in quattro moduli progressivi. Il primo affronta le grandi trasformazioni del mercato del lavoro portate dalla digitalizzazione e introduce il concetto di divario di competenze. Il secondo esplora le piattaforme istituzionali disponibili a livello nazionale e regionale, con particolare riferimento al sistema campano. Il terzo spiega come avviene concretamente la presa in carico del cittadino da parte dei centri per l'impiego. Il quarto si concentra sull'apprendimento permanente e sulle strategie per restare aggiornati in un mercato in costante evoluzione.

Non è richiesta alcuna competenza tecnica per seguire questo modulo, che consente di approfondire come funziona il mondo del lavoro oggi e di sfruttare al meglio gli strumenti che la pubblica amministrazione e il mercato digitale mettono a disposizione di tutti.

Questo capitolo è pensato per essere usato, non solo letto. Tienilo sempre a portata di mano quando devi fare una pratica ai centri per l'impiego, iscriverti a un corso, o capire a quale programma hai diritto: è uno strumento di orientamento, non soltanto un testo da studiare.

Il digitale come strumento di cittadinanza attiva

Esercitare i propri diritti nell'era digitale

La trasformazione digitale non riguarda soltanto le imprese e le tecnologie. Riguarda ogni persona che ogni giorno deve accedere a un servizio pubblico, cercare un'opportunità di lavoro, iscriversi a un corso di formazione o comprendere a quale contributo o agevolazione ha diritto. Il digitale è diventato il canale principale attraverso cui questi servizi vengono erogati, e saperlo usare è diventato tanto importante quanto saper leggere e scrivere.

Il modulo di Formazione e Servizi Digitali consente di acquisire gli strumenti per diventare cittadini più autonomi: persone che accedono con consapevolezza ai servizi digitali senza rivolgersi ad intermediari per accedere, che sanno

dove cercare le informazioni, che riconoscono le opportunità e sanno coglierle. Significa colmare quel divario digitale che, quando presente, tiene lontani non soltanto dalla tecnologia, ma dalle opportunità concrete di migliorare la propria vita professionale.

Perché questo percorso è importante per te

La domanda che spesso ci si pone quando ci si imbatte in questi temi è: è davvero utile sapere queste cose? La risposta è concreta e immediata. Conoscere le piattaforme digitali dei servizi per l'impiego significa poter verificare in autonomia a quali programmi si ha accesso, senza dover necessariamente aspettare un appuntamento allo sportello. Capire come funziona la profilazione algoritmica significa sapere perché si ricevono certe proposte e non altre, e come migliorare il proprio profilo per essere indirizzati verso le opportunità più adatte.

Saper usare i servizi di formazione digitale significa avere accesso a corsi gratuiti o a costo ridotto che possono cambiare concretamente le proprie prospettive professionali. In un contesto in cui le competenze richieste dal mercato del lavoro cambiano rapidamente, chi impara a imparare ha un vantaggio enorme rispetto a chi si ferma a ciò che già sa.

Obiettivi del modulo

Al termine di questo modulo comprenderai cosa significa Workforce Transformation e quali effetti concreti ha già prodotto sul mercato del lavoro. Saprai riconoscere il divario di competenze digitali – il cosiddetto Digital Skill Gap – e capirai la differenza tra le due principali strategie per affrontarlo: l'upskilling e il reskilling. Conoscerai, inoltre, il ruolo delle Politiche Attive del Lavoro come risposta istituzionale a queste trasformazioni.

Dal valore fisico al valore intangibile: la Workforce Transformation

Per secoli, il valore economico è stato strettamente legato a fattori fisici e tangibili: la terra, le materie prime, le fabbriche, i macchinari. Il lavoro più remunerato era quello che produceva oggetti concreti o che gestiva risorse materiali. Questo paradigma ha subito una trasformazione radicale nell'arco di pochi decenni, e la velocità di questo cambiamento non ha precedenti nella storia economica.

Oggi, l'informazione, la conoscenza e il dato sono la vera ricchezza. Le aziende che creano più valore non sono necessariamente quelle che possiedono più asset fisici, ma quelle che sanno raccogliere, analizzare e valorizzare i dati. Il lavoro intellettuale – l'analisi predittiva, la creazione di algoritmi, la gestione di grandi quantità di informazioni – è diventato il motore principale della produzione e dell'innovazione. Questo fenomeno viene indicato con il termine Workforce Transformation: la trasformazione profonda della natura del lavoro e delle competenze necessarie per svolgerlo. Non si tratta semplicemente di imparare a usare nuovi strumenti: si tratta di un cambiamento strutturale nel modo in cui il valore viene creato e nelle abilità che permettono di partecipare a questo processo di creazione.

Emblematico è il modello delle piattaforme digitali. Aziende come quelle che gestiscono i grandi marketplace online o le piattaforme di trasporto e ospitalità non possiedono i prodotti che vendono né le case che affittano né le auto con cui trasportano persone. Creano valore connettendo domanda e offerta attraverso un uso intelligente dei dati e delle tecnologie. Questo modello di business sarebbe stato impensabile senza la rivoluzione digitale, poiché richiede competenze radicalmente diverse da quelle del modello industriale tradizionale.

L'impatto sui settori tradizionali: trasformazione, non sostituzione

Un timore diffuso quando si parla di digitalizzazione è che questa porti inevitabilmente alla sparizione di interi settori lavorativi. La realtà è più complessa e, per molti aspetti, più rassicurante: la digitalizzazione non elimina i settori

tradizionali, ma li trasforma profondamente, richiedendo nuove competenze per svolgere lavori che nella sostanza continuano a esistere.

L'agricoltura ne è un esempio illuminante. Il lavoro nei campi non è scomparso, ma si è trasformato: droni che monitorano le colture dall'alto, sensori che misurano l'umidità del suolo e la salute delle piante, software che elaborano i dati meteorologici per ottimizzare i tempi di semina e raccolta. Ciò che oggi si chiama agricoltura di precisione richiede competenze digitali che un contadino di trent'anni fa non avrebbe mai immaginato di dover acquisire. La manifattura ha vissuto una trasformazione simile. La robotica avanzata, l'Internet of Things — la rete di oggetti connessi tra loro — e la manutenzione predittiva hanno cambiato la natura del lavoro in fabbrica: meno operazioni manuali ripetitive, più supervisione, programmazione e gestione di sistemi complessi. I lavoratori più richiesti non sono quelli con le braccia più forti, ma quelli con la capacità di leggere un pannello di controllo digitale e intervenire quando qualcosa non funziona.

Accanto alla trasformazione dei settori esistenti, la digitalizzazione ha generato figure professionali che semplicemente non esistevano in precedenza. Il Cloud Architect progetta infrastrutture digitali che gestiscono quantità enormi di dati. Lo Specialista di Cybersecurity protegge sistemi e informazioni dagli attacchi informatici. Il Data Scientist estrae significato e valore da grandi insiemi di dati grezzi. Il Blockchain Developer crea sistemi di registrazione decentralizzati e sicuri. Queste professioni non comparivano nei libri di orientamento al lavoro di vent'anni fa: oggi sono tra le più richieste e meglio remunerate sul mercato.

Il Digital Skill Gap: il divario che frena

Da questa trasformazione emerge il problema centrale che questo modulo intende affrontare: il Digital Skill Gap, ovvero il divario tra le competenze digitali richieste dalle imprese e quelle effettivamente disponibili sul mercato del lavoro. Non è un problema marginale né temporaneo: è una delle principali sfide economiche del nostro tempo, riconosciuta a livello europeo come una priorità strategica. Il divario si manifesta su più livelli. Da un lato, molte persone — soprattutto nelle fasce d'età più avanzate, nelle aree geografiche meno sviluppate e nelle categorie sociali meno avvantaggiate — mancano delle competenze digitali di base necessarie per accedere anche solo ai servizi pubblici più elementari.

Dall'altro, anche chi lavora in settori tecnici si trova spesso a dover aggiornare continuamente le proprie competenze per stare al passo con tecnologie che evolvono a un ritmo senza precedenti. Il Digital Skill Gap non è una colpa individuale. È il risultato di un cambiamento troppo rapido per essere gestito spontaneamente dal sistema formativo tradizionale, che ha tempi di

aggiornamento molto più lenti rispetto all'evoluzione tecnologica. La risposta a questo problema deve quindi essere sia individuale — l'impegno di ciascuno a formarsi continuamente — sia collettiva, attraverso politiche pubbliche adeguate.

Il Digital Skill Gap non riguarda soltanto i lavori tecnici. Anche chi opera in settori tradizionali come il commercio, i servizi alla persona, l'agricoltura o l'artigianato si trova sempre più spesso a dover usare strumenti digitali. Imparare a usarli non è un optional: è una condizione di sopravvivenza professionale.

Upskilling e Reskilling: le due strategie di risposta

Di fronte al Digital Skill Gap, individui e organizzazioni hanno a disposizione due strategie principali, spesso complementari tra loro.

L'upskilling — letteralmente “potenziamento delle competenze” — consiste nell'approfondire, espandere o aggiornare le abilità già possedute per migliorare le proprie prestazioni nel ruolo che si occupa attualmente. Un contabile che impara a usare un nuovo software di gestione finanziaria sta facendo upskilling. Un operaio che si forma sull'uso di un nuovo macchinario controllato digitalmente sta facendo upskilling. L'obiettivo è diventare più efficaci e più competitivi nel proprio ruolo attuale, adattandosi alle nuove richieste del contesto.

Il reskilling — letteralmente “riqualificazione” — è invece l'acquisizione di un insieme di competenze completamente nuovo, spesso orientato a un cambiamento radicale di ruolo o di settore professionale. Un addetto alla produzione manifatturiera che si forma come tecnico di manutenzione di sistemi robotici sta facendo reskilling. Una commessa di negozio fisico che si forma come gestore di un e-commerce sta facendo reskilling. Il punto di arrivo è un profilo professionale diverso da quello di partenza.

Nella pratica, le due strategie si intrecciano spesso. Un percorso che inizia con l'upskilling — imparare meglio ciò che già si sa — può aprire porte verso nuovi ambiti professionali, trasformandosi gradualmente in un percorso di reskilling. Ciò che conta è la direzione: verso una maggiore competenza, maggiore adattabilità, maggiore valore nel mercato del lavoro.

Le Politiche Attive del Lavoro: la risposta istituzionale

Le Politiche Attive del Lavoro — indicate con l'acronimo PAL — sono l'insieme degli interventi pubblici progettati per aumentare l'occupabilità dei cittadini, favorire l'incontro tra domanda e offerta di lavoro e sostenere i lavoratori nelle transizioni professionali. Si distinguono dalle politiche passive — come la

cassa integrazione o la disoccupazione – perché non si limitano a sostenere il reddito di chi ha perso il lavoro, ma mirano attivamente a reinserirlo nel mercato.

Le PAL si articolano in diverse tipologie di intervento. I servizi di orientamento professionale aiutano il cittadino a fare il punto sulla propria situazione, a identificare le competenze possedute e quelle da sviluppare, e a costruire un percorso professionale realistico.

I programmi di formazione finanziano corsi gratuiti o fortemente agevolati per colmare il Digital Skill Gap, sia per chi è disoccupato sia per chi è occupato e vuole aggiornarsi. Gli incentivi alle assunzioni riducono il costo per le aziende che assumono categorie specifiche di lavoratori – giovani, over 50, persone con disabilità, disoccupati di lunga durata – aumentando le loro probabilità di reinserimento.

Un aspetto cruciale delle PAL nell'era digitale è che la maggior parte dei servizi che le riguardano – dalla registrazione all'accesso ai bandi, dalla candidatura ai corsi di formazione alla consultazione delle offerte di lavoro – avviene ormai esclusivamente o prevalentemente attraverso canali digitali. Questo rende la competenza digitale non soltanto una delle competenze che le PAL cercano di sviluppare, ma anche la condizione necessaria per accedervi.

Da ricordare: Senza una minima competenza digitale, è sempre più difficile accedere anche solo ai servizi che dovrebbero aiutarti a sviluppare competenze digitali. Per questo il modulo che stai seguendo è il primo e più importante passo.

LE PIATTAFORME ISTITUZIONALI: ORIENTARSI TRA I PORTALI

Obiettivi del modulo

Al termine di questo modulo saprai orientarti tra i principali portali istituzionali dedicati al lavoro e alla formazione, con particolare attenzione al sistema campano. Conoscerai il SILF Campania e la sua funzione di collegamento tra i servizi nazionali e il territorio. Saprai cos'è la Scheda Anagrafica Professionale e perché tenerla aggiornata è fondamentale. Avrai una comprensione chiara del programma Garanzia Giovani e a chi si rivolge.

Il Ministero del Lavoro e ClicLavoro

Il punto di riferimento nazionale per le politiche del lavoro è il Ministero del Lavoro e delle Politiche Sociali. Il suo sito istituzionale raccoglie informazioni su normative, programmi, bandi e opportunità di formazione a livello nazionale. È il punto di partenza per chiunque voglia capire il quadro generale dei servizi pubblici per il lavoro.

ClicLavoro è il portale nazionale sviluppato dal Ministero del Lavoro come punto di incontro tra domanda e offerta di lavoro. Permette ai cittadini di consultare le offerte di lavoro disponibili sul territorio, di caricare il proprio curriculum vitae rendendolo visibile alle aziende registrate, e di accedere a informazioni sui programmi di formazione e le opportunità finanziate. A livello regionale, la Regione Campania gestisce una versione del portale specificamente orientata alle opportunità presenti sul territorio campano.

Il SILF Campania: l'interfaccia unica regionale

A livello regionale, il sistema centrale attraverso cui si accede a tutti i servizi relativi al lavoro e alla formazione in Campania è il SILF – Sistema Informativo Lavoro e Formazione. Si tratta della piattaforma digitale gestita dalla Regione Campania che funge da collegamento tra i servizi nazionali e la rete territoriale dei Centri per l'Impiego.

Comprendere il SILF è fondamentale perché qualsiasi interazione formale con il Centro per l'Impiego – dall'iscrizione alla registrazione dello stato di disoccupazione, dalla candidatura a un programma di formazione alla consultazione delle offerte – avviene oggi prevalentemente attraverso questa piattaforma. Non si tratta di uno strumento accessorio: è il passaggio obbligato per chi vuole accedere ai servizi di supporto all'occupazione sul territorio campano. Per accedere al SILF è necessario disporre delle credenziali digitali riconosciute dalla pubblica amministrazione italiana: lo SPID (Sistema Pubblico di Identità Digitale), la CIE (Carta d'Identità Elettronica) o la CNS (Carta Nazionale dei Servizi). Queste credenziali non servono soltanto per il SILF: sono oggi il passaporto digitale per accedere alla quasi totalità dei servizi pubblici online,

dall'Agenzia delle Entrate all'INPS, dai Comuni ai servizi sanitari regionali.

Se non hai ancora attivato la tua identità digitale tramite Carta d'Identità Elettronica, questo può essere il momento giusto. È gratuita, basta scaricare l'app CIE ID sul proprio smartphone, attivare le credenziali e, in questo modo, accedere alla quasi totalità dei servizi pubblici digitali, incluso il SILF Campania.

La Scheda Anagrafica Professionale: il tuo profilo ufficiale

La Scheda Anagrafica Professionale – SAP – è il documento ufficiale che viene creato nel momento in cui un cittadino si iscrive ai servizi per l'impiego. Non è un semplice curriculum vitae: è un registro standardizzato e ufficiale che contiene l'intera storia professionale e formativa della persona, comprensiva di dati anagrafici, titoli di studio, qualifiche riconosciute, esperienze lavorative certificate e competenze professionali acquisite. La differenza rispetto a un curriculum vitae tradizionale è sostanziale. Mentre il curriculum è un documento soggettivo che ciascuno scrive e presenta secondo la propria valutazione, la SAP è un documento istituzionale che segue una struttura standardizzata e che viene aggiornato nel corso del tempo a mano a mano che si accumulano nuove esperienze e qualifiche.

È, in un certo senso, la versione ufficiale del proprio percorso professionale agli occhi della pubblica amministrazione. La SAP svolge un ruolo cruciale nel processo di matching algoritmico: il sistema informatico la utilizza per incrociare il profilo del cittadino con le offerte di lavoro disponibili, i corsi di formazione attivi e i bandi delle Politiche Attive del Lavoro a cui si ha diritto. Una SAP incompleta, non aggiornata o compilata in modo superficiale produce abbinamenti di scarsa qualità: il sistema non riesce a identificare le opportunità più adatte perché non ha le informazioni necessarie per farlo. Tenerla aggiornata non è un adempimento burocratico: è un investimento diretto sulla propria occupabilità.

Consiglio pratico: Ogni volta che completi un corso, ottieni una certificazione o cambi posizione lavorativa, aggiorna la tua Scheda Anagrafica Professionale sul SILF. Un profilo aggiornato aumenta le probabilità di essere abbinato alle opportunità più pertinenti.

Garanzia Giovani: il programma europeo per i NEET

Garanzia Giovani è uno dei programmi più importanti tra quelli gestiti attraverso le piattaforme regionali come il SILF. Si tratta di un'iniziativa europea nata per rispondere a uno dei problemi sociali più gravi degli ultimi decenni: la quota elevata di giovani che non studiano, non lavorano e non seguono alcun percorso formativo, indicati con l'acronimo NEET (Not in Education, Employ-

ment, or Training). Il programma si rivolge a giovani tra i 15 e i 35 anni che si trovano in questa condizione e si impegna a garantire loro, entro un periodo definito dalla presa in carico, un'offerta concreta: un lavoro, un tirocinio, un apprendistato, un percorso di formazione o un'esperienza di servizio civile. Non si tratta di una promessa generica: è un impegno strutturato, che prevede la profilazione della persona, la costruzione di un percorso personalizzato e il monitoraggio dei risultati.

In Campania, l'accesso a Garanzia Giovani avviene attraverso il SILF: è lì che si effettua l'iscrizione, la profilazione e la gestione di tutte le tappe del percorso. Conoscere questa piattaforma non è quindi soltanto utile per chi ha già un'esperienza lavorativa e cerca di aggiornarsi: è essenziale anche per i giovani che si affacciano per la prima volta al mercato del lavoro e vogliono sfruttare le opportunità che il sistema pubblico mette a loro disposizione.

COME I SERVIZI PER L'IMPIEGO TI PRENDONO IN CARICO

Obiettivi del modulo

Al termine di questo modulo saprai cos'è la Dichiarazione di Immediata Disponibilità, come rilasciarla e perché è il punto di partenza imprescindibile per accedere ai servizi pubblici per il lavoro. Comprenderai il meccanismo della profilazione quantitativa e il significato delle classi di occupabilità. Conoscerai il Patto di Servizio Personalizzato e il ruolo che svolge nel definire il percorso di supporto.

La Dichiarazione di Immediata Disponibilità: il primo passo ufficiale

Cercare lavoro è un'attività che chiunque può svolgere in modo autonomo: inviare curriculum vitae, rispondere ad annunci, contattare aziende. Ma per accedere ai servizi pubblici dedicati all'occupazione – i programmi di formazione finanziati, il supporto del Centro per l'Impiego, gli ammortizzatori sociali – è necessario compiere un atto formale che attiva ufficialmente la propria posizione di persona in cerca di lavoro. Questo atto si chiama Dichiarazione di Immediata Disponibilità, indicata con l'acronimo DID.

La DID è la dichiarazione con cui un cittadino comunica al sistema pubblico di essere immediatamente disponibile a svolgere un'attività lavorativa. Non è un semplice gesto simbolico: ha una precisa natura giuridica. È la condizione preliminare e necessaria per acquisire ufficialmente lo stato di disoccupazione – con tutto ciò che ne deriva in termini di diritti e accesso ai servizi – e per entrare nel sistema delle Politiche Attive del Lavoro.

Fino a non molti anni fa, la DID si rilasciava recandosi fisicamente allo sportello del Centro per l'Impiego. Oggi questa procedura è stata digitalizzata: la DID si rilascia esclusivamente in modalità telematica, attraverso i portali regionali interconnessi come il SILF Campania, accedendo con le credenziali digitali (SPID, CIE o CNS). Questa digitalizzazione ha reso la procedura più rapida e accessibile da qualsiasi luogo, ma ha anche introdotto una barriera per chi non dispone delle competenze digitali o delle credenziali necessarie.

I requisiti per rilasciare la DID sono semplici: avere compiuto sedici anni, non essere più soggetto all'obbligo scolastico e non essere attualmente occupato. Il rilascio telematico avvia immediatamente la Scheda Anagrafica Professionale, segnando ufficialmente l'inizio del percorso con il Centro per l'Impiego.

La DID non è un documento che si fa “per avere la disoccupazione”. È il modo in cui comunichi al sistema pubblico che: sei disponibile a lavorare, hai bisogno di supporto, vuoi accedere alle opportunità che la legge ti garantisce. È un diritto, non una concessione.

La profilazione quantitativa: come il sistema ti valuta

Una volta rilasciata la DID, il sistema attiva automaticamente un meccanismo fondamentale per il funzionamento delle Politiche Attive del Lavoro: la profilazione quantitativa. Si tratta di un processo algoritmico attraverso cui il Centro per l'Impiego valuta il cittadino sulla base di dati oggettivi per stimare il suo grado di occupabilità, ovvero la probabilità che riesca a trovare lavoro in modo autonomo in un arco di tempo ragionevole.

È importante comprendere lo scopo della profilazione per non interpretarla come un giudizio o una classificazione di valore. L'obiettivo non è stabilire chi è un buon lavoratore e chi non lo è: è allocare le risorse di supporto in modo efficiente, assicurando che chi ha più bisogno di aiuto riceva un supporto più intenso, e che chi è già in una posizione favorevole non occupi risorse che potrebbero essere destinate a chi ne ha maggiore necessità.

I parametri che il sistema considera nella profilazione sono principalmente tre. Il primo è la storia lavorativa: la durata dei periodi di disoccupazione precedenti, la continuità dei contratti, la tipologia e il settore delle esperienze maturate. Il secondo è l'anagrafica: l'età, il genere, la residenza geografica – fattori che influenzano statisticamente le probabilità di reinserimento nel mercato del lavoro locale. Il terzo è il livello di istruzione e formazione: la rilevanza dei titoli posseduti rispetto alla domanda del mercato locale e la presenza di certificazioni aggiornate.

Le classi di occupabilità: cosa significano

Sulla base del punteggio assegnato dalla profilazione, il cittadino viene inserito in una classe di occupabilità che determina l'intensità del supporto che riceverà. Il sistema prevede tipicamente quattro classi, che vanno da un rischio basso a un rischio alto di disoccupazione prolungata.

Chi rientra nella Classe 1 – rischio basso – è un profilo che, sulla base dei dati storici e del proprio profilo professionale, ha un'alta probabilità di trovare lavoro in tempi relativamente brevi. Si tratta tipicamente di persone giovani, con competenze aggiornate, esperienze lavorative recenti e titoli di studio coerenti con le richieste del mercato locale. Il supporto che riceverà sarà più leggero: principalmente servizi di matching e orientamento di base.

Le Classi 2 e 3 rappresentano situazioni di rischio medio: persone che potrebbero incontrare difficoltà nel reinserimento ma che hanno comunque buone possibilità di farlo con un supporto mirato. Il percorso previsto include coaching professionale, orientamento al lavoro e possibilmente un accompagnamento nella ricerca attiva.

Chi rientra nella Classe 4 – rischio alto – è un profilo che presenta caratteristiche associate statisticamente a una maggiore difficoltà di reinserimento: lunghi periodi di disoccupazione, competenze obsolete rispetto alle richieste del mercato, titoli di studio scarsamente valorizzati nel contesto locale, o condizioni anagrafiche e geografiche sfavorevoli. Paradossalmente, essere classificati in questa categoria non è necessariamente uno svantaggio: significa ricevere il massimo livello di supporto disponibile, con percorsi intensivi di reskilling, alta frequenza di contatti con il CPI e un monitoraggio costante del percorso.

Da sapere: La classe di occupabilità non è permanente. Cambia ogni volta che si aggiorna la propria Scheda Anagrafica Professionale, si completa un percorso formativo o si acquisisce una nuova esperienza lavorativa. Investire nella propria formazione migliora concretamente il proprio profilo algoritmico.

Il Patto di Servizio Personalizzato: un accordo su misura

Il Patto di Servizio Personalizzato – PSP – è il documento che formalizza il rapporto tra il cittadino e il Centro per l'Impiego. Si tratta di un accordo vero e proprio: non un modulo da firmare per obbligo burocratico, ma un piano condiviso che definisce gli obiettivi da raggiungere, le azioni che il cittadino si impegna a compiere e i servizi che il CPI si impegna a erogare.

Il contenuto del PSP è direttamente influenzato dalla classe di occupabilità assegnata. Chi è classificato a basso rischio avrà un PSP più flessibile, con obiettivi meno vincolanti e meno obblighi formali. Chi è classificato ad alto rischio – Classe 4 – avrà un PSP più strutturato e impegnativo: obblighi di partecipazione a percorsi formativi, convocazioni periodiche più frequenti, requisiti più stringenti riguardo all'accettazione di offerte di lavoro o formazione adeguate al proprio profilo.

Rispettare gli impegni del PSP non è soltanto un obbligo formale: è la condizione per mantenere l'accesso ai benefici e ai servizi a cui si ha diritto. Chi non rispetta gli impegni previsti dal patto rischia di perdere lo stato di disoccupazione e, di conseguenza, l'accesso alle Politiche Attive del Lavoro e agli eventuali ammortizzatori sociali collegati.

LIFELONG LEARNING: IMPARARE PER TUTTA LA VITA

Obiettivi del modulo

Al termine di questo modulo avrai compreso il significato e il valore del Lifelong Learning come strategia professionale in un mercato del lavoro in continua evoluzione. Saprai identificare i tuoi Skill Gap e scegliere le fonti di formazione digitale più affidabili e appropriate. Conoscerai i principali strumenti e programmi disponibili per la formazione continua, con particolare attenzione alle opportunità gratuite o finanziate.

Il Lifelong Learning: imparare non finisce mai

L'idea che l'apprendimento si concentri nella prima fase della vita — scuola, formazione professionale, università — e che poi si passi a mettere in pratica ciò che si è imparato è sempre meno corrispondente alla realtà del mercato del lavoro contemporaneo. Le competenze richieste cambiano troppo rapidamente perché ciò che si impara a vent'anni basti a garantire una carriera stabile fino alla pensione.

Il Lifelong Learning — letteralmente “apprendimento per tutta la vita” — non è un semplice aggiornamento sporadico. È un approccio proattivo e sistematico all'acquisizione di conoscenze e competenze, che dura per l'intero arco della vita professionale. È l'impegno a non smettere mai di imparare, non perché sia piacevole in sé — anche se spesso lo è — ma perché è l'unica strategia efficace per restare competitivi in un contesto in cui la stabilità non è più garantita da ciò che si sa fare oggi, ma dalla capacità di imparare ciò che sarà richiesto domani.

Un concetto correlato è quello di “carriera liquida”: in opposizione alle carriere rigide e lineari del passato — un solo datore di lavoro, un solo ruolo, per tutta la vita — la carriera contemporanea è fluida, discontinua, fatta di transizioni, riposizionamenti e cambiamenti di direzione. In questo contesto, le persone che meglio riescono ad adattarsi sono quelle che hanno sviluppato la capacità di imparare velocemente, di trasferire le competenze da un contesto all'altro e di non lasciarsi paralizzare dall'incertezza.

Identificare il proprio Skill Gap

Prima di scegliere un percorso formativo, è utile fare un'analisi onesta della propria situazione. Identificare i propri Skill Gap — le competenze che si vorrebbero avere e che attualmente non si possiedono, o che si posseggono in misura insufficiente — è il punto di partenza per costruire un piano di sviluppo professionale efficace.

Il processo di autovalutazione può seguire alcuni passi semplici. Il primo è de-

finire un obiettivo: qual è il ruolo professionale che si vuole ricoprire, o in quale direzione si vuole far evolvere la propria carriera? Essere specifici aiuta: non “voglio lavorare nel digitale”, ma “voglio fare il gestore di un e-commerce” o “voglio diventare assistente alla comunicazione di un ente pubblico”.

Il secondo passo è mappare le competenze richieste per quel ruolo. Le offerte di lavoro sono una fonte preziosa: leggerne dieci o venti per lo stesso tipo di posizione permette di identificare le hard skills tecniche che vengono sistematicamente richieste. Il terzo passo è valutare onestamente il proprio livello attuale in ciascuna di quelle competenze. La differenza tra ciò che si sa fare e ciò che viene richiesto è il Gap da colmare.

Accanto alle hard skills tecniche, è importante non dimenticare le soft skills – le competenze trasversali come il problem solving, la resilienza, la capacità di comunicare efficacemente, il saper lavorare in team e l’adattabilità. Queste competenze sono particolarmente preziose perché sono trasferibili: una volta sviluppate, rimangono utili indipendentemente da quale strumento tecnico si stia usando o da quale settore si stia operando.

Le fonti digitali per la formazione: come scegliere

Non tutte le fonti di formazione digitale hanno lo stesso valore. Orientarsi tra la vastità dell’offerta disponibile online richiede criteri di selezione chiari, che permettano di distinguere ciò che è davvero utile da ciò che è soltanto apparentemente conveniente.

Il primo criterio è il riconoscimento: la certificazione che si ottiene al termine del corso è riconosciuta nel settore in cui si vuole lavorare, o è soltanto un attestato di partecipazione? Una certificazione rilasciata da un’azienda tecnologica leader del settore – come Google, Microsoft o Amazon per il cloud computing – ha un peso molto diverso rispetto a un attestato emesso da un sito sconosciuto. Prima di investire tempo e denaro, vale sempre la pena verificare il valore reale della certificazione sul mercato.

Il secondo criterio è la rilevanza: il contenuto del corso è aggiornato e risponde esattamente al Gap che si vuole colmare? I campi tecnologici evolvono rapidamente: un corso su un software specifico che non è stato aggiornato negli ultimi due anni potrebbe insegnare procedure già obsolete. Verificare la data dell’ultima revisione del materiale didattico è un accorgimento semplice ma importante.

Il terzo criterio è il costo e l’accessibilità. Esistono opportunità formative di alta qualità completamente gratuite, finanziate da programmi pubblici o da grandi aziende tecnologiche che hanno interesse a diffondere le proprie com-

petenze. Prima di pagare per un corso, vale sempre la pena verificare se esiste un'alternativa gratuita o finanziata di qualità comparabile.

Le principali tipologie di risorse formative

Il panorama delle risorse formative digitali si articola in alcune grandi categorie, ognuna con caratteristiche e vantaggi specifici.

I programmi istituzionali e finanziati sono il punto di partenza più conveniente per chi cerca formazione senza sostenere costi elevati. Il Programma GOL – Garanzia di Occupabilità dei Lavoratori – è il principale programma nazionale che finanzia percorsi formativi per lavoratori occupati a rischio, disoccupati e persone in cerca di prima occupazione. In Campania, l'accesso avviene attraverso il SILF. Questi programmi offrono corsi gratuiti, spesso erogati da enti di formazione accreditati, con un'attenzione particolare alle competenze digitali.

Le certificazioni aziendali sono corsi e percorsi formativi offerti direttamente da grandi aziende tecnologiche, spesso gratuitamente o a costo molto ridotto. Google Digital Training, ad esempio, offre una serie di corsi gratuiti sulle competenze digitali di base – dal marketing online alla gestione dei dati – che rilasciano certificazioni riconosciute a livello internazionale. Microsoft, Amazon Web Services, Cisco e molte altre aziende hanno programmi simili. Si tratta di risorse di alta qualità, riconosciute dai datori di lavoro e accessibili a chiunque abbia una connessione internet.

I MOOC – Massive Open Online Courses – sono corsi online aperti e accessibili a un numero potenzialmente illimitato di partecipanti, erogati da università e istituzioni accademiche di tutto il mondo attraverso piattaforme dedicate. Coursera, edX, FutureLearn e Udemy sono alcune delle piattaforme più note. Molti di questi corsi sono gratuiti nella modalità di sola fruizione dei contenuti, mentre richiedono un pagamento soltanto per ottenere il certificato ufficiale. Offrono un livello di approfondimento spesso paragonabile a quello di un corso universitario, con la flessibilità di seguire i contenuti nel momento e nei tempi più convenienti.

Consiglio: Se non sai da dove iniziare, Google Digital Training è una delle risorse più accessibili e riconosciute disponibili in italiano. È gratuito, non richiede conoscenze pregresse e offre un percorso guidato che parte dalle basi del digitale per arrivare a competenze concrete e spendibili nel mercato del lavoro.

Un servizio spesso sconosciuto, ma prezioso

Il Centro per l'Impiego – CPI – è uno dei servizi pubblici più importanti per chi cerca lavoro o vuole riqualificarsi professionalmente, eppure è anche uno dei meno conosciuti e utilizzati. Molti cittadini non sanno cosa offre, come funziona e a chi si rivolge. Questa sezione vuole colmare questa lacuna, spiegando in modo chiaro cosa ci si può aspettare da un CPI e come sfruttarne al meglio le risorse.

I Centri per l'Impiego sono strutture pubbliche distribuite sul territorio, di competenza delle Regioni e delle Province autonome. In Campania operano su tutto il territorio regionale e gestiscono, attraverso il SILF, l'erogazione dei servizi legati alle Politiche Attive del Lavoro. Non sono uffici di collocamento nel senso tradizionale del termine – non “trovano” lavoro per i cittadini – ma offrono un insieme di servizi che aumentano concretamente le probabilità di trovarlo.

I servizi offerti dal CPI

L'accoglienza e l'orientamento di primo livello è il servizio base che chiunque può richiedere. Un operatore del CPI ascolta la situazione della persona, spiega i servizi disponibili, aiuta a compilare la Scheda Anagrafica Professionale e fornisce le prime indicazioni sul percorso più adatto. È il punto di ingresso per chi non sa da dove iniziare.

Il bilancio di competenze è un servizio più approfondito, che prevede uno o più incontri con un orientatore professionale qualificato. L'obiettivo è aiutare la persona a fare il punto sulla propria storia formativa e professionale, a identificare le competenze acquisite – anche quelle che non si considerano tali, come le capacità sviluppate in un ruolo di caregiver familiare o in attività di volontariato – e a definire un progetto professionale realistico e coerente con il contesto del mercato locale.

L'accompagnamento alla ricerca attiva del lavoro include servizi pratici di supporto: aiuto nella stesura del curriculum vitae, preparazione ai colloqui di lavoro, orientamento all'uso delle piattaforme digitali per la ricerca di offerte, e in alcuni casi anche la segnalazione diretta alle aziende che collaborano con il CPI. Non è una garanzia di occupazione, ma è un supporto concreto nel processo.

La formazione finanziata è forse il servizio più direttamente utile in chiave di upskilling e reskilling. Attraverso il CPI è possibile accedere ai corsi gratuiti finanziati con fondi pubblici – nazionali ed europei – che coprono una vasta

gamma di ambiti: dalle competenze digitali di base alla gestione aziendale, dalla logistica all'assistenza alle persone, dalle lingue straniere alle certificazioni informatiche riconosciute a livello internazionale.

Come prepararsi al meglio a un appuntamento al CPI

Presentarsi al CPI senza preparazione è un'occasione parzialmente sprecata. Chi si presenta con le idee chiare – sa cosa sta cercando, ha già una bozza del proprio curriculum, conosce le proprie competenze e i propri obiettivi – ottiene risultati molto migliori rispetto a chi si affida completamente all'operatore per capire la propria situazione.

Prima di un appuntamento al CPI è utile aver già attivato lo SPID, aver compilato una prima versione della propria Scheda Anagrafica Professionale sul SILF, aver raccolto i documenti relativi alle proprie esperienze lavorative e formative – contratti, diplomi, attestati di corsi – e aver riflettuto su qual è la direzione professionale che si vuole perseguire. Non è necessario avere certezze assolute: è sufficiente avere un'idea di massima e la disponibilità a ragionarci insieme con un operatore qualificato.

Consiglio: Porta con te tutta la documentazione disponibile: diploma, attestati di corsi, contratti di lavoro precedenti, lettere di referenza. Più informazioni concrete hai, più accurata sarà la tua SAP e migliori saranno i risultati del matching.

Navigare sicuri: attenzione alle truffe nel digitale del lavoro

Un rischio reale, da non sottovalutare

L'accesso ai servizi per il lavoro attraverso canali digitali porta con sé un rischio che non può essere ignorato: le truffe online. Il mondo del lavoro digitale è purtroppo terreno fertile per chi tenta di approfittarsi delle persone in cerca di occupazione, spesso proprio perché si trovano in una situazione di vulnerabilità emotiva ed economica.

Conoscere le forme più comuni di truffa nel settore del lavoro online non significa diventare diffidenti verso tutto, ma sviluppare un senso critico che permette di distinguere le opportunità reali da quelle false. È una competenza che rientra direttamente nell'area della sicurezza digitale del quadro DigComp e che vale la pena acquisire prima di iniziare a usare le piattaforme online.

Le forme più comuni di truffa lavorativa online

L'offerta di lavoro troppo bella per essere vera è la forma più classica. Annunci che promettono stipendi molto alti per lavori che sembrano richiedere poche

competenze, orari ridottissimi e nessuna esperienza richiesta sono quasi sempre fraudolenti. Il principio generale è semplice: se un'offerta sembra troppo vantaggiosa rispetto al mercato reale, è quasi certamente falsa.

La richiesta di pagamento anticipato è un segnale di allarme inequivocabile. Nessun datore di lavoro legittimo chiede a un candidato di pagare per essere assunto: né per l'accesso a una formazione obbligatoria, né per materiali di lavoro, né per la verifica delle credenziali, né per qualsiasi altra ragione. Se qualcuno chiede soldi in cambio di un'opportunità di lavoro, si tratta quasi certamente di una truffa.

Il furto di identità attraverso finti colloqui è una forma più sofisticata di frode. I truffatori contattano persone in cerca di lavoro, simulano un processo di selezione credibile e, nel corso del processo, richiedono documenti personali – copia del documento di identità, del codice fiscale, del conto corrente – sostenendo che servano per le pratiche di assunzione. Questi dati vengono poi usati per aprire conti correnti fraudolenti, richiedere prestiti o commettere altri reati.

I siti che imitano portali istituzionali sono un'altra minaccia. Possono esistere siti web che imitano graficamente il SILF Campania, ClicLavoro o altri portali ufficiali, con URL leggermente diversi dall'originale. Prima di inserire le proprie credenziali su qualsiasi sito, è fondamentale verificare che l'indirizzo web corrisponda esattamente a quello del portale ufficiale.

Come proteggersi

La regola d'oro è verificare sempre l'identità di chi contatta. Un'azienda seria ha un sito web verificabile, un indirizzo fisico, una partita IVA consultabile nei registri pubblici. Prima di candidarsi a un'offerta di lavoro trovata online, vale sempre la pena dedicare cinque minuti a verificare l'esistenza e la credibilità dell'azienda.

Non condividere mai dati sensibili – numero di conto corrente, copia di documenti di identità, codice fiscale, numero di carta di credito – prima di aver verificato con certezza l'identità del destinatario e la legittimità della richiesta. In caso di dubbio, è sempre meglio chiedere chiarimenti o consultare un operatore del CPI.

Se si sospetta di essere vittime di una truffa, è importante segnalarlo alle autorità competenti – la Polizia Postale è l'organismo preposto in Italia alla gestione dei reati informatici – e alle piattaforme dove l'annuncio fraudolento è stato pubblicato. Segnalare non solo protegge sé stessi, ma contribuisce a proteggere altri potenziali vittime.

Il portale della Polizia Postale (www.commissariatodips.it) permette di segnalare truffe online e consultare una lista aggiornata di tipologie di frodi conosciute. È una risorsa utile da tenere a portata di mano.

Riepilogo dei concetti fondamentali

Questo capitolo ha affrontato quattro grandi temi, ognuno dei quali contribuisce a costruire una comprensione più completa del rapporto tra digitale, lavoro e formazione.

La Workforce Transformation ha cambiato profondamente la natura del lavoro: il valore economico si è spostato dal fisico all'intangibile, nuove professioni sono nate e quelle tradizionali si sono trasformate. Chi non si adatta rischia di trovarsi escluso da un mercato del lavoro che cambia più velocemente di quanto i sistemi formativi tradizionali riescano a stare al passo.

Il Digital Skill Gap è la conseguenza più visibile di questa trasformazione: la distanza tra le competenze digitali che le imprese richiedono e quelle che i lavoratori possiedono. Non è una colpa individuale, ma è un problema individuale da affrontare: attraverso l'upskilling, potenziando ciò che già si sa fare, e attraverso il reskilling, acquisendo competenze nuove per ruoli diversi.

Le piattaforme istituzionali – il SILF Campania, ClicLavoro, i portali delle PAL – sono gli strumenti attraverso cui lo Stato mette a disposizione dei cittadini supporto concreto nella ricerca di lavoro e nella formazione. Ma questi strumenti funzionano soltanto se vengono utilizzati: richiedono di avere le credenziali digitali, di compilare accuratamente la propria Scheda Anagrafica Professionale, di rilasciare la DID e di onorare il Patto di Servizio Personalizzato.

Il Lifelong Learning è l'unica risposta sostenibile alla velocità del cambiamento. Non basta imparare una volta e fermarsi: in un mercato del lavoro liquido e in continua evoluzione, la capacità di imparare continuamente è la competenza più preziosa che si possa possedere. Le risorse per farlo – spesso gratuite o finanziate – sono più accessibili che mai: MOOC, certificazioni aziendali, programmi istituzionali. La difficoltà non è trovarle: è sviluppare l'abitudine a usarle.

Il percorso che hai appena concluso è esso stesso un atto di Lifelong Learning. Ogni conoscenza acquisita qui è una competenza che puoi spendere da domani: per navigare con maggiore sicurezza tra i portali istituzionali, per capire come funziona il sistema dei servizi per l'impiego, per scegliere il percorso formativo più adatto a te.

Scheda di autovalutazione DigComp

Al termine del capitolo, rifletti su ciò che hai imparato compilando questa scheda. Per ciascuna area indica il tuo livello su una scala da 1 a 5: 1 = non mi sento ancora in grado, 5 = mi sento completamente autonomo.

Area di Competenza	Prima del corso	Dopo il corso
Comprendo cosa significa Workforce Transformation e Digital Skill Gap		
So distinguere upskilling e reskilling e applicarli al mio percorso		
Conosco le principali piattaforme istituzionali per lavoro e formazione		
So come rilasciare la DID e cosa significa la profilazione		
Conosco almeno una fonte digitale gratuita per la mia formazione continua		

Glossario essenziale

CIE (Carta d'Identità Elettronica): documento di identità in formato digitale che permette di accedere ai servizi online della pubblica amministrazione, in alternativa allo SPID.

ClicLavoro: portale nazionale del Ministero del Lavoro per l'incontro tra domanda e offerta di lavoro. Disponibile anche in versione regionale per la Campania.

DID (Dichiarazione di Immediata Disponibilità): atto formale e telematico con cui un cittadino dichiara di essere immediatamente disponibile a lavorare. È la condizione necessaria per acquisire lo stato di disoccupazione e accedere alle Politiche Attive del Lavoro.

Digital Skill Gap: divario tra le competenze digitali richieste dal mercato del

lavoro e quelle effettivamente possedute dai lavoratori. Rappresenta una delle principali sfide del mercato del lavoro contemporaneo.

Garanzia Giovani: programma europeo che garantisce ai giovani NEET tra i 15 e i 35 anni un'offerta concreta di lavoro, formazione, tirocinio o apprendistato entro un periodo definito dalla presa in carico.

Lifelong Learning: apprendimento continuo e permanente. La strategia di formarsi costantemente per tutto l'arco della vita professionale, adattandosi ai cambiamenti del mercato del lavoro.

MOOC (Massive Open Online Courses): corsi online aperti, spesso gratuiti, erogati da università e istituzioni su piattaforme come Coursera, edX e FutureLearn. Offrono formazione di livello accademico con grande flessibilità.

NEET (Not in Education, Employment, or Training): giovani che non studiano, non lavorano e non seguono alcun percorso formativo. Il programma Garanzia Giovani è specificamente rivolto a questa categoria.

PAL (Politiche Attive del Lavoro): insieme degli interventi pubblici — formazione, orientamento, incentivi — finalizzati ad aumentare l'occupabilità dei cittadini e favorire il loro reinserimento nel mercato del lavoro.

Programma GOL (Garanzia di Occupabilità dei Lavoratori): programma nazionale che finanzia percorsi formativi per lavoratori occupati a rischio, disoccupati e persone in cerca di prima occupazione, con particolare attenzione alle competenze digitali.

PSP (Patto di Servizio Personalizzato): accordo formale tra il cittadino e il Centro per l'Impiego che definisce obiettivi, obblighi e servizi nel percorso di reinserimento lavorativo. Il suo contenuto dipende dalla classe di occupabilità assegnata.

Reskilling: acquisizione di un set di competenze completamente nuovo per cambiare ruolo o settore professionale. Si distingue dall'upskilling perché implica un cambiamento più radicale del profilo professionale.

SAP (Scheda Anagrafica Professionale): documento ufficiale e standardizzato che registra la storia professionale e formativa del cittadino iscritto ai servizi per l'impiego. Viene usata dal sistema per il matching algoritmico con le opportunità disponibili.

SILF Campania (Sistema Informativo Lavoro e Formazione): piattaforma digitale regionale che gestisce tutti i servizi relativi al lavoro e alla formazione in Campania. È il punto di accesso obbligato per i servizi dei Centri per l'Impiego

e per i programmi PAL sul territorio campano.

SPID (Sistema Pubblico di Identità Digitale): sistema di autenticazione che permette di accedere ai servizi online della pubblica amministrazione con un'unica identità digitale. È gratuito e indispensabile per accedere al SILF e alla maggior parte dei portali istituzionali.

Upskilling: potenziamento o aggiornamento delle competenze già possedute per migliorare le proprie prestazioni nel ruolo attuale. Si distingue dal reskilling perché non implica un cambio di ruolo ma un approfondimento del profilo esistente.

Workforce Transformation: trasformazione profonda della natura del lavoro e delle competenze richieste, guidata dalla digitalizzazione. Comporta la nascita di nuove professioni, la trasformazione di quelle esistenti e l'obsolescenza di alcune figure lavorative tradizionali.

TEMA A
LAVORO E SVILUPPO PRODUTTIVO
RICERCA DEL LAVORO



Digita Facile
Campania

A chi è rivolto questo capitolo

Questo capitolo accompagna il percorso formativo dedicato alla Ricerca del Lavoro, sviluppato nell'ambito del progetto Digita Facile Campania. Si rivolge a chi vuole orientarsi nel mercato del lavoro locale e nazionale con maggiore consapevolezza, sfruttando al meglio gli strumenti digitali disponibili: dalle piattaforme per la ricerca di offerte alla costruzione di un profilo professionale efficace, dalle tecniche per affrontare un colloquio alla pianificazione di un percorso di crescita professionale a lungo termine.

Il percorso è articolato in sei moduli. Il primo offre una panoramica delle tendenze attuali del mercato del lavoro, con attenzione alle opportunità specifiche del territorio campano. Il secondo approfondisce le tecniche per scrivere un curriculum vitae e una lettera di presentazione efficaci. Il terzo si concentra sulla simulazione dei colloqui e sulle tecniche di networking. Il quarto esplora le piattaforme online per la ricerca di lavoro e la costruzione del profilo professionale digitale. Il quinto affronta lo sviluppo delle competenze trasversali – le soft skills – sempre più valorizzate dal mercato. Il sesto, infine, guida nella costruzione di un piano d'azione personalizzato per la propria carriera.

Ogni percorso è scritto in un linguaggio accessibile, con esempi concreti, consigli pratici e spunti di riflessione. Non è necessario avere competenze digitali avanzate per beneficiarne: basta la curiosità di capire come funziona il mercato del lavoro oggi e la voglia di affrontarlo con gli strumenti giusti.

Questo capitolo non è solo un testo da leggere: è uno strumento da usare. Puoi tornarci ogni volta che devi scrivere un CV, prepararti a un colloquio, aggiornare il tuo profilo LinkedIn o costruire il tuo piano professionale. Tienila a portata di mano.

Il digitale come chiave per il mercato del lavoro

Diventare cittadini digitali autonomi

Partecipare attivamente al mercato del lavoro nell'era digitale non significa soltanto saper usare un computer o uno smartphone. Significa saper navigare tra le piattaforme dove si trovano le offerte di lavoro, costruire una presenza professionale online credibile, comunicare efficacemente in ambienti digitali e sfruttare gli strumenti che la tecnologia mette a disposizione per presentarsi al meglio ai potenziali datori di lavoro.

Il divario digitale – la distanza tra chi sa usare questi strumenti e chi non li conosce – si traduce direttamente in un divario di opportunità. Chi non sa come funziona LinkedIn o come ottimizzare il proprio curriculum per i sistemi

di selezione automatica rischia di essere invisibile a una fetta crescente del mercato del lavoro, anche se ha le competenze giuste per il ruolo che cerca. Colmare questo divario è esattamente l'obiettivo di questo percorso.

I vantaggi concreti del digitale nella ricerca del lavoro

L'uso consapevole degli strumenti digitali nella ricerca del lavoro offre vantaggi concreti e misurabili. Il primo è il risparmio di tempo: invece di girare di azienda in azienda con il curriculum in mano, oggi è possibile candidarsi a decine di posizioni in pochi minuti, direttamente da casa. Il secondo è la visibilità: un profilo LinkedIn ben curato può essere trovato dai recruiter che cercano attivamente candidati, senza che ci sia bisogno di candidarsi a nessun annuncio specifico.

Il terzo vantaggio è la personalizzazione: le piattaforme digitali permettono di filtrare le offerte per settore, luogo, tipo di contratto e livello di esperienza, risparmiando il tempo di consultare centinaia di annunci irrilevanti. Il quarto è la rete: il networking digitale permette di costruire e mantenere relazioni professionali con persone di tutta Italia e di tutto il mondo, ampliando enormemente le opportunità rispetto a quelle accessibili solo attraverso contatti personali diretti.

IL MERCATO DEL LAVORO: TENDENZE E OPPORTUNITÀ DEL TERRITORIO

Obiettivi del modulo

Al termine di questo modulo comprenderai le principali tendenze che stanno trasformando il mercato del lavoro a livello nazionale e locale. Saprà identificare i settori in crescita nel territorio campano e le competenze più richieste, così da orientare la tua ricerca di lavoro e i tuoi investimenti formativi nella direzione più produttiva.

Le tendenze che trasformano il mercato del lavoro

Il mercato del lavoro è in continua trasformazione, guidato da forze che agiscono a livello globale ma che producono effetti molto concreti anche a livello locale. Quattro grandi tendenze stanno ridisegnando il paesaggio delle opportunità professionali.

La digitalizzazione è la trasformazione più pervasiva. Ogni settore, dalla grande industria alla piccola bottega artigiana, è attraversato da una crescente domanda di competenze digitali. Non si tratta soltanto di sapere usare un computer: le aziende cercano persone capaci di gestire la presenza online, di analizzare i dati sui clienti, di ottimizzare i processi con strumenti digitali. Anche settori tradizionalmente lontani dal mondo tecnologico – come l'agricoltura, il commercio al dettaglio o i servizi alla persona – sono sempre più interessati da questa trasformazione.

La sostenibilità è la seconda grande tendenza. La transizione verso un'economia più rispettosa dell'ambiente sta creando nuove figure professionali e trasformando quelle esistenti. L'agricoltura biologica, il turismo sostenibile, le energie rinnovabili, l'economia circolare: questi non sono soltanto slogan ma settori in crescita reale, che cercano professionisti con competenze specifiche. Agronomi, esperti ambientali, guide naturalistiche, tecnici per le energie rinnovabili: sono figure sempre più richieste anche nei territori rurali e montani.

Il turismo enogastronomico rappresenta un'opportunità particolarmente rilevante per il territorio campano. La valorizzazione delle produzioni locali – vino, olio, prodotti tipici – e la crescente attenzione dei viaggiatori per le esperienze autentiche legate al territorio hanno creato una domanda sostenuta di professionisti dell'ospitalità, della ristorazione, della comunicazione del territorio e dell'organizzazione di esperienze turistiche. Il Sannio, il Cilento, l'Irpinia, la Costiera: sono aree con un patrimonio enorme, che aspetta di essere valorizzato da persone capaci di comunicarlo e gestirlo.

I servizi alla persona costituiscono il quarto filone di opportunità in forte crescita. L'invecchiamento della popolazione, l'aumento delle fragilità sociali e la crescente attenzione alla qualità della vita stanno producendo una domanda crescente di figure professionali nel settore socio-sanitario, nell'assistenza agli anziani e nelle attività educative. Si tratta di lavori che richiedono competenze relazionali oltre che tecniche, e che hanno il vantaggio di essere difficilmente delocalizzabili: si svolgono vicino alle persone, sul territorio.

Opportunità specifiche nel territorio campano

Il territorio campano, e in particolare le aree interne, presenta caratteristiche che lo rendono ricco di opportunità in alcuni settori specifici. Conoscerle permette di orientare la propria ricerca di lavoro e le proprie scelte formative in modo più mirato ed efficace. Nel settore agroalimentare, le opportunità sono legate sia alla produzione che alla comunicazione e alla commercializzazione. Esperti in produzione biologica, tecnici per la trasformazione dei prodotti tipici, professionisti del marketing agricolo capaci di portare i prodotti locali sui mercati digitali, sommelier e guide enogastronomiche: sono figure richieste da un territorio che ha molto da offrire ma non sempre le risorse umane per valorizzarlo adeguatamente. Nel settore turistico, le opportunità spaziano dalle guide turistiche locali agli operatori di strutture ricettive – bed and breakfast, agriturismo, piccoli hotel – fino agli organizzatori di esperienze enogastronomiche e culturali. Chi sa combinare la conoscenza del territorio con competenze digitali di base – gestione di un sito web, presenza sui social network, uso delle piattaforme di prenotazione online – ha un vantaggio competitivo significativo.

Nel commercio e nell'artigianato, la sfida principale è portare online ciò che tradizionalmente si vendeva solo in presenza. Chi sa gestire un negozio online, comunicare efficacemente sui social network, raggiungere clienti al di fuori del mercato locale: queste sono competenze preziose per valorizzare le produzioni artigianali e commerciali del territorio. Nel settore dei servizi, sono particolarmente richiesti formatori e facilitatori digitali – come quelli formati dal progetto Digita Facile Campania – oltre a consulenti per l'accesso a finanziamenti e bandi pubblici (PSR, PNRR), tecnici per la manutenzione e l'installazione di sistemi digitali ed energetici, e figure di supporto alle istituzioni locali nella gestione dei servizi digitali.

Le competenze più richieste

Conoscere le tendenze del mercato serve a poco se non si traduce in una comprensione chiara delle competenze che le aziende cercano. Due grandi categorie di competenze dominano le richieste dei datori di lavoro, indipendentemente dal settore. Le hard skills digitali più richieste includono la capacità di gestire la presenza online di un'azienda o di un professionista – attraverso i

social network, un sito web, le piattaforme di e-commerce – la conoscenza dei principi base del marketing digitale, la capacità di gestire dati e informazioni attraverso strumenti digitali, e la padronanza di almeno una lingua straniera, con l'inglese come priorità assoluta. Queste competenze sono trasversali: servono in quasi tutti i settori del mercato del lavoro contemporaneo.

Le soft skills più valorizzate sono la proattività – la capacità di agire senza aspettare che qualcuno dica cosa fare – la flessibilità e la disponibilità ad adattarsi a situazioni nuove, la capacità di lavorare in team anche in contesti complessi, il problem solving – affrontare i problemi con metodo anziché bloccarsi di fronte alle difficoltà – e l'orientamento al cliente, ovvero la capacità di capire e rispondere alle esigenze di chi si serve.

Da ricordare: Non devi avere tutte queste competenze per iniziare a cercare lavoro, ma sapere quali sono le più richieste ti aiuta a capire come investire il tuo tempo di formazione per aumentare le tue possibilità.

Obiettivi del modulo

Al termine di questo modulo saprai applicare le principali tecniche per scrivere un curriculum vitae efficace, personalizzato e ottimizzato per i sistemi di selezione automatica. Saprai anche costruire una lettera di presentazione che completi il CV senza ripeterlo, comunicando con chiarezza la tua motivazione e il valore che puoi portare all'azienda.

Tecniche per un curriculum vitae che funziona

Un curriculum vitae efficace non è semplicemente un elenco di cose fatte: è un documento strategico, costruito per rispondere alle esigenze di chi lo legge e per superare i filtri – umani e automatici – che separano una candidatura dal cestino dall'invito a un colloquio.

La struttura e la chiarezza sono la base di tutto. Il documento deve essere ordinato, immediatamente leggibile, organizzato in sezioni ben definite. L'ordine cronologico inverso – dalla esperienza più recente alla più datata – è lo standard riconosciuto a livello internazionale: inizia dall'ultimo lavoro o dall'ultimo titolo di studio conseguito. I caratteri devono essere leggibili – Arial, Calibri, Georgia sono scelte sicure – e la lunghezza non dovrebbe superare le due pagine, salvo casi di profili con molti anni di esperienza.

La personalizzazione è forse l'aspetto più importante e più spesso trascurato. Ogni curriculum vitae dovrebbe essere adattato all'annuncio specifico a cui ci si candida, incorporando le parole chiave – sia per le hard skills tecniche che per le soft skills – presenti nell'offerta di lavoro. Questo non significa inventarsi competenze che non si hanno, ma presentare quelle che si possiedono usando il linguaggio che il datore di lavoro usa. Questa pratica è particolarmente importante per superare i sistemi ATS – i software che molte aziende usano per pre-selezionare automaticamente i curriculum – che cercano corrispondenze tra le parole dell'annuncio e quelle del documento. Il focus sui risultati distingue un curriculum generico da uno efficace. Invece di limitarsi a elencare le mansioni svolte – “mi occupavo della gestione dei clienti” – quantifica i risultati ottenuti: “Ho gestito un portafoglio di 40 clienti, contribuendo a un aumento del fatturato del 15% in dodici mesi”.

I numeri rendono le affermazioni credibili e concrete, e aiutano il selezionatore a capire non solo cosa hai fatto ma quanto bene lo hai fatto.

I dettagli essenziali non vanno mai dimenticati: contatti aggiornati con e-mail professionale e numero di telefono con prefisso, link al profilo LinkedIn se aggiornato, e una breve sintesi professionale – tre o quattro righe all'inizio del documento – che presenti chi sei, quali sono le tue competenze principali e qual è il tuo obiettivo professionale attuale.

La lettera di presentazione: raccontare il perché

La lettera di presentazione è il documento che accompagna il curriculum vitae e svolge una funzione completamente diversa: non ripete le informazioni già presenti nel CV, ma le interpreta, le contestualizza e le connette alle esigenze specifiche dell'azienda a cui ci si rivolge. È l'occasione per mostrare la propria motivazione, la propria personalità e la propria comprensione del ruolo e del contesto aziendale.

La personalizzazione estrema è la prima regola. Una lettera di presentazione inviata a dieci aziende diverse con solo il nome modificato è praticamente inutile: i selezionatori riconoscono immediatamente le lettere standard e le trattano di conseguenza. Una lettera efficace dimostra di aver letto con attenzione l'annuncio, di conoscere l'azienda – la sua storia, i suoi prodotti o servizi, la sua cultura – e di aver pensato specificamente al valore che si può portare in quel contesto.

La brevità e la struttura chiara sono altrettanto importanti. Una pagina è il limite massimo: nessun selezionatore legge lettere di presentazione lunghe. La struttura ideale prevede un'apertura che cattura l'attenzione e spiega perché ci si candida per quella posizione specifica, un corpo in cui si collegano le proprie esperienze e competenze alle esigenze del ruolo – senza ripetere il CV ma spiegando il significato di quelle esperienze – e una chiusura con una chiara call to action: la richiesta di un colloquio o di un incontro.

L'attenzione alle specificità locali può fare la differenza, soprattutto in un contesto come quello campano. Se si ha un legame con il territorio – si è cresciuti in quella zona, si ha un'esperienza professionale nel settore locale, si conosce la realtà specifica dell'azienda – metterlo in evidenza può essere un elemento di distinzione rispetto ad altri candidati. Un'azienda che opera nel turismo del Sannio apprezzerà che un candidato dimostri di conoscere e amare quel territorio.

Consiglio: Prima di scrivere la lettera di presentazione, dedica dieci minuti a cercare informazioni sull'azienda: il suo sito web, le sue pagine social, eventuali articoli o notizie recenti che la riguardano. Quelle informazioni ti permetteranno di scrivere qualcosa di specifico e genuino, che nessun altro candidato potrà copiare.

IL COLLOQUIO E IL NETWORKING: COSTRUIRE RELAZIONI CHE APRONO PORTE

Obiettivi del modulo

Al termine di questo modulo avrai gli strumenti per prepararti efficacemente a un colloquio di lavoro, inclusa la conoscenza del metodo STAR per rispondere alle domande comportamentali. Saprai anche come costruire e coltivare una rete di relazioni professionali – sia online che di persona – che può aprirti opportunità non sempre visibili sui portali di ricerca lavoro.

Prepararsi al colloquio: più che rispondere a domande

Il colloquio di lavoro è un incontro, non un interrogatorio. Chi lo affronta come tale – con la curiosità di conoscere l'azienda, oltre che con il desiderio di presentarsi bene – ottiene quasi sempre risultati migliori di chi lo vive come una prova da superare. Questa premessa non è filosofia: ha conseguenze pratiche molto concrete sul modo in cui ci si prepara.

La preparazione sulle domande comuni è il punto di partenza. Alcune domande compaiono in quasi tutti i colloqui e non hanno nulla di imprevedibile: chi sei e cosa hai fatto, quali sono i tuoi punti di forza e di debolezza, perché vuoi lavorare in quell'azienda, dove ti vedi tra cinque anni. Prepararsi una risposta personale, autentica e concisa per ciascuna di queste domande è il modo più efficace per non essere colti di sorpresa e per comunicare con chiarezza. La risposta alla domanda “parlami di te” non è la storia della tua vita: è una presentazione professionale di circa due minuti, focalizzata su chi sei oggi e perché sei lì.

La ricerca sull'azienda è altrettanto fondamentale. Prima di un colloquio, leggi tutto ciò che riesci a trovare sull'azienda: il sito web, le pagine social, le ultime notizie che la riguardano. Comprendi cosa fa, come lo fa, per chi lo fa. Questo ti permette di rispondere alle domande in modo contestualizzato – non in modo generico – e di formulare domande intelligenti sull'azienda, che dimostrano interesse reale e preparazione.

Il metodo STAR: rispondere con chiarezza e concretezza

Molti colloqui moderni includono domande comportamentali: domande che chiedono di raccontare situazioni reali del passato come indicatori di come ci si comporterà in futuro. “Raccontami di una volta in cui hai dovuto gestire un conflitto in un team”, “Descrivi una situazione in cui hai dovuto rispettare una scadenza molto stretta”, “Parlami di un progetto che non è andato come previsto e di cosa hai imparato”.

Il metodo STAR è uno strumento semplice e potente per rispondere a questo tipo di domande in modo strutturato, chiaro e convincente. L'acronimo sta per Situation (Situazione), Task (Compito), Action (Azione) e Result (Risultato). Si

descrive prima il contesto in cui ci si trovava, poi qual era il compito o la responsabilità specifica, poi le azioni concrete che si sono intraprese, e infine il risultato ottenuto — preferibilmente quantificabile.

Un esempio pratico: alla domanda “Raccontami di una volta in cui hai dovuto gestire una situazione difficile con un cliente”, una risposta STAR potrebbe essere: “Lavoravo come addetto al ricevimento di un agriturismo (Situazione). Un cliente si lamentava perché la sua camera non corrispondeva a quella prenotata online e minacciava di andarsene (Compito: gestire la situazione senza perdere il cliente). Ho ascoltato senza interrompere, ho riconosciuto il disagio, e ho proposto di aggiornarli gratuitamente alla suite disponibile (Azione). Il cliente non solo è rimasto, ma ha lasciato una recensione a cinque stelle sottolineando la nostra attenzione al servizio (Risultato).”. Questo tipo di risposta è enormemente più efficace di una risposta generica come “Cerco sempre di essere gentile con i clienti”.

Il networking: costruire relazioni che creano opportunità

Si stima che una percentuale molto alta delle posizioni lavorative venga coperta attraverso reti di conoscenza, senza mai comparire su un portale di annunci. Il networking — la costruzione e la cura di una rete di relazioni professionali — non è quindi un'attività accessoria per chi cerca lavoro: è una delle strategie più efficaci in assoluto.

L'obiettivo del networking non è chiedere lavoro alle persone che si incontrano. È costruire relazioni genuine, basate su interesse reciproco, fiducia e scambio di valore. Chi si avvicina al networking con la mentalità del “cosa posso ottenere” ottiene quasi sempre meno di chi lo affronta con la mentalità del “come posso essere utile”. Condividere risorse, fare presentazioni tra persone che potrebbero beneficiarne, offrire il proprio aiuto senza aspettarsi nulla in cambio: queste sono le basi di relazioni professionali solide e durature. Le occasioni di networking sono ovunque: fiere del lavoro, convegni di settore, eventi organizzati da associazioni professionali, meetup tematici, eventi universitari. In un contesto territoriale come quello campano, anche le sagre, i mercati dei produttori locali e gli eventi culturali possono essere occasioni per incontrare imprenditori, professionisti e potenziali collaboratori. Il follow-up è fondamentale: un breve messaggio di ringraziamento dopo un incontro, un commento a un post LinkedIn, una segnalazione occasionale: questi piccoli gesti tengono viva una relazione che altrimenti si spegne nel giro di pochi giorni.

LinkedIn è lo strumento di networking digitale per eccellenza. Permette di mantenere i contatti con persone incontrate dal vivo, di raggiungerne di nuove nel proprio settore, di partecipare a discussioni professionali e di essere trovati da chi cerca competenze come le tue. Seguire le aziende di interesse, commentare i post dei professionisti del proprio settore, condividere contenuti rilevanti: sono azioni semplici che aumentano la visibilità e costruiscono una reputazione professionale online.

LE PIATTAFORME ONLINE: DOVE E COME CERCARE LAVORO

Obiettivi del modulo

Al termine di questo modulo saprai utilizzare le principali piattaforme digitali per la ricerca di lavoro, con particolare attenzione a LinkedIn e ClicLavoro. Saprai costruire un profilo professionale online attraente e completo, capace di farti trovare dai recruiter e di rappresentarti efficacemente nel mercato del lavoro digitale.

LinkedIn: molto più di un curriculum online

LinkedIn è la piattaforma professionale più utilizzata al mondo, con oltre un miliardo di utenti registrati. Non è soltanto un posto dove caricare il proprio curriculum: è un ecosistema professionale completo, dove si cercano e si trovano lavori, si costruiscono reti di contatti, si seguono le aziende di interesse, si pubblicano e si leggono contenuti professionali, si partecipa a discussioni di settore.

La differenza tra chi usa LinkedIn in modo passivo – si iscrive, carica il CV e aspetta – e chi lo usa in modo attivo è enorme. Chi partecipa alle discussioni del proprio settore, pubblica occasionalmente contenuti rilevanti, commenta i post delle aziende che segue e interagisce con i professionisti della propria rete aumenta significativamente la propria visibilità. I recruiter non cercano soltanto i profili che si candidano attivamente: cercano anche quelli che emergono nelle ricerche per parole chiave e nelle discussioni di settore.

Per la ricerca di lavoro attiva, LinkedIn offre strumenti potenti: la sezione “Offerte di lavoro” permette di filtrare gli annunci per ruolo, settore, luogo e tipo di contratto, di impostare notifiche per le nuove offerte corrispondenti al proprio profilo, e di candidarsi direttamente dalla piattaforma. La funzione “Aperto a nuove opportunità” – che può essere resa visibile soltanto ai recruiter, non ai propri contatti – segnala la disponibilità a essere contattati per proposte di lavoro.

ClicLavoro e i portali istituzionali

ClicLavoro è il portale ufficiale del Ministero del Lavoro per l'incontro tra domanda e offerta di lavoro. Ha una natura istituzionale che lo distingue dalle piattaforme commerciali: gli annunci presenti sono pubblicati da aziende registrate e verificate, ed è il canale attraverso cui molti enti pubblici e aziende convenzionate con i Centri per l'Impiego comunicano le proprie offerte. In Campania, il portale è integrato con il sistema SILF Campania.

Mantenere il proprio profilo aggiornato su ClicLavoro – con il curriculum sempre attuale e tutte le sezioni compilate correttamente – aumenta la visibi-

lità presso una categoria specifica di datori di lavoro che usa questo canale istituzionale. Non è uno strumento alternativo a LinkedIn: è complementare, e consente di raggiungere opportunità che spesso non compaiono sulle piattaforme commerciali.

Costruire un profilo professionale attraente

Sia su LinkedIn che su ClicLavoro, la qualità del profilo determina direttamente la qualità delle opportunità che si ricevono. Costruire un profilo professionale efficace richiede attenzione a diversi elementi.

La foto professionale è il primo elemento che chi visita il profilo nota. Deve essere chiara, con uno sfondo neutro, un abbigliamento appropriato al proprio settore e un'espressione seria ma accogliente. Non una foto di vacanza, non un selfie, non una foto in compagnia: una foto che trasmetta professionalità e affidabilità.

Il titolo professionale – la headline su LinkedIn – è lo spazio più prezioso del profilo. Non deve limitarsi a indicare la posizione attuale, ma deve comunicare il proprio valore in modo sintetico e d'impatto. “Guida turistica | Esperta di enogastronomia del Sannio” dice molto di più di “Dipendente presso Agenzia XYZ”. Deve includere le parole chiave con cui i recruiter cercano profili come il tuo.

Il sommario – la sezione “Info” su LinkedIn – è lo spazio per presentarsi in prima persona, in modo coinvolgente e specifico. Non è il riassunto del CV: è la risposta alla domanda “chi sei e cosa puoi fare per me?”. Deve essere scritto in modo diretto, mostrare la propria personalità professionale e includere una call to action implicita: far capire che si è disponibili a essere contattati.

Le esperienze devono essere descritte in termini di risultati, non solo di mansioni. Per ogni ruolo, indica l'azienda, le date, il ruolo e – nella descrizione – i risultati concreti ottenuti, preferibilmente con dati numerici. Le competenze elencate devono essere coerenti con il profilo che si vuole costruire. Le raccomandazioni – testi scritti da ex colleghi o superiori che attestano le proprie capacità – sono tra gli elementi più convincenti per un recruiter.

Consiglio: Personalizza il tuo URL LinkedIn: invece dell'indirizzo generato automaticamente dalla piattaforma, crea un indirizzo del tipo [linkedin.com/in/mariabianchi](https://www.linkedin.com/in/mariabianchi). È più professionale, più facile da ricordare e da inserire nel curriculum vitae.

LE SOFT SKILLS: LE COMPETENZE CHE FANNO LA DIFFERENZA

Obiettivi del modulo

Al termine di questo modulo comprenderai perché le competenze trasversali – le soft skills – sono sempre più valorizzate nel mercato del lavoro contemporaneo. Conoscerai le principali soft skills richieste e saprai come svilupparle attraverso attività pratiche, come comunicarle efficacemente in un colloquio o in un curriculum, e come riconoscerle nelle proprie esperienze di vita quotidiana, anche in assenza di un'esperienza lavorativa formale.

Cosa sono le soft skills e perché contano

Le soft skills – letteralmente “competenze morbide” – sono le abilità relazionali, comportamentali e cognitive che determinano il modo in cui una persona interagisce con gli altri, gestisce il proprio lavoro e affronta le sfide. Si distinguono dalle hard skills – le competenze tecniche specifiche, come la padronanza di un software o la conoscenza di una lingua straniera – perché non sono legate a un settore o a uno strumento specifico: sono trasversali, cioè utili in qualsiasi contesto lavorativo.

Per molto tempo, le soft skills sono state considerate secondarie rispetto alle competenze tecniche. Oggi, questa gerarchia è stata ribaltata. In un mercato del lavoro in cui le competenze tecniche si aggiornano rapidamente e molte operazioni vengono automatizzate, le capacità che rimangono irriproducibili dalle macchine – la comunicazione empatica, la creatività, il pensiero critico, la capacità di costruire relazioni di fiducia – sono diventate le competenze più preziose. Non a caso, molti selezionatori affermano che preferiscono assumere qualcuno con ottime soft skills e competenze tecniche di base da sviluppare, piuttosto che qualcuno con competenze tecniche eccellenti ma difficoltà relazionali.

Le principali soft skills e come svilupparle

La comunicazione efficace è la prima e forse la più importante soft skill. Comunicare bene non significa soltanto saper parlare in modo chiaro e persuasivo: significa anche saper ascoltare con attenzione, capire il punto di vista dell'altro prima di rispondere, adattare il proprio stile comunicativo al contesto e all'interlocutore, e saper scrivere messaggi ed e-mail che trasmettano esattamente ciò che si vuole dire senza ambiguità.

Per sviluppare la comunicazione efficace nella vita quotidiana, si può praticare l'ascolto attivo: nelle conversazioni, invece di pensare a cosa si dirà mentre l'altro parla, ci si concentra su ciò che l'altro sta dicendo, riassumendone il punto principale prima di rispondere. Si possono fare presentazioni davanti a un gruppo ristretto di amici o familiari, chiedendo feedback specifico. Si

può tenere un diario di scrittura, per migliorare la capacità di esprimere i propri pensieri in forma scritta. Il lavoro di squadra è la capacità di collaborare efficacemente con altri verso un obiettivo comune, gestendo le differenze di opinione, le tensioni interpersonali e le diverse modalità di lavoro.

Non si tratta soltanto di andare d'accordo con tutti: si tratta di saper contribuire in modo complementare alle competenze altrui, di saper cedere il proprio punto di vista quando quello di un altro è più valido, e di saper sostenere i colleghi in difficoltà senza aspettare che qualcuno lo chieda. La gestione del tempo e delle priorità è sempre più richiesta in un contesto lavorativo in cui le richieste si moltiplicano e le scadenze si sovrappongono. Saper distinguere l'urgente dall'importante, pianificare la propria giornata in modo realistico, rispettare le scadenze e saper dire no quando il carico di lavoro supera le proprie capacità: queste sono competenze che si imparano con la pratica e con strumenti specifici. Metodologie come la Tecnica Pomodoro – lavorare in blocchi di 25 minuti con brevi pause – o il metodo GTD (Getting Things Done) possono aiutare a costruire abitudini di lavoro più efficaci.

L'adattabilità e la flessibilità sono le competenze del cambiamento: la capacità di affrontare situazioni nuove e impreviste senza bloccarsi, di imparare rapidamente da errori e fallimenti, di modificare il proprio approccio quando la situazione lo richiede. In un mercato del lavoro in continua evoluzione, chi sa adattarsi ha un vantaggio enorme rispetto a chi cerca di mantenere le cose come sono. Si sviluppa esponendosi deliberatamente a situazioni nuove, accettando incarichi diversi da quelli abituali e cercando attivamente il feedback degli altri.

La leadership e l'intelligenza emotiva completano il quadro delle soft skills più richieste. La leadership non è un attributo esclusivo di chi ha un ruolo gerarchico: è la capacità di influenzare positivamente gli altri, di motivare un team verso un obiettivo, di prendere decisioni anche in condizioni di incertezza. L'intelligenza emotiva – la capacità di riconoscere e gestire le proprie emozioni e di comprendere quelle degli altri – è la base di qualsiasi forma di leadership efficace.

Come comunicare le soft skills in un colloquio

Le soft skills non si dichiarano: si dimostrano attraverso esempi. Dire “sono un buon comunicatore” non convince nessuno; raccontare una situazione in cui la propria capacità comunicativa ha risolto un problema concreto, sì. Il metodo STAR – presentato nel modulo precedente – è lo strumento ideale per trasformare le proprie soft skills in storie convincenti.

Chi non ha ancora esperienze lavorative formali non è in svantaggio: le soft skills si acquisiscono e si dimostrano anche attraverso la vita quotidiana. Un progetto di gruppo scolastico dimostra capacità di lavoro di squadra. Un'attività sportiva dimostra disciplina e resilienza. Un'esperienza di volontariato dimostra empatia e orientamento agli altri. Riconoscere queste esperienze come esempi di competenze professionali è il primo passo per comunicarle efficacemente.

AUTOVALUTAZIONE E PIANO D'AZIONE PER LA PROPRIA CARRIERA

Obiettivi del modulo

Al termine di questo modulo saprai condurre un'autovalutazione strutturata delle tue competenze e dei tuoi obiettivi professionali. Sarai in grado di costruire un piano d'azione realistico e concreto per la tua ricerca di lavoro, usando strumenti come l'analisi SWOT personale e gli obiettivi SMART. Avrai una roadmap – un percorso tracciato – che ti guiderà nei prossimi mesi.

L'autovalutazione: il punto di partenza

Qualsiasi percorso professionale efficace inizia da una domanda fondamentale: chi sono e dove voglio andare? Rispondere a questa domanda con onestà e chiarezza richiede un esercizio di riflessione strutturata che va oltre il semplice compilare un curriculum vitae. Si tratta di guardare alla propria storia – formativa, lavorativa, personale – e di estrarne il significato professionale: quali competenze ho sviluppato? Quali sono i miei punti di forza autentici? Dove invece sono più fragile? Cosa mi motiva davvero?

Uno strumento utile per questa riflessione è l'analisi SWOT personale, mutuata dal mondo aziendale ma perfettamente applicabile al percorso individuale. Le Strengths – i punti di forza – sono le competenze, le caratteristiche e le esperienze che ti differenziano positivamente dagli altri candidati. Le Weaknesses – i punti di debolezza – sono le aree in cui sei meno competente o meno efficace, che è utile riconoscere onestamente non per scoraggiarsi ma per decidere dove investire in formazione. Le Opportunities – le opportunità – sono le tendenze del mercato del lavoro, i settori in crescita, i cambiamenti nel contesto economico e sociale che creano spazio per profili come il tuo. Le Threats – le minacce – sono i rischi che possono ostacolare il tuo percorso: la concorrenza di altri candidati, la mancanza di una certificazione specifica, la lontananza geografica dalle opportunità più interessanti.

Un secondo strumento di autovalutazione è il riconoscimento dei propri valori e interessi. Capire cosa ti motiva profondamente – non soltanto cosa sai fare, ma cosa ti dà soddisfazione fare – è fondamentale per costruire un percorso professionale sostenibile nel lungo periodo. Chi lavora in un settore che non lo appassiona finisce per essere meno produttivo, meno proattivo e meno soddisfatto, indipendentemente dallo stipendio. Allineare i propri obiettivi professionali ai propri valori autentici non è un lusso: è la condizione per una carriera che duri e che faccia stare bene.

Gli obiettivi SMART: trasformare i sogni in piani

Avere un obiettivo professionale è il primo passo; averlo formulato in modo

SMART è il secondo, e forse il più importante. Il metodo SMART è un framework semplice per trasformare un'idea vaga in un obiettivo concreto, misurabile e raggiungibile.

Un obiettivo è Specifico quando indica esattamente cosa si vuole ottenere: non “voglio trovare un lavoro” ma “voglio ottenere una posizione come addetta alla comunicazione di un'azienda agroalimentare campana”. È Misurabile quando è possibile verificare se è stato raggiunto: non “voglio migliorare le mie competenze digitali” ma “voglio ottenere la certificazione Google Digital Marketing”. È Achievable – raggiungibile – quando è realistico rispetto alle proprie risorse e al contesto: ambizioso ma non impossibile. È Relevant – rilevante – quando è coerente con i propri valori, i propri interessi e la propria situazione di vita. È Time-bound – temporizzato – quando ha una scadenza: non “prima o poi” ma “entro sei mesi”.

La distinzione tra obiettivi a breve termine – da uno a due anni – e a lungo termine – da tre a cinque anni o più – è altrettanto importante. Gli obiettivi a breve termine sono quelli su cui si lavora concretamente nei prossimi mesi: completare un corso, ottenere una certificazione, candidarsi a un primo lavoro nel settore desiderato, costruire una rete di contatti in un determinato ambito. Gli obiettivi a lungo termine indicano la direzione generale della carriera: dove si vuole arrivare, che tipo di professionista si vuole diventare.

Il piano d'azione: dai propositi ai passi concreti

Un piano d'azione è la traduzione degli obiettivi in azioni concrete, sequenziali e temporizzate. È la differenza tra chi dice “devo aggiornarmi” e chi sa che ogni martedì dalle 19 alle 20 segue il corso online di marketing digitale che finirà tra tre mesi con una certificazione. È la differenza tra chi vuole fare networking e chi si iscrive all'associazione di categoria locale e partecipa al primo evento del mese.

Il piano d'azione per la ricerca di lavoro si articola in alcune aree fondamentali. Lo sviluppo delle competenze prevede l'iscrizione ai corsi o ai programmi di formazione identificati come prioritari, la pianificazione dei tempi di studio e la definizione delle certificazioni da ottenere. La ricerca mirata delle opportunità prevede la consultazione regolare dei portali di lavoro, la definizione delle aziende target e il monitoraggio delle loro aperture, e l'uso strutturato delle piattaforme digitali. Il networking prevede la partecipazione a eventi di settore, l'attività costante su LinkedIn e la cura delle relazioni esistenti. La preparazione dei materiali prevede l'aggiornamento del curriculum vitae e del profilo LinkedIn, la preparazione di più versioni del CV per diversi tipi di candidatura, e l'esercizio sulle tecniche di colloquio.

Il monitoraggio regolare del piano è altrettanto importante della sua costruzione. Ogni mese, è utile fare un bilancio: cosa si è fatto, cosa si è ottenuto, cosa non ha funzionato e perché. I piani non devono essere rigidi: devono es-

sere flessibili a sufficienza da adattarsi ai cambiamenti del contesto e della propria situazione. L'obiettivo non è eseguire il piano alla lettera, ma usarlo come guida per non perdere di vista la direzione.

Consiglio: Inizia con un passo piccolo ma concreto. Invece di pianificare l'intera carriera, chiediti: qual è la cosa più utile che posso fare questa settimana per avvicinarmi al mio obiettivo? Falla. Poi passa alla prossima. I grandi percorsi si costruiscono un passo alla volta.

Le domande più frequenti: risposte concrete

Nel corso delle sessioni formative, alcuni interrogativi ricorrono con regolarità. Sono domande che molti si pongono ma che spesso non si osano formulare ad alta voce. Rispondere a queste domande in modo diretto e onesto fa parte dell'obiettivo di questo percorso: fornire strumenti reali, non risposte vaghe.

Devo per forza cercare lavoro solo tra le professioni più richieste nella mia zona?

No. Conoscere le professioni più richieste sul territorio è utile non per limitarsi a quelle, ma per capire quali competenze aggiuntive potrebbero rendere il tuo profilo più interessante per le aziende. Se la tua passione e le tue competenze sono in un settore specifico, quella è la direzione giusta da seguire. Il mercato del lavoro premia chi porta competenze uniche e motivazione genuina tanto quanto chi insegue le mode del momento.

Detto questo, conoscere le tendenze ti permette di fare scelte più informate: se il settore che ti interessa è in crescita nel territorio, è una buona notizia. Se è in calo, non significa che devi abbandonarlo, ma che potresti dover essere più creativo nell'identificare le nicchie in cui le tue competenze sono ancora richieste, o nel pensare a come combinarle con competenze digitali per aprire mercati nuovi.

Perché non posso inviare lo stesso CV a tutte le aziende per fare prima?

Perché un CV generico dice al selezionatore che non sei disposto a fare lo sforzo minimo necessario per dimostrare il tuo interesse. In un mercato competitivo, dove centinaia di persone si candidano per lo stesso ruolo, il dettaglio che fa la differenza è spesso proprio questo: qualcuno che ha letto l'annuncio con attenzione, ha capito cosa si cerca e ha presentato la propria esperienza in modo coerente con quella ricerca.

La personalizzazione non richiede riscrivere il CV da zero ogni volta. Significa adattare il profilo professionale iniziale, riorganizzare l'ordine delle esperienze per mettere in evidenza quelle più rilevanti, e assicurarsi che le parole chiave presenti nell'annuncio compaiano nel documento. Venti minuti di lavoro aggiuntivo che possono fare la differenza tra essere chiamati o no.

Cosa rispondo alla domanda “parlami di te” se non ho mai lavorato?

Parla di chi sei come persona e come professionista in divenire. Racconta brevemente il tuo percorso formativo, le tue passioni — soprattutto quelle che hanno un collegamento con il ruolo per cui ti candidi — e perché sei motivato a entrare in quel settore specifico. Mostra curiosità, entusiasmo e una disponibilità concreta a imparare.

Ricorda che il selezionatore che incontra un candidato senza esperienza lavorativa non si aspetta un professionista formato: si aspetta una persona con potenziale, voglia di crescere e caratteristiche personali che la rendano un buon investimento. Concentra la risposta su queste dimensioni, non sull'assenza di un curriculum professionale.

Come fisso un obiettivo professionale se non so ancora che lavoro voglio fare?

Non devi sapere con certezza dove vuoi arrivare per iniziare a muoverti. Un obiettivo a breve termine può essere molto semplice: esplorare un settore che ti incuriosisce, fare un corso su una competenza che non possiedi, cercare un primo lavoro part-time per capire cosa ti piace e cosa no. La chiarezza sull'obiettivo finale viene spesso dopo le prime esperienze, non prima.

L'importante è evitare il blocco da perfezionismo: aspettare di avere le idee perfettamente chiare prima di iniziare è una delle trappole più comuni. Inizia dal passo più piccolo che puoi fare oggi — seguire un canale YouTube professionale, leggere due articoli sul settore che ti interessa, chiedere a qualcuno che lavora in quel campo come si trova — e lascia che l'esperienza ti guidi verso una maggiore chiarezza.

Ho un obiettivo grande ma mi sembra irraggiungibile. Da dove inizio?

Spezzettalo in obiettivi più piccoli e concreti. Un obiettivo come “voglio lavorare nel mondo della comunicazione” diventa gestibile quando lo traduci in una serie di passi: questa settimana seguo tre professionisti del settore su LinkedIn; questo mese leggo due libri di marketing; entro tre mesi completo un corso gratuito di content marketing; entro sei mesi ho un piccolo portfolio con tre esempi di lavoro che ho fatto gratuitamente per un'associazione locale.

I grandi obiettivi si raggiungono quasi sempre un passo alla volta, non con un salto solo. E ogni passo completato, per quanto piccolo, costruisce la motivazione e la fiducia necessarie per fare il passo successivo. Non sottovalutare il potere dei risultati intermedi.

Gli errori più comuni nella ricerca del lavoro: come evitarli

Conoscere gli errori che le persone in cerca di lavoro commettono più frequentemente è tanto importante quanto conoscere le buone pratiche. Spesso si tratta di errori involontari, frutto di informazioni incomplete o di abitudini consolidate che non rispecchiano le aspettative del mercato del lavoro moderno.

Candidarsi a tutto senza un criterio

L'idea che mandare più candidature aumenti le probabilità di trovare lavoro è comprensibile ma fuorviante. Candidarsi a decine di posizioni ogni giorno, senza una selezione basata su competenze, interessi e coerenza con il proprio profilo, produce quasi sempre risultati deludenti. I selezionatori riconoscono le candidature non mirate, e la quantità non compensa la mancanza di qualità. Una strategia più efficace è identificare venti o trenta aziende target – quelle che operano nel settore di interesse, che hanno valori coerenti con i propri, che hanno dimensioni e localizzazione adeguate – e concentrare le energie su quelle, seguendole su LinkedIn, candidandosi quando aprono posizioni pertinenti e costruendo relazioni con le persone che vi lavorano.

Trascurare il follow-up

Inviare una candidatura e aspettare passivamente una risposta è uno degli errori più diffusi. Una settimana dopo aver inviato il CV, un breve messaggio di follow-up – via email o su LinkedIn – che ringrazia per l'attenzione e ribadisce l'interesse per la posizione dimostra proattività e determinazione. Non è invadente: nella stragrande maggioranza dei casi, è apprezzato.

Lo stesso principio vale dopo un colloquio: un messaggio di ringraziamento entro ventiquattro ore, in cui si ricapitola brevemente perché si è convinti di essere adatti al ruolo, può fare la differenza in una selezione in bilico tra due candidati equivalenti.

Non aggiornare i profili digitali

Un profilo LinkedIn non aggiornato, con esperienze che risalgono a tre anni fa e una foto poco professionale, trasmette scarsa cura e scarso interesse. Lo stesso vale per il profilo su ClicLavoro o su altri portali istituzionali. Aggiornare i propri profili dopo ogni nuova esperienza, corso o certificazione dovrebbe essere un'abitudine automatica, come aggiornare il numero di telefono in rubrica quando cambia.

Concentrarsi solo sulle offerte online

Le offerte di lavoro pubblicate sui portali rappresentano soltanto una parte delle posizioni disponibili. Una quota significativa dei posti di lavoro – alcune stime indicano tra il 60 e l'80 per cento – viene coperta attraverso reti informali, prima ancora di essere pubblicata. Chi si affida esclusivamente ai portali online si perde questa fetta del mercato. Il networking, le candidature spontanee, le visite dirette alle aziende di interesse: questi canali, meno comodi ma spesso più efficaci, non vanno trascurati.

Smettere di formarsi mentre si cerca lavoro

Il periodo di ricerca del lavoro non è un tempo di attesa: è un tempo da investire attivamente nel proprio sviluppo professionale. Chi durante una ricerca

di lavoro completa un corso, ottiene una certificazione o acquisisce una nuova competenza non solo migliora concretamente il proprio profilo, ma dimostra ai selezionatori una proattività e una motivazione che fanno una differenza significativa.

Da ricordare: Gli errori non sono fallimenti permanenti: sono informazioni. Ogni candidatura che non ha avuto risposta, ogni colloquio che non è andato bene contiene indicazioni preziose su dove migliorare. Chi sa estrarre queste indicazioni e usarle per calibrare la propria strategia trasforma ogni ostacolo in un passo avanti.

Riepilogo dei concetti fondamentali

Questo percorso formativo ha coperto sei grandi temi, costruendo gradualmente un quadro completo degli strumenti e delle competenze necessarie per una ricerca di lavoro efficace nell'era digitale.

Il mercato del lavoro campano offre opportunità concrete in settori in crescita — agroalimentare, turismo enogastronomico, servizi digitali, assistenza alla persona — ma coglierle richiede di conoscere le tendenze, le competenze richieste e i canali attraverso cui le opportunità vengono comunicate. Chi conosce il territorio e sa usare gli strumenti digitali per valorizzarlo ha un vantaggio reale.

Il curriculum vitae e la lettera di presentazione sono strumenti strategici, non semplici documenti burocratici. Vanno costruiti con cura, personalizzati per ogni candidatura, ottimizzati per i sistemi ATS e focalizzati sui risultati concreti ottenuti, non soltanto sulle mansioni svolte. Un curriculum ben fatto non garantisce il lavoro, ma un curriculum trascurato impedisce di arrivare al colloquio.

Il colloquio è un incontro, non un'interrogazione. Chi si prepara conoscendo l'azienda, esercitandosi sulle domande comuni e usando strumenti come il metodo STAR per raccontare le proprie esperienze ottiene risultati significativamente migliori di chi arriva impreparato. Il networking, parallelo alla ricerca attiva, apre porte che i portali di annunci non mostrano.

Le piattaforme digitali — LinkedIn, ClicLavoro, SILF Campania — sono i canali principali attraverso cui il mercato del lavoro moderno funziona. Usarle bene richiede un profilo professionale curato, un'attività costante e la capacità di sfruttare le funzionalità avanzate di ciascuna. Non basta essere presenti: bisogna essere visibili e credibili.

Le soft skills sono le competenze del futuro. Comunicazione, lavoro di squa-

dra, adattabilità, gestione del tempo, intelligenza emotiva: in un mercato in cui molte competenze tecniche diventano obsolete rapidamente, queste capacità umane sono quelle che resistono e che fanno la differenza. Si acquisiscono e si dimostrano attraverso le esperienze concrete, anche quelle non lavorative.

L'autovalutazione e la pianificazione sono il punto di partenza e il filo conduttore di qualsiasi percorso professionale efficace. Chi sa chi è, dove vuole andare e quale passo fare oggi è in una posizione enormemente più vantaggiosa di chi aspetta che le opportunità cadano dall'alto. Il piano d'azione trasforma i propositi in azioni, e le azioni in risultati.

Ogni competenza acquisita in questo percorso è immediatamente applicabile. Non aspettare di sapere tutto prima di iniziare: inizia oggi, con quello che hai imparato oggi. Il primo passo è sempre il più importante.

Scheda di autovalutazione

Compila questa scheda al termine del percorso. Per ciascuna area indica il tuo livello su una scala da 1 a 5: 1 = non mi sento ancora in grado, 5 = mi sento completamente autonomo.

Area di Competenza	Prima del corso	Dopo il corso
Conosco le principali tendenze del mercato del lavoro campano		
So scrivere un CV personalizzato e ottimizzato per gli ATS		
So costruire una lettera di presentazione efficace		
So come prepararmi a un colloquio usando il metodo STAR		
So costruire e usare un profilo LinkedIn professionale		
So riconoscere e comunicare le mie soft skills		
Ho un piano d'azione concreto per la mia ricerca di lavoro		

ATS (Applicant Tracking System): software utilizzato dalle aziende per pre-selezionare automaticamente i curriculum vitae in base a parole chiave. Per superarlo, è essenziale usare nel CV il linguaggio dell'annuncio di lavoro.

ClicLavoro: portale ufficiale del Ministero del Lavoro per l'incontro tra domanda e offerta di lavoro. In Campania è integrato con il sistema SILF.

Hard skills: competenze tecniche specifiche e misurabili, come la padronanza di un software, la conoscenza di una lingua straniera o la gestione di sistemi digitali.

Headline (LinkedIn): il titolo professionale che appare subito sotto il nome sul profilo LinkedIn. Deve comunicare il proprio valore in modo sintetico e includere le parole chiave con cui i recruiter cercano profili come il proprio.

Lifelong Learning: apprendimento continuo per tutta la vita professionale. La strategia di formarsi costantemente per adattarsi ai cambiamenti del mercato del lavoro.

LinkedIn: principale piattaforma di networking professionale al mondo. Strumento fondamentale per la ricerca di lavoro, la costruzione di una rete di contatti e la visibilità presso i recruiter.

Metodo STAR: framework per rispondere alle domande comportamentali nei colloqui: Situazione, Task (compito), Action (azione), Result (risultato). Permette di raccontare le proprie esperienze in modo strutturato e convincente.

NEET: acronimo inglese per Not in Education, Employment, or Training. Indica i giovani che non studiano, non lavorano e non seguono percorsi formativi.

Networking: costruzione e cura di una rete di relazioni professionali. Una delle strategie più efficaci per trovare opportunità di lavoro, spesso non visibili sui portali di annunci.

Obiettivi SMART: framework per la definizione di obiettivi efficaci: Specifici, Misurabili, Achievable (raggiungibili), Relevant (rilevanti), Time-bound (temporizzati).

Piano d'azione: traduzione degli obiettivi professionali in azioni concrete, sequenziali e temporizzate. Trasforma i propositi in risultati concreti.
Soft skills: competenze trasversali relazionali e comportamentali come la co-

municazione, il lavoro in team, l'adattabilità e la gestione del tempo. Sempre più valorizzate nel mercato del lavoro contemporaneo.

Analisi SWOT personale: strumento di autovalutazione che esamina i propri Punti di Forza (Strengths), Punti di Debolezza (Weaknesses), Opportunità (Opportunities) e Minacce (Threats) nel contesto del mercato del lavoro.

Upskilling: potenziamento delle competenze esistenti per migliorare le proprie prestazioni nel ruolo attuale.

Reskilling: acquisizione di competenze nuove per cambiare ruolo o settore professionale.

TEMA A
LAVORO E SVILUPPO PRODUTTIVO
 OPPORTUNITÀ DEL TERRITORIO



A chi è rivolto questo capitolo

Questo capitolo riguarda il corso “Le opportunità del Territorio”, sviluppato nell’ambito del progetto Digita Facile Campania, Tema A – Lavoro e Sviluppo Produttivo. Il corso ha un obiettivo preciso e concreto: fornire ai partecipanti strumenti pratici per leggere il proprio territorio con occhi nuovi, riconoscerne le risorse, interpretare i dati del mercato del lavoro locale e individuare le opportunità emergenti – inclusa quella di creare una propria attività imprenditoriale.

Il capitolo si articola in cinque moduli. Il primo introduce l’analisi del mercato del lavoro locale: come si misura, con quali strumenti, e come si interpretano i dati ISTAT per capire dove sta andando l’occupazione. Il secondo affronta la mappatura delle risorse del territorio: le risorse naturali e umane che costituiscono il patrimonio di sviluppo di ogni area, e gli strumenti digitali – inclusi i GIS – per analizzarle e valorizzarle. Il terzo esplora i settori produttivi emergenti: turismo sostenibile, agricoltura biologica e di precisione, tecnologie ecologiche. Il quarto è una sezione personalizzabile sulle specificità del territorio in cui si svolge il corso. Il quinto guida attraverso il processo di ideazione e creazione di una start-up, dalla valutazione dell’idea ai finanziamenti disponibili.

L’obiettivo finale non è trasmettere nozioni astratte: è restituire alle persone la capacità di orientarsi nel mercato del lavoro con consapevolezza, di riconoscere le opportunità concrete del proprio territorio e di agire per coglierle. Essere un cittadino digitale autonomo significa esattamente questo: esercitare i propri diritti e le proprie opportunità risparmiando tempo e denaro – e farlo senza stress.

La difficoltà non è mai la tecnologia in sé: è la paura di sbagliare o la mancanza di una guida. Questa dispensa è quella guida, e la buona notizia è che contiene tutto ciò che serve per comprendere, riconoscere e cogliere le opportunità del territorio.

Perché le opportunità del territorio riguardano tutti

Essere cittadini digitali autonomi: il punto di partenza

Essere un cittadino digitale autonomo non significa saper usare tutte le app disponibili. Significa qualcosa di più concreto e più importante: significa poter esercitare i propri diritti risparmiando tempo e denaro, senza dipendere da altri per accedere a informazioni, servizi e opportunità che sono già disponibili, spesso gratuitamente, nei canali digitali.

Nel contesto del lavoro e dello sviluppo produttivo, questa autonomia ha implicazioni dirette. Chi sa come leggere i dati del mercato del lavoro locale può prendere decisioni più informate sulla propria carriera, sulla formazione da intraprendere, sul tipo di attività da avviare. Chi sa mappare le risorse del proprio territorio può identificare opportunità che sfuggono a chi guarda solo ai grandi centri urbani. Chi conosce i settori emergenti sa dove indirizzare le proprie energie.

Questo corso non è riservato a chi ha già competenze imprenditoriali o economiche. Si rivolge a chiunque voglia capire meglio il contesto in cui vive e/o lavora, e cercare in modo più consapevole le opportunità. Il punto di partenza è sempre lo stesso: la bussola DigComp 2.2, e in particolare la competenza fondamentale dell'Alfabetizzazione su informazioni e dati, cioè la capacità di trovare, valutare e usare le informazioni giuste attraverso i canali digitali giusti.

Il valore del digitale per chi cerca lavoro o vuole crearlo

I vantaggi concreti degli strumenti digitali nel contesto del lavoro e dello sviluppo sono tre, e toccano direttamente la vita di tutti i giorni. Il primo è il risparmio di tempo e costi: le informazioni sul mercato del lavoro, sui bandi di finanziamento, sulle opportunità formative sono disponibili online, gratuitamente, ventiquattro ore su ventiquattro. Non servono più intermediari, non sono necessarie code agli sportelli, non serve aspettare che qualcuno ci richiami.

Il secondo è l'autonomia e la trasparenza: chi sa navigare le fonti ufficiali – ISTAT, portali regionali, banche dati del Ministero del Lavoro – può accedere agli stessi dati su cui si basano le politiche pubbliche, senza dipendere da interpretazioni di terzi. Può verificare le informazioni, confrontarle, trarre le proprie conclusioni. Il terzo è l'inclusione e l'accessibilità: gli strumenti digitali hanno democratizzato l'accesso a molte risorse che in passato erano riservate a chi aveva le connessioni o le risorse economiche giuste. Una start-up nelle aree interne della Campania può oggi accedere agli stessi strumenti, alle stesse piattaforme e agli stessi mercati di una start-up a Milano.

ANALISI DEL MERCATO LOCALE: DINAMICHE ECONOMICHE E OCCUPAZIONALI

Obiettivi del modulo

Al termine di questo modulo saprai cos'è l'analisi del mercato del lavoro locale e a cosa serve, conoscerai i principali strumenti di analisi statistica disponibili, dalle applicazioni accessibili a tutti fino agli strumenti professionali. Sarai in grado di orientarti nelle fonti ISTAT e di interpretare i dati più rilevanti per il mercato del lavoro italiano e campano.

Cos'è l'analisi del mercato del lavoro locale

L'analisi del mercato del lavoro locale è un'indagine dettagliata delle dinamiche occupazionali, economiche e sociali in un'area geografica circoscritta. Non è uno studio accademico astratto: è uno strumento operativo che monitora assunzioni, cessazioni, tassi di disoccupazione, settori produttivi e fabbisogni professionali, supportando le istituzioni, i Centri per l'Impiego e le imprese nella programmazione di politiche attive del lavoro, percorsi di formazione e strategie di gestione del personale.

Per un singolo lavoratore o per chi vuole avviare un'attività, l'analisi del mercato del lavoro locale risponde a domande concrete: quali settori stanno assumendo nella mia area? Quali competenze sono più richieste? Ci sono nicchie di mercato sottoservite che rappresentano un'opportunità? Come si confronta il mio territorio con la media regionale e nazionale? Le risposte a queste domande non richiedono di diventare statistici: richiedono di sapere dove trovare le informazioni e come leggerle.

Obiettivi e contenuti dell'analisi

L'analisi del mercato del lavoro locale ha quattro obiettivi principali che si integrano tra loro.

Comprendere le tendenze locali: identificare la direzione in cui si muove l'occupazione nell'area — quali settori stanno crescendo, quali sono in contrazione, quali nuove professioni emergono — per anticipare le opportunità invece di rincorrerle.

Identificare domanda e offerta di lavoro: analizzare da un lato quante e quali persone sono disponibili a lavorare, con quali competenze e aspettative; dall'altro quante e quali imprese stanno cercando lavoratori, per quali ruoli e con quali requisiti. Il mismatch — il disallineamento — tra domanda e offerta è uno dei principali problemi del mercato del lavoro italiano, e riconoscerlo aiuta a capire dove investire nella propria formazione.

Individuare le aree in crisi e le nuove opportunità: non tutti i settori e non tutte le zone geografiche di un territorio si muovono allo stesso modo. Alcune aree soffrono di spopolamento e declino economico, altre stanno vivendo una fase di crescita inaspettata. Identificare questo differenziale è fondamentale per chi deve prendere decisioni su dove vivere, dove lavorare, dove investire.

Supportare lo sviluppo locale: le informazioni prodotte dall'analisi del mercato del lavoro non sono utili solo ai singoli cittadini: informano le scelte degli enti locali, delle scuole di formazione, delle associazioni di categoria. Capire come queste decisioni vengono prese – e su quali dati si basano – aiuta anche a partecipare più consapevolmente ai processi di sviluppo del proprio territorio.

I contenuti specifici dell'analisi includono: tassi di occupazione, disoccupazione e inattività; analisi delle assunzioni e delle cessazioni per settore; mappatura della segregazione di genere nel mercato del lavoro, cioè la distribuzione disomogenea di uomini e donne in certi settori e livelli gerarchici; flussi di manodopera, inclusa l'immigrazione, che in molte aree del Sud Italia costituisce una componente importante del lavoro stagionale e agricolo.

Gli strumenti usati per questo tipo di analisi sono gli Osservatori del Mercato del Lavoro – OML – presenti in ogni Regione, le indagini statistiche periodiche, i report elaborati dai Centri per l'Impiego e le banche dati pubbliche. In Campania, l'Osservatorio del Mercato del Lavoro della Regione Campania produce report regolari accessibili online, con dati disaggregati per provincia e per settore.

Gli strumenti di analisi e statistica

Gli strumenti di analisi e statistica sono applicazioni software e metodologie che permettono di raccogliere, elaborare, interpretare e visualizzare grandi quantità di dati, trasformandoli da numeri grezzi in informazioni utili per prendere decisioni. Esistono strumenti di diversa complessità, adatti a diversi livelli di competenza.

Software di fogli di calcolo (livello base): Microsoft Excel e Google Sheets sono i più diffusi e accessibili. Permettono di organizzare dati in tabelle, eseguire calcoli, creare grafici e tabelle pivot per riassumere informazioni. Per chi si avvicina per la prima volta all'analisi dei dati, sono il punto di partenza ideale: Google Sheets è gratuito e accessibile da qualsiasi browser.

Business Intelligence (BI) e visualizzazione: Tableau e Microsoft Power BI sono strumenti professionali per creare dashboard interattive, cruscotti vivaci che mostrano in tempo reale le performance e i trend. Sono usati dalle

aziende per monitorare i KPI – Key Performance Indicators – e rendere i dati comprensibili anche a chi non ha formazione tecnica.

Linguaggi di programmazione: Python e R sono i linguaggi più usati per analisi statistiche complesse, manipolazione di grandi quantità di dati e data science. Richiedono una curva di apprendimento più ripida, ma offrono potenza e flessibilità che nessun altro strumento può eguagliare. Sono la scelta di riferimento per i professionisti dell'analisi dati.

Software statistici avanzati: SPSS e SAS sono tradizionalmente usati nella ricerca accademica e clinica per analisi statistiche sofisticate: regressioni, analisi multivariate, test di ipotesi. Sono potenti ma richiedono formazione specifica.

Database: BigQuery, sviluppato da Google, permette di gestire e interrogare grandi volumi di dati in modo molto rapido. È lo strumento di riferimento per chi lavora con dati su scala molto grande.

Per iniziare: Non è necessario padroneggiare tutti questi strumenti. Per chi si avvicina all'analisi dei dati del mercato del lavoro, Google Sheets offre già potenzialità molto ampie ed è completamente gratuito. Il passo successivo, per chi vuole approfondire, è imparare le basi di Python (ci sono ottimi corsi gratuiti online su piattaforme come Coursera, edX e Google Digital Garage).

Come interpretare i dati ISTAT

L'ISTAT – Istituto Nazionale di Statistica – è la principale fonte ufficiale di dati statistici sull'economia e la società italiana. I suoi dati sono pubblici, gratuiti e accessibili online attraverso il portale istat.it. Imparare a orientarsi in questo portale è una competenza preziosissima per chiunque voglia capire le dinamiche del mercato del lavoro.

I dati ISTAT più rilevanti per il mercato del lavoro sono organizzati in tre grandi pubblicazioni periodiche. La Rilevazione sulle Forze di Lavoro viene pubblicata mensilmente e monitora mese per mese i tassi di occupazione, disoccupazione e inattività della popolazione italiana, disaggregati per sesso, età, area geografica e livello di istruzione. È la fotografia più aggiornata dello stato del mercato del lavoro.

Il Rapporto Annuale ISTAT è una pubblicazione più ampia che offre il quadro strutturale delle trasformazioni sociali e lavorative del paese: non solo i numeri del momento, ma le tendenze di medio e lungo periodo, le trasformazioni demografiche, l'evoluzione dei settori produttivi. È una lettura fondamentale

per chi vuole capire dove sta andando il mercato del lavoro nei prossimi anni.

Il Rapporto sulla Competitività dei Settori Produttivi analizza le performance dei diversi comparti dell'economia italiana, confrontandole con i competitor europei e internazionali. È particolarmente utile per chi vuole capire quali settori italiani sono in crescita, quali stanno perdendo terreno e dove ci sono margini di sviluppo.

I dati più recenti – fine 2024 e inizio 2026 – mostrano alcune tendenze chiare nel mercato del lavoro italiano. La crescita è trainata prevalentemente dal settore dei servizi – turismo, logistica, sanità, istruzione, tecnologie dell'informazione – mentre il manifatturiero tradizionale continua la sua trasformazione verso modelli più automatizzati e ad alta intensità di conoscenza. I contratti a tempo indeterminato mostrano una certa stabilizzazione rispetto al periodo post-pandemia. La spinta verso competenze digitali e green è trasversale a tutti i settori: qualsiasi impresa, in qualsiasi settore, ha bisogno di personale con competenze digitali di base e di una sensibilità crescente verso la sostenibilità ambientale.

MAPPATURA DELLE RISORSE LOCALI: NATURALI, UMANE E DIGITALI

Obiettivi del modulo

Al termine di questo modulo saprai identificare e valorizzare le risorse naturali e umane del tuo territorio. Conoscerai i principali strumenti GIS e le piattaforme online per analizzare e visualizzare le risorse territoriali. Comprenderai come queste risorse costituiscono la base per lo sviluppo economico locale e per la creazione di opportunità lavorative.

Perché mappare le risorse del territorio

L'identificazione e la valorizzazione delle risorse naturali e umane sono fondamentali per lo sviluppo sostenibile e la competitività territoriale, in particolare nelle aree rurali e agricole. Queste risorse costituiscono la base per la creazione di valore economico e per l'implementazione di modelli di impresa agricola multifunzionale.

Ma cosa si intende esattamente per 'risorse del territorio'? Il concetto è più ampio di quanto si possa pensare. Non riguarda solo le materie prime fisiche (i terreni, l'acqua, il paesaggio) ma anche il capitale umano (le competenze, le tradizioni, le reti di relazione) e il capitale sociale (la capacità di una comunità di cooperare, di fare sistema, di costruire progetti condivisi). Un territorio che non valorizza queste risorse – o che non sa nemmeno di possederle – perde opportunità di sviluppo che altrimenti sarebbero disponibili.

Le risorse naturali

Le risorse naturali rappresentano le materie prime e i beni forniti direttamente dall'ambiente. Nelle aree interne della Campania – dove opera il progetto Digita Facile Campania – queste risorse sono spesso eccezionali ma sottovalutate o poco valorizzate.

Terreni agricoli: le superfici utilizzabili per produzioni vegetali o zootecniche, incluse le aree ad alto valore naturale. In Campania, la varietà climatica e pedologica consente produzioni di eccellenza in settori molto diversi: dalla Mozzarella di Bufala Campana DOP alla Colatura di Alici di Cetara, dal Provolone del Monaco al Limoncello di Sorrento. La mappatura digitale dei suoli agricoli – disponibile attraverso i portali dell'AGEA, Agenzia per le Erogazioni in Agricoltura – permette di identificare le zone più adatte a specifiche colture e di accedere ai relativi finanziamenti europei.

Risorse idriche: l'acqua disponibile in superficie (fiumi, laghi, torrenti) e nel sottosuolo (acquiferi) è fondamentale non solo per l'irrigazione, che consuma circa il 70% dell'acqua dolce disponibile a livello mondiale, ma anche per il so-

stentamento degli ecosistemi, per il turismo naturalistico e per alcune produzioni alimentari che dipendono dalla qualità dell'acqua locale.

Biodiversità e suolo: la flora, la fauna e le caratteristiche pedologiche del suolo sostengono l'attività agricola e costituiscono risorse per il turismo naturalistico e scientifico. La Campania ospita tre parchi nazionali (Cilento, Vallo di Diano e Alburni; Vesuvio; Alta Murgia) che rappresentano sia una responsabilità di conservazione che un'opportunità economica significativa per le comunità locali.

Le risorse umane

Le risorse umane rappresentano il valore delle persone che vivono e lavorano in un territorio: le loro conoscenze, le loro abilità, le loro esperienze e le loro reti di relazione. In molte analisi dello sviluppo locale, le risorse umane sono sottostimate rispetto a quelle naturali e infrastrutturali, ma spesso sono quelle determinanti.

Competenze locali: il know-how tradizionale e i saperi legati alle produzioni tipiche (la vinificazione, la caseificazione, la pesca artigianale, la lavorazione della ceramica, le ricette della cucina tradizionale) sono risorse economiche di enorme valore nel contesto della crescente domanda di autenticità, di esperienze genuine, di prodotti artigianali con una storia. Il problema è che spesso queste competenze vengono percepite come 'vecchie' e non come patrimonio da valorizzare nel mercato contemporaneo.

Manodopera: la forza lavoro disponibile sul territorio — inclusi i familiari degli imprenditori agricoli ai sensi dell'art. 230-bis del codice civile e i lavoratori dipendenti, stagionali o a tempo indeterminato — è una risorsa che cambia nel tempo. La mappatura della disponibilità e delle competenze della forza lavoro locale è fondamentale per le imprese che vogliono crescere e per le politiche di sviluppo locale.

Capitale sociale: la capacità di cooperazione e le reti di relazioni locali che favoriscono lo sviluppo. Un territorio con un alto capitale sociale — dove ci si fida degli altri, dove le reti associative funzionano, dove le istituzioni locali e i cittadini collaborano — ha un vantaggio competitivo significativo rispetto a territori frammentati e sfiduciati. Il capitale sociale non si vede nei dati statistici, ma si sente nei territori che riescono a fare sistema.

Gli strumenti GIS per la mappatura del territorio

I GIS — Geographic Information Systems, Sistemi Informativi Geografici — sono strumenti software che permettono di raccogliere, elaborare, analizzare e visualizzare dati geograficamente riferiti: cioè dati associati a una posizione

nello spazio. In parole semplici, permettono di rispondere a domande come ‘cosa c’è in questo territorio?’ e ‘dove si trovano le risorse che mi interessano?’ attraverso mappe interattive e analisi spaziali.

ArcGIS (Esri): è la piattaforma leader a livello mondiale per la cartografia professionale e l’analisi spaziale. Offre sia una versione desktop installabile che ArcGIS Online, una versione web che non richiede installazione e permette di creare mappe interattive direttamente nel browser. Molte amministrazioni pubbliche italiane usano ArcGIS per la gestione del territorio.

QGIS: è un software GIS desktop open source e gratuito, ampiamente utilizzato nella pubblica amministrazione, nella ricerca e dal terzo settore. Offre funzionalità paragonabili a quelle dei software commerciali e ha una comunità di utenti molto attiva che produce documentazione, tutorial e plugin.

WebGIS e piattaforme online: strumenti che permettono la pubblicazione e la consultazione di dati geografici via browser, senza installare alcun software. UrbisMap è un portale italiano che offre dati sui comuni italiani; Leaflet è una libreria JavaScript per creare mappe interattive su siti web. Molti enti locali campani stanno sviluppando portali WebGIS per rendere accessibili al pubblico i dati territoriali.

Google Earth Pro: disponibile gratuitamente, permette di visualizzare immagini satellitari aggiornate, sovrapporre dati geografici in formato KML/KMZ, misurare distanze e superfici. È uno strumento accessibile a tutti e molto utile per una prima analisi visiva del territorio.

Come usarli concretamente: Per chi si avvicina al GIS per la prima volta, Google Earth Pro è il punto di partenza ideale – è gratuito, intuitivo e permette di esplorare il territorio con immagini satellitari di alta qualità. Il passo successivo è QGIS, che offre funzionalità molto più avanzate restando completamente gratuito.

SETTORI PRODUTTIVI EMERGENTI: LE OPPORTUNITÀ DEL FUTURO

Obiettivi del modulo

Al termine di questo modulo comprenderai come le innovazioni tecnologiche stanno trasformando i settori produttivi esistenti e creando settori nuovi. Conoscerai le caratteristiche e le opportunità lavorative dei tre settori emergenti più rilevanti per il territorio campano: turismo sostenibile ed esperienziale, agricoltura biologica e di precisione, tecnologie ecologiche green tech.

Le innovazioni tecnologiche che stanno ridisegnando il lavoro

Le innovazioni tecnologiche attuali stanno trasformando radicalmente imprese e società, guidando quella che viene chiamata la transizione digitale e sostenibile. Non si tratta di un cambiamento graduale: è una trasformazione rapida e pervasiva che riguarda tutti i settori, dalle industrie tradizionali alle professioni più consolidate.

Le tecnologie più trasformative in questo momento sono l'intelligenza artificiale – in particolare i nuovi modelli di AI generativa e i sistemi AI agentici, capaci di agire in modo autonomo per completare compiti complessi – il cloud computing, che ha reso accessibili a piccole imprese e individui risorse computazionali che in passato erano riservate alle grandi organizzazioni; la blockchain, che permette transazioni sicure e trasparenti senza intermediari; e la stampa 3D, che sta rivoluzionando la produzione manifatturiera consentendo la fabbricazione su domanda e la personalizzazione estrema.

L'innovazione si divide tradizionalmente in incrementale – il miglioramento progressivo di tecnologie esistenti, che produce cambiamenti gradualmente e prevedibili – e radicale – l'introduzione di tecnologie completamente nuove che cambiano le regole del gioco in un settore. Internet e gli smartphone sono esempi storici di innovazione radicale: hanno trasformato completamente il modo in cui le persone lavorano, si informano e si relazionano. L'AI generativa e la transizione energetica sono probabilmente le innovazioni radicali del nostro momento.

Turismo sostenibile ed esperienziale

Il turismo è uno dei settori più importanti per l'economia campana e uno di quelli che sta vivendo la trasformazione più significativa. Il modello del turismo di massa – grandi numeri, prezzi bassi, impatto ambientale elevato, benefici economici concentrati in poche strutture – sta cedendo il posto a un modello molto diverso, più rispettoso dell'ambiente e delle culture locali, ma anche economicamente più sostenibile nel lungo periodo.

Il turismo rigenerativo è la nuova frontiera: un approccio che non si limita a minimizzare l'impatto negativo del turismo, ma aspira a lasciare i luoghi visi-

tati in condizioni migliori di come li ha trovati. Si concretizza in pratiche come il ripristino di sentieri e paesaggi, il sostegno alle comunità locali, la valorizzazione delle tradizioni artigianali, la promozione di prodotti alimentari locali.

Turismo lento e cammini: la valorizzazione di percorsi pedonali e rurali – cammini storici, vie di pellegrinaggio, sentieri naturalistici – sta generando una domanda crescente di agriturismi e strutture di ospitalità diffusa che offrano esperienze autentiche. La Via Silente, il Cammino di San Nilo, i percorsi del Cilento: sono esempi campani di prodotti turistici che attraggono un visitatore con alta disponibilità di spesa, basso impatto ambientale e alto indice di soddisfazione.

Mobilità sostenibile: l'integrazione di mezzi di trasporto a basso impatto ambientale – biciclette elettriche, shuttle elettrici, ferrovie locali – è un elemento chiave per rendere accessibili aree remote mantenendone il carattere. Il cicloturismo è uno dei segmenti a più alta crescita nel turismo europeo.

Certificazioni eco: la sostenibilità sta diventando una 'infrastruttura' del viaggio: il turista attento cerca strutture certificate, prodotti tracciabili, esperienze che dimostrino un impegno reale verso la sostenibilità, non solo dichiarazioni di facciata. Le certificazioni come il Marchio del Parco, l'Ecolabel europeo e le varie certificazioni di sostenibilità turistica sono strumenti di marketing potenti nel mercato contemporaneo.

Agricoltura biologica e di precisione

L'Italia è il paese europeo leader per superficie coltivata a biologico: oltre 2,5 milioni di ettari – il 20,2% della superficie agricola totale nazionale – contro una media europea dell'11,2%. Questo primato non è solo una questione di moda o di nicchia di mercato: riflette una trasformazione strutturale del settore agricolo italiano verso modelli più sostenibili, più remunerativi e più resistenti alle crisi.

Rivoluzione bio: il settore biologico continua a crescere sia in termini di superfici che di fatturato. Le opportunità non riguardano solo la produzione primaria, ma anche la trasformazione, la distribuzione e la commercializzazione dei prodotti. L'economia circolare – che riduce gli sprechi riutilizzando gli scarti di produzione – e la valorizzazione dei prodotti locali attraverso i mercati contadini, la GAS – Gruppi di Acquisto Solidale – e i canali di vendita diretta stanno creando nuovi modelli di business sostenibili.

Agritech e AI: l'intelligenza artificiale e l'agricoltura di precisione stanno trasformando il modo in cui si coltiva. Droni per il monitoraggio delle colture e la distribuzione mirata di fitofarmaci. Sensori IoT – Internet of Things – che misurano in tempo reale l'umidità del suolo, la temperatura, la presenza di parassiti. Sistemi GPS per la guida automatizzata dei macchinari agricoli. Que-

sti strumenti permettono di ottimizzare l'uso delle risorse – acqua, concimi, energia – riducendo i costi e l'impatto ambientale mentre aumentano la produttività.

Nuove tecniche genomiche: il dibattito e la ricerca sulle nuove tecniche genomiche – NGT, New Genomic Techniques – offrono prospettive molto interessanti per sviluppare varietà vegetali più resistenti alla siccità, alle malattie e ai parassiti, più adatte ai cambiamenti climatici in atto, con migliori profili nutrizionali. È un campo in rapida evoluzione, con importanti implicazioni sia scientifiche che normative.

Tecnologie ecologiche (Green Tech)

La sostenibilità ambientale non è più un'opzione o un valore aggiunto: è diventata un elemento centrale delle strategie aziendali e delle politiche pubbliche. Questo cambiamento sta creando un settore economico completamente nuovo – le tecnologie ecologiche o green tech – con opportunità occupazionali in forte crescita.

Gestione energetica: le piattaforme di gestione dell'energia e le tecnologie per ridurre l'impronta di carbonio sono in forte espansione. Le comunità energetiche rinnovabili – CER – sono un fenomeno nuovo e in rapida crescita anche in Campania: gruppi di cittadini, imprese e amministrazioni locali che producono e condividono energia rinnovabile, riducendo i costi e aumentando l'indipendenza energetica. Creare o gestire una CER è una competenza professionale molto richiesta.

Economia circolare: il principio dell'economia circolare – riduci, riusa, ricicla – sta trasformando i modelli di produzione e consumo. Con l'avvento dell'European Circular Economy Act – atteso per il 2026 – si apriranno nuove opportunità nel riciclo e nel riutilizzo dei materiali, nella progettazione di prodotti concepiti fin dall'inizio per essere riparati, riutilizzati o riciclati.

Soluzioni basate sulla natura: gli investimenti in quelle che vengono chiamate 'nature-positive solutions' – come il ripristino di ecosistemi degradati, l'agricoltura rigenerativa, il rewilding di aree abbandonate – sono al centro delle politiche ambientali europee. Queste soluzioni creano benefici multipli: mitigazione del cambiamento climatico, biodiversità, qualità dell'acqua, prevenzione delle alluvioni, turismo naturalistico.

LE OPPORTUNITÀ DEL TUO TERRITORIO

Un modulo personalizzato per ogni luogo

Il Modulo 4 è strutturalmente diverso dagli altri: non ha contenuti fissi, ma è progettato per essere personalizzato in base al luogo specifico in cui si svolge il corso. Ogni territorio ha la sua storia, le sue risorse, i suoi punti di forza e le sue sfide. Un'analisi delle opportunità che non tiene conto di queste specificità rischia di essere inutile o addirittura fuorviante.

Nelle aree interne della Campania, dove si concentra la maggior parte delle attività del progetto Digita Facile Campania, le specificità territoriali sono molto marcate. Alcuni comuni del Cilento hanno caratteristiche completamente diverse da quelli dell'Irpinia o del Sannio. Le risorse produttive, le tradizioni culturali, le infrastrutture disponibili, i flussi turistici, la struttura demografica: tutti questi elementi variano significativamente da un'area all'altra e devono essere analizzati con strumenti e dati localizzati.

Come fare un'analisi delle opportunità del proprio territorio

Anche senza una formazione specifica in economia locale, è possibile fare un'analisi utile delle opportunità del proprio territorio combinando fonti diverse e alcune domande guida.

Il punto di partenza sono i dati demografici: quante persone vivono nel territorio? La popolazione sta crescendo o calando? Qual è la struttura per età? Un territorio con una popolazione anziana e in calo avrà bisogno di certi servizi e offrirà certe opportunità; uno con una popolazione giovane e in crescita offrirà opportunità molto diverse. I dati demografici comunali sono disponibili gratuitamente sul portale ISTAT Tuttitalia.it.

Il secondo passo è l'analisi del tessuto produttivo: quali imprese esistono nel territorio? Quali settori sono rappresentati? Ci sono grandi imprese o prevalgono le piccole e medie? Le imprese locali assumono o hanno difficoltà a trovare personale? Molte di queste informazioni sono disponibili nelle Camere di Commercio locali, che pubblicano report periodici sullo stato dell'economia provinciale.

Il terzo elemento è la mappatura delle risorse naturali e culturali: quali sono le bellezze naturali del territorio? Quali sono le produzioni tipiche, le tradizioni artigianali, i monumenti storici, i paesaggi distintivi? Queste risorse sono già valorizzate, o c'è margine di sviluppo? I Parchi Nazionali e Regionali, le Pro Loco, le associazioni culturali locali sono fonti preziose di informazioni.

Il quarto elemento è l'analisi delle infrastrutture: come è collegato il territo-

rio? Ci sono problemi di mobilità, di connettività digitale, di accesso ai servizi? Queste carenze rappresentano spesso anche opportunità: chi riesce a portare servizi in un'area carente può trovare un mercato non conteso.

Strumento pratico: Il portale **OpenCoesione** opencoessione.gov.it permette di vedere i finanziamenti pubblici europei, nazionali e regionali investiti nel proprio comune, con i dettagli sui progetti finanziati, le somme erogate e lo stato di avanzamento. È uno strumento eccellente per capire dove sta andando il denaro pubblico nel proprio territorio e quali progetti sono in corso.

Obiettivi del modulo

Al termine di questo modulo conoscerai le fasi principali del processo di creazione di una start-up, dalla valutazione dell'idea alla pianificazione strategica. Saprai orientarti nel panorama dei finanziamenti disponibili per le nuove imprese, inclusi gli incentivi statali, le fonti private e i programmi europei. Comprenderai l'importanza del marketing, del monitoraggio e del networking per il successo di un'impresa nascente.

Cosa è una start-up e perché è diversa da un'impresa tradizionale

Il termine 'start-up' viene spesso usato come sinonimo di piccola impresa tecnologica, ma il concetto è più preciso e più interessante. Una start-up è un'organizzazione temporanea alla ricerca di un modello di business scalabile e ripetibile. L'elemento chiave è la scalabilità: a differenza di un'impresa tradizionale che cresce linearmente con l'aggiunta di risorse, una start-up aspira a trovare un modello che possa crescere esponenzialmente senza un proporzionale aumento dei costi.

Non tutte le nuove imprese sono start-up nel senso tecnico del termine. Aprire un ristorante è creare una piccola impresa, non una start-up: la crescita è necessariamente lineare, in quanto per servire più clienti, bisogna avere più tavoli e più personale. Sviluppare un'app o un servizio digitale che può servire milioni di utenti con costi marginali vicini allo zero è invece un modello start-up classico.

Ma il pensiero da start-up, che prevede la ricerca metodica di un modello di business innovativo, il test rapido delle ipotesi, l'adattamento continuo in risposta ai feedback del mercato, è applicabile anche in settori tradizionali. Un'azienda agricola che sviluppa un modello di vendita diretta online, una struttura turistica che crea un'esperienza unica e replicabile, un artigiano che digitalizza la propria distribuzione: tutti stanno applicando una logica start-up ai settori tradizionali.

Le fasi del processo di creazione

Creare una start-up è un processo che richiede pianificazione, strategia e capacità di esecuzione. Non esiste un percorso universale, ma alcune fasi sono comuni a quasi tutte le esperienze di successo.

Valuta il mercato: prima di investire tempo e risorse in un'idea, è fondamentale analizzare se esiste una domanda reale per ciò che si vuole offrire. Chi sono i potenziali clienti? Quanti sono? Quanto sarebbero disposti a pagare? Esistono già soluzioni alternative? Come si differenzia la propria idea da quelle

già disponibili? Questa fase richiede ricerca, con sondaggi, interviste, analisi della concorrenza, nonché onestà intellettuale: è meglio scoprire precocemente che un'idea non ha mercato che investirci risorse ingenti.

Pianificazione: il business plan è il documento che traduce un'idea imprenditoriale in un piano operativo: analisi del mercato e della concorrenza, descrizione del prodotto o servizio, strategia di marketing e comunicazione, struttura organizzativa, proiezioni finanziarie. Non deve essere un documento rigido e immutabile — le migliori start-up modificano continuamente il loro piano in risposta all'esperienza — ma è uno strumento essenziale per chiarire il pensiero, comunicare la proposta agli investitori e identificare i nodi critici da risolvere.

Formazione del team: le start-up di successo raramente sono creazioni di un singolo individuo. Trovare cofondatori e collaboratori che condividano la visione ma abbiano competenze complementari è uno dei passaggi più critici. Un team con competenze diversificate come tecniche, commerciali, creative, operative è molto più resiliente e capace di affrontare le sfide inevitabili del percorso imprenditoriale.

Finanziamenti: la questione dei finanziamenti è spesso percepita come l'ostacolo principale, ma il panorama delle risorse disponibili è molto più ricco di quanto molti pensino. Gli incentivi statali includono contributi a fondo perduto — cioè denaro che non deve essere restituito — agevolazioni fiscali, finanziamenti agevolati a tassi ridotti e voucher per l'innovazione. Invitalia gestisce molti di questi programmi a livello nazionale. A livello regionale, la Regione Campania ha programmi specifici per start-up innovative e imprenditorialità giovanile.

Le fonti di finanziamento private includono: il Venture Capital, fondi di investimento specializzati in aziende ad alto potenziale di crescita; gli Angel Investor, investitori individuali che finanziano start-up nelle fasi iniziali in cambio di quote azionarie; il Crowdfunding, raccolta di piccoli contributi da molte persone attraverso piattaforme online; gli Incubatori e Acceleratori, organizzazioni che offrono spazi di lavoro, mentorship e connessioni in cambio di quote azionarie; i Prestiti bancari con garanzia pubblica.

I programmi europei offrono opportunità enormi, spesso sottoutilizzate: Horizon Europe, il programma per la ricerca e l'innovazione con un budget di oltre 95 miliardi di euro e COSME, il programma per la competitività delle PMI, sono i più rilevanti per le start-up e le piccole imprese innovative.

Marketing e vendite: un prodotto eccellente senza visibilità non raggiunge i clienti. Sviluppare un piano marketing che includa branding (l'identità visiva e valoriale dell'impresa) relazioni pubbliche, ottimizzazione per i motori di ricerca SEO, social media e pubblicità è essenziale. La scelta dei canali di vendita più appropriati, ossia online, retail, partnership con altre imprese, dipende dalle caratteristiche del prodotto e del cliente target.

Lancio: l'introduzione sul mercato è un momento cruciale che richiede preparazione. Una campagna di lancio efficace crea aspettativa, genera copertura mediatica e attira i primi clienti. I primi clienti sono preziosi non solo per il fatturato, ma per i feedback che forniscono e per l'effetto di credibilità che producono – i clienti acquisiti possono diventare ambasciatori dell'impresa.

Monitoraggio e adattamento: il monitoraggio continuo delle performance attraverso KPI (Key Performance Indicators) è la base per le decisioni informate. Quali metriche contano davvero dipende dal modello di business: per un e-commerce potrebbero essere il tasso di conversione dei visitatori in acquirenti; per un servizio in abbonamento, il tasso di churn, ossia quanti clienti si cancellano ogni mese. La volontà di modificare la strategia in risposta ai dati e ai feedback dei clienti è una delle competenze più preziose di un imprenditore.

Networking e supporto: la comunità imprenditoriale è un asset fondamentale. Trovare mentori, imprenditori esperti che abbiano già percorso quel cammino e possano offrire consigli basati sull'esperienza, è uno dei passi più utili che si possano fare. Partecipare a eventi, conferenze e incontri di settore non solo per costruire visibilità, ma per creare relazioni con potenziali partner, clienti, investitori e collaboratori.

L'imprenditoria nelle aree interne: sfide e opportunità specifiche

Creare un'impresa nelle aree interne della Campania ha sfide specifiche: minor accessibilità, minor densità di servizi, mercati locali più piccoli. Ma ha anche opportunità che non esistono nei grandi centri urbani.

Il costo dei fattori produttivi è generalmente più basso: affitti degli spazi, costo della manodopera, costo della vita. C'è meno concorrenza in molti settori, ragione per cui chi apre una struttura turistica di qualità in un'area rurale poco frequentata trova meno competitor di chi si posiziona in una città turistica saturata. La disponibilità di risorse naturali, culturali e agroalimentari di eccellenza crea possibilità di differenziazione molto forte nel mercato.

Il digitale ha poi ridotto molte delle barriere legate alla distanza. Un artigiano dell'Irpinia può vendere i propri prodotti a Londra attraverso Etsy o il proprio sito e-commerce. Un agriturismo nel Cilento può raggiungere clienti in tutta

Europa attraverso Airbnb e Booking. Un professionista delle aree interne può lavorare per clienti globali in smartworking. La distanza fisica conta sempre meno; la qualità del prodotto, dell'esperienza e della comunicazione conta sempre di più.

La scelta più importante non è dove si vuole arrivare: è dove si vuole iniziare. Analizza le risorse del territorio in cui vivi, identifica le opportunità non sfruttate, e costruisci la tua idea di impresa partendo da ciò che il territorio ti offre. Il vantaggio competitivo più solido è quello costruito su radici autentiche.

Riepilogo dei concetti fondamentali

Questo percorso ha costruito una comprensione pratica e operativa delle opportunità del territorio, partendo dall'analisi del mercato del lavoro locale per arrivare all'ideazione di una propria impresa.

L'analisi del mercato del lavoro locale — con gli strumenti ISTAT e gli Osservatori regionali — permette di capire le tendenze occupazionali, identificare i settori in crescita e in contrazione, e prendere decisioni più informate sulla propria carriera e formazione. I dati indicano una crescita trainata dai servizi, una spinta sistemica verso le competenze digitali e green, e una stabilizzazione dei contratti a tempo indeterminato.

La mappatura delle risorse territoriali (naturali, umane e digitali) è la base per identificare le opportunità di sviluppo specifiche di ogni area. Le risorse naturali di molte aree campane, tra cui terreni agricoli di eccellenza, biodiversità, paesaggio, sono spesso sotto-valorizzate rispetto al loro potenziale. Le risorse umane (competenze tradizionali, capitale sociale, know-how artigianale) sono altrettanto preziose. Gli strumenti GIS permettono di analizzare e visualizzare queste risorse in modo sistematico. I tre settori produttivi emergenti più rilevanti per il territorio campano sono il turismo sostenibile ed esperienziale, che risponde alla crescente domanda di autenticità e di esperienze rigenerative; l'agricoltura biologica e di precisione, in cui l'Italia è leader europeo e la tecnologia Agritech crea nuove efficienze; le tecnologie ecologiche green tech, che trasformano la sostenibilità da costo a opportunità economica.

Il processo di creazione di una start-up richiede pianificazione, capacità di esecuzione e adattamento continuo. Le fasi fondamentali, tra cui valutazione del mercato, business plan, formazione del team, finanziamenti, marketing, lancio e monitoraggio, si applicano a qualsiasi tipo di impresa, sia tecnologica che tradizionale. Le risorse disponibili, incentivi statali, fonti private, programmi europei, sono molto più numerose di quanto molti credano.

Non vi resta che analizzare attentamente le opportunità disponibili e scegliere quelle più adatte al vostro settore d'interesse e al vostro business. Il territorio campano offre risorse straordinarie: sta a ciascuno di voi trasformarle in opportunità concrete.

Test di autovalutazione

Indica la risposta corretta. Le risposte si trovano in fondo alla sezione.

1. L'analisi del mercato del lavoro locale serve principalmente a: a) Produrre statistiche accademiche sul lavoro. b) Comprendere le tendenze occupazionali locali, identificare domanda e offerta di lavoro e supportare lo sviluppo locale. c) Gestire i procedimenti amministrativi dei Centri per l'Impiego.
2. Quale strumento di analisi dei dati è gratuito e accessibile direttamente dal browser senza installazione? a) SPSS. b) Google Sheets. c) SAS.
3. I dati ISTAT sulla Rilevazione delle Forze di Lavoro vengono pubblicati: a) Una volta all'anno nel Rapporto Annuale. b) Ogni trimestre. c) Mensilmente, con dati su occupazione, disoccupazione e inattività.
4. Quale percentuale della superficie agricola italiana è coltivata a biologico? a) 5%. b) 11,2% (la media europea). c) 20,2%, il che rende l'Italia leader europeo nel biologico.
5. Cos'è un GIS? a) Un tipo di contratto di lavoro europeo. b) Un sistema informatico per raccogliere, analizzare e visualizzare dati geograficamente riferiti. c) Una piattaforma per la vendita di prodotti agricoli online.
6. Nell'economia circolare, qual è il principio fondamentale? a) Massimizzare la produzione per ridurre i costi unitari. b) Esportare i rifiuti industriali in paesi con normative meno stringenti. c) Ridurre gli sprechi riutilizzando e riciclando i materiali, progettando prodotti pensati per durare e per essere riparati.
7. Cos'è il capitale sociale di un territorio? a) Il valore degli immobili del territorio. b) La capacità di cooperazione e le reti di relazioni locali che favoriscono lo sviluppo. c) Il totale degli investimenti pubblici nel territorio.
8. Quale programma europeo finanzia la ricerca e l'innovazione ed è rilevante per le start-up? a) COSME. b) Horizon Europe. c) Entrambi sono rilevanti ma per finalità diverse: Horizon Europe per ricerca e innovazione, COSME per la competitività delle PMI.

Autovalutazione delle competenze DigComp 2.2

Compila questa scheda prima e dopo il percorso formativo. Indica il tuo livello su una scala da 1 a 5: 1 = non mi sento ancora in grado, 5 = mi sento completamente autonomo.

Area di Competenza	Prima (1-5)	Dopo (1-5)
So identificare le risorse naturali e umane del mio territorio		
Ho familiarità con strumenti GIS di base (es. Google Earth Pro)		
Conosco le caratteristiche dei principali settori produttivi emergenti		
Capisco le fasi del processo di creazione di una start-up		
Conosco le principali fonti di finanziamento per nuove imprese		
Riconosco le opportunità specifiche del mio territorio		
Mi sento in grado di progettare un percorso professionale o imprenditoriale autonomo		

Glossario essenziale

Agritech: insieme di tecnologie applicate all'agricoltura – droni, sensori IoT, GPS, intelligenza artificiale – per ottimizzare la produzione, ridurre i consumi e aumentare la sostenibilità.

Angel Investor: investitore individuale che finanzia start-up nelle fasi iniziali in cambio di quote azionarie, portando non solo denaro ma anche esperienza e reti di contatti.

Business Intelligence (BI): strumenti software per la raccolta, l'analisi e la visualizzazione di dati aziendali attraverso dashboard interattive, usati per supportare le decisioni strategiche.

Business Plan: documento che descrive la strategia di un'impresa nascente: analisi del mercato, descrizione del prodotto/servizio, piano di marketing, struttura organizzativa e proiezioni finanziarie.

Capitale sociale: risorsa intangibile di un territorio: la capacità di cooperazione, la fiducia reciproca e le reti di relazioni tra individui, imprese e istituzioni che facilitano lo sviluppo economico.

COSME: programma europeo per la Competitività delle PMI, che offre garanzie sui prestiti, accesso a fondi di rischio e supporto all'internazionalizzazione per le piccole e medie imprese.

Crowdfunding: raccolta di fondi da molte persone attraverso piattaforme online, in cambio di prodotti, servizi, quote azionarie o semplicemente a titolo di donazione.

DigComp 2.2: quadro europeo delle competenze digitali per i cittadini, sviluppato dalla Commissione Europea. Definisce le competenze digitali fondamentali organizzate in cinque aree: alfabetizzazione su informazioni e dati; comunicazione e collaborazione; creazione di contenuti digitali; sicurezza; risoluzione di problemi.

Economia circolare: modello economico che mira a eliminare gli sprechi attraverso la progettazione di prodotti destinati a essere riutilizzati, riparati e riciclati, in alternativa al modello lineare 'produci-usa-getta'.

GIS (Geographic Information System): sistema informatico per raccogliere, gestire, analizzare e visualizzare dati geograficamente riferiti, cioè associati a una posizione nello spazio.

Green Tech: settore delle tecnologie orientate alla sostenibilità ambientale: energie rinnovabili, efficienza energetica, economia circolare, gestione delle risorse idriche, mobilità sostenibile.

Horizon Europe: programma quadro dell'Unione Europea per la ricerca e l'innovazione con un budget di oltre 95 miliardi di euro per il periodo 2021-2027.

ISTAT: Istituto Nazionale di Statistica. Produce e pubblica statistiche ufficiali sull'economia, la società e il territorio italiano. I dati sono pubblici e accessibili gratuitamente su istat.it.

KPI (Key Performance Indicators): metriche quantitative usate per misurare il progresso verso gli obiettivi di un'impresa. La scelta dei KPI giusti dipende

dal modello di business specifico.

Mercato del lavoro locale: insieme delle dinamiche occupazionali in un'area geografica circoscritta: domanda e offerta di lavoro, tassi di occupazione e disoccupazione, settori produttivi presenti, fabbisogni professionali.

OML (Osservatorio del Mercato del Lavoro): struttura regionale che monitora e analizza le dinamiche occupazionali del territorio, producendo report e dati statistici accessibili al pubblico.

OpenCoesione: portale pubblico italiano — opencoessione.gov.it — che rende trasparenti i dati sui finanziamenti pubblici europei, nazionali e regionali investiti nei comuni e nelle regioni italiane.

Rilevazione sulle Forze di Lavoro (ISTAT): indagine mensile che monitora i tassi di occupazione, disoccupazione e inattività della popolazione italiana, disaggregati per sesso, età, area geografica e livello di istruzione.

Start-up: organizzazione temporanea alla ricerca di un modello di business scalabile e ripetibile, caratterizzata da alta innovazione, alto rischio e alto potenziale di crescita.

Venture Capital: fondi di investimento specializzati nel finanziamento di aziende ad alto potenziale di crescita, tipicamente nelle fasi di sviluppo successive al seed funding iniziale.

Risorse utili

ISTAT — Istituto Nazionale di Statistica: istat.it — per dati sul mercato del lavoro, statistiche regionali e provinciali, Rapporto Annuale.

OpenCoesione: opencoessione.gov.it — per la mappa dei finanziamenti pubblici nel proprio comune.

Invitalia: invitalia.it — agenzia nazionale per lo sviluppo che gestisce incentivi nazionali per start-up e PMI, inclusi Resto al Sud, Smart&Start e altri programmi.

Regione Campania — Sviluppo Economico: regione.campania.it — per bandi regionali, programmi di formazione e incentivi per la nuova imprenditorialità.

Camera di Commercio di Napoli: na.camcom.it — per dati sull'economia locale, servizi alle imprese e supporto alla creazione di nuove attività.

Horizon Europe: ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe — per i programmi di finanziamento europeo per la ricerca e l'innovazione.

Google Digital Garage: grow.google — corsi gratuiti di Google su competenze digitali, marketing online e analisi dei dati.

TEMA B
SICUREZZA E USO CONSAPEVOLE
DEI SERVIZI DIGITALI

 **CYBERBULLISMO ED ESCLUSIONE SOCIALE**



Digita Facile
Campania

Presentazione del capitolo

Questo capitolo accompagna il percorso formativo dedicato al tema Cyberbullismo ed Esclusione Sociale, sviluppato nell'ambito del progetto Digita Facile Campania. Si rivolge a chiunque voglia comprendere più a fondo un fenomeno che attraversa ogni fascia d'età, ogni ambiente sociale e ogni angolo della rete: il cyberbullismo e, più in generale, le dinamiche di aggressione, esclusione e violenza che si producono negli spazi digitali. Il percorso è articolato in cinque moduli. Il primo introduce le caratteristiche del cyberbullismo, distinguendolo dal bullismo tradizionale e illustrando i reati digitali correlati e i meccanismi psicologici che li alimentano. Il secondo analizza i ruoli degli attori coinvolti – vittima, bullo, spettatori – con particolare attenzione al potere trasformativo di chi assiste. Il terzo propone strumenti concreti per un uso etico della rete: la netiquette, la gestione della privacy, la difesa dal phishing e il pensiero critico come antidoto ai bias cognitivi. Il quarto fornisce un protocollo operativo per rispondere concretamente a episodi di cyberbullismo, con indicazioni sugli strumenti tecnologici di protezione e sul quadro normativo vigente. Il quinto, infine, pone al centro la cultura dell'inclusione e la responsabilità collettiva, con un toolkit di regole d'oro per un uso quotidiano consapevole della rete.

Questo non è un tema da affrontare con distacco accademico. È una questione che riguarda la vita reale di persone reali: adolescenti che abbandonano la scuola, adulti che perdono il lavoro a causa di contenuti diffusi senza consenso, anziani raggirati da truffe digitali. Comprendere questi fenomeni è il primo passo per contrastarli – come individui, come genitori, come educatori, come cittadini.

La rete non è un mondo parallelo: è il nostro mondo

Il digitale come spazio di vita, non solo di svago

Uno degli equivoci più pericolosi riguardo alla vita online è quello di considerarla una dimensione separata, parallela, meno reale della vita di tutti i giorni. “È solo internet” è la frase con cui si tende a minimizzare insulti, umiliazioni e violenze che avvengono attraverso schermi e tastiere. Ma questa distinzione è falsa, e le sue conseguenze possono essere devastanti. Le parole scritte in una chat, le foto condivise senza consenso, i commenti pubblicati sotto un post: questi atti producono effetti reali su persone reali. La vergogna, la paura, l'isolamento, la depressione che derivano dai fenomeni di cyberbullismo sono altrettanto reali quanto quelli prodotti da una violenza fisica. In alcuni casi, sono anche più duraturi, perché il contenuto digitale può restare accessibile per anni, rivivendo il danno ogni volta che viene trovato o ricondiviso.

Il digitale come estensione della responsabilità

Riconoscere che la rete non è un mondo separato significa anche riconoscere che le regole della convivenza civile – il rispetto, l’empatia, il consenso, la responsabilità per le proprie azioni – non si sospendono quando si entra online. Chi pubblica un contenuto offensivo, chi condivide una foto privata senza consenso, chi si unisce a una campagna di odio contro una persona reale sta compiendo atti con conseguenze reali, legalmente perseguibili e moralmente inaccettabili. Questa dispensa non intende soltanto informare sui rischi della rete: intende contribuire a costruire una cultura digitale in cui la responsabilità, l’empatia e il rispetto siano valori praticati online con la stessa naturalezza con cui si praticano, o si dovrebbero praticare, nella vita quotidiana.

COS'È IL CYBERBULLISMO: CARATTERISTICHE, REATI E MECCANISMI PSICOLOGICI

Obiettivi del modulo

Al termine di questo modulo saprai distinguere il cyberbullismo dal bullismo tradizionale attraverso le sue caratteristiche specifiche di pervasività, anonimato, risonanza pubblica e permanenza. Conoscerai i principali reati digitali correlati (revenge porn, cyberstalking, dissing) e le relative conseguenze legali. Saprai riconoscere le forme più comuni di aggressione online e comprenderai i meccanismi psicologici che trasformano un utente comune in un aggressore.

Dal bullismo al cyberbullismo: cosa cambia

Il bullismo esiste da sempre: è una forma di aggressione sistematica e intenzionale nei confronti di una persona più debole o percepita come tale. Il cyberbullismo ne è la versione digitale, ma non si tratta soltanto di un trasferimento dello stesso fenomeno su un nuovo mezzo. Le caratteristiche specifiche della rete trasformano profondamente la natura e la portata del fenomeno, rendendolo in molti casi più grave e più difficile da gestire rispetto alla sua versione tradizionale.

Nel bullismo tradizionale, l'aggressione è limitata nello spazio e nel tempo: avviene a scuola, in un quartiere, in un contesto definito. Quando la vittima torna a casa, ha almeno un momento di respiro. Nel cyberbullismo, questa distinzione scompare: lo smartphone è con la vittima ventiquattro ore su ventiquattro, sette giorni su sette. L'aggressione può raggiungerla a qualsiasi ora, in qualsiasi luogo. È questa la caratteristica che i ricercatori definiscono pervasività: l'impossibilità di sfuggire all'aggressore rifugiandosi in uno spazio fisico separato.

La seconda caratteristica distintiva è l'anonimato. Online è relativamente facile creare profili falsi, usare nickname, nascondere la propria identità. Questo abbassa enormemente la soglia di inibizione: molte persone scrivono online cose che non direbbero mai di persona, protette dalla sensazione — spesso illusoria — di essere invisibili. L'anonimato non protegge però dal punto di vista legale: le autorità competenti sono in grado di risalire all'identità reale di chi compie reati digitali.

La risonanza pubblica è la terza caratteristica. Un atto di bullismo tradizionale ha tipicamente un numero limitato di testimoni. Un contenuto offensivo pubblicato online può essere visto, condiviso e amplificato da migliaia di persone in pochissimo tempo. La dimensione pubblica del danno moltiplicato è spesso ciò che rende il cyberbullismo particolarmente devastante per la vittima.

La permanenza è forse la caratteristica più insidiosa. Il web ha una memoria lunghissima: un contenuto una volta pubblicato è estremamente difficile da eliminare completamente. Può essere salvato, ricondiviso, riemerso anni dopo. Per la vittima, questo significa che l'umiliazione non è circoscritta a un momento specifico ma può rivivere indefinitamente, ogni volta che qualcuno trova quel contenuto.

Quando il comportamento online diventa reato

Molti comportamenti che si manifestano online non sono semplici mancanze di educazione o “ragazzate”: sono reati penalmente perseguibili. Conoscerli è fondamentale sia per proteggersi sia per non commettere atti di cui non si comprendono le conseguenze legali.

Il revenge porn – tecnicamente definito dalla legge italiana come “diffusione illecita di immagini o video sessualmente espliciti” – è la condivisione senza consenso di immagini o video intimi di una persona. Dalla legge 69 del 2019, è un reato specifico punito con la reclusione da uno a sei anni e con la multa. Non è necessario che il contenuto sia stato originariamente prodotto senza consenso: anche condividere immagini che erano state condivise privatamente e volontariamente costituisce reato, se avviene senza l'autorizzazione della persona ritratta.

Il cyberstalking è la persecuzione sistematica attraverso mezzi digitali: messaggi ripetuti e indesiderati, monitoraggio dei profili social, minacce, pubblicazione di informazioni private. È perseguibile penalmente come atto persecutorio ai sensi dell'articolo 612-bis del Codice Penale, con pene che possono arrivare fino a sei anni di reclusione in caso di aggravanti.

Il dissing è la divulgazione pubblica di informazioni riservate, umilianti o dannose riguardanti una persona, con l'intento di danneggiarla agli occhi degli altri. Può assumere la forma di diffamazione aggravata quando avviene attraverso strumenti informatici, un reato previsto dall'articolo 595 del Codice Penale con l'aggravante dell'articolo 595, terzo comma.

Le forme di aggressione online: riconoscerle per contrastarle

Le aggressioni online assumono forme diverse, non sempre immediatamente riconoscibili come tali. Conoscerle aiuta a identificarle quando si verificano, a non perpetrarle inconsapevolmente e a sapere come rispondere.

Il trolling è la pratica di provocare deliberatamente altre persone online con commenti offensivi, fuori luogo o contraddittori, con l'unico scopo di generare reazioni emotive negative. Non ha mai un obiettivo costruttivo: è aggressione mascherata da opinione. La risposta più efficace al trolling è il non rispondere:

privare il troll della reazione emotiva che cerca è l'unico modo per disinnescarlo.

L'hate speech — discorso d'odio — è qualsiasi forma di comunicazione che incita all'odio, alla discriminazione o alla violenza contro persone o gruppi in base alla loro identità: etnia, religione, genere, orientamento sessuale, disabilità. È vietato dalla legge italiana e dalle politiche di quasi tutte le piattaforme digitali. È importante distinguerlo dalla critica, anche dura: l'hate speech non è una opinione, è un atto di aggressione verso una categoria di persone.

Il body shaming è la pratica di criticare, deridere o umiliare una persona per il suo aspetto fisico. Sebbene possa sembrare meno grave di altri tipi di aggressione, può avere conseguenze psicologiche molto serie, soprattutto negli adolescenti, e contribuisce a una cultura tossica che associa il valore delle persone al loro aspetto esteriore.

Il furto d'identità e il catfishing sono fenomeni diversi ma correlati. Nel primo caso, qualcuno usa l'identità di un'altra persona (il suo nome, le sue foto, i suoi dati) per impersonarla online, spesso per danneggiarla. Nel secondo, qualcuno costruisce un'identità falsa per instaurare relazioni ingannevoli, spesso a scopo manipolativo o truffaldino.

I meccanismi psicologici: perché le persone diventano aggressive online

Comprendere perché le persone si comportano online in modi che non adotterebbero mai nella vita di tutti i giorni è fondamentale per affrontare il problema alla radice. Due meccanismi psicologici giocano un ruolo centrale.

L'effetto di disinibizione descrive il fenomeno per cui la mancanza di contatto visivo diretto — non vedere la faccia dell'altra persona, non sentire la sua voce, non percepire le sue reazioni emotive — riduce significativamente i freni inibitori naturali che regolano i comportamenti sociali. Nella comunicazione faccia a faccia, l'empatia è attivata automaticamente dalla percezione delle emozioni altrui: vediamo qualcuno soffrire e sentiamo una risposta interna che ci frena dall'infliggere ulteriore sofferenza. Online, questa retroazione emotiva è assente, e il comportamento aggressivo diventa più facile da mettere in atto.

I bias cognitivi — in particolare il bias di conferma e il bias di ostilità — sono un ulteriore fattore che contribuisce alle aggressioni online. Il bias di conferma porta a cercare e a interpretare le informazioni in modo da confermare le proprie opinioni preesistenti, rifiutando quelle contraddittorie. Il bias di ostilità porta a interpretare azioni o parole ambigue come intenzionalmente ostili: un commento neutro viene letto come un attacco, un emoji viene interpretato come sarcasmo. Questi meccanismi, amplificati dalla rapidità della comunicazione digitale e dall'assenza di contesto non verbale, producono conflitti che possono degenerare rapidamente.

Condividere o mettere “like” a un atto di cyberbullismo significa diventarne complici. La complicità online non è moralmente neutrale e può avere conseguenze legali, specialmente per i minori che raggiungono l’età penalmente rilevante.

GLI ATTORI, I FATTORI DI RISCHIO E LE CONSEGUENZE

Obiettivi del modulo

Al termine di questo modulo saprai analizzare i ruoli degli attori coinvolti in una dinamica di cyberbullismo: la vittima, il bullo e, con particolare attenzione, gli spettatori. Conoscerai i principali fattori di rischio individuali e ambientali che rendono alcune persone più vulnerabili. Saprai riconoscere i segnali di allarme che indicano che qualcuno potrebbe essere vittima di cyberbullismo e comprenderai la natura delle conseguenze fisiche, comportamentali e psicopatologiche che il fenomeno può produrre.

Gli attori: molto più di bullo e vittima

L'analisi del cyberbullismo che si ferma alla coppia bullo-vittima è incompleta e fuorviante. La realtà è più complessa e coinvolge un terzo protagonista spesso trascurato ma forse il più importante: gli spettatori.

La vittima è la persona che subisce sistematicamente e intenzionalmente le aggressioni digitali. Spesso si sente sola, incompresa e senza via d'uscita. Uno degli aspetti più dolorosi del cyberbullismo è la sensazione che nessuno intervenga, che chi assiste preferisca guardare senza prendere posizione. La permanenza dei contenuti online e la difficoltà di sfuggire all'aggressione amplificano la sofferenza e il senso di impotenza.

Il cyberbullo è la persona che attua le aggressioni. Non sempre si tratta di un individuo caratterizzato da cattiveria o da problemi psicologici gravi: spesso è qualcuno che non ha piena consapevolezza delle conseguenze delle proprie azioni, che agisce per cercare approvazione nel gruppo, che usa l'aggressione come strumento per affermare un dominio sociale, o che è a sua volta vittima di dinamiche negative in altri contesti. Comprendere le motivazioni del bullo non significa giustificarlo, ma è necessario per costruire interventi efficaci.

Il potere degli spettatori: da testimoni a protagonisti

Gli spettatori sono le persone che assistono alle aggressioni digitali: chi vede il post offensivo, chi legge i commenti, chi riceve lo screenshot. Sono la maggioranza silenziosa che, con il suo comportamento — attivo o passivo — determina in modo cruciale l'evoluzione della situazione.

Lo spettatore attivo è chi interviene amplificando l'aggressione: condivide i contenuti, aggiunge commenti offensivi, mette like, si unisce alla campagna di schermo. Anche se non è l'iniziatore dell'aggressione, contribuisce attivamente ad essa e ne è corresponsabile sul piano morale e, in certi casi, legale.

Lo spettatore passivo è chi assiste senza fare nulla: vede ma tace, legge ma non commenta, è consapevole ma non interviene. Spesso il silenzio è motivato dalla paura di diventare a propria volta vittima, dal desiderio di non complicarsi la vita, o dalla sensazione che il problema non riguardi direttamente se stessi. Ma il silenzio dello spettatore ha un effetto concreto: dice al bullo che il suo comportamento è accettato, o almeno tollerato, e dice alla vittima che è sola.

L'alleato è lo spettatore che sceglie di intervenire in difesa della vittima. Non necessariamente con confronti diretti con il bullo – che potrebbero essere controproducenti – ma supportando la vittima privatamente, segnalando i contenuti alle piattaforme, coinvolgendo adulti di riferimento o semplicemente facendo sentire alla vittima che non è sola. Il potere dell'alleato è spesso sottovalutato: anche un singolo gesto di sostegno può fare una differenza enorme nella vita di chi subisce.

La ricerca mostra che il cyberbullismo tende a cessare o a ridursi significativamente quando un numero sufficiente di spettatori si trasforma in alleati. Il cyberbullo smette quando smette di ricevere il rinforzo del gruppo. La decisione di non essere spettatore passivo è una delle più potenti che si possa prendere online.

I fattori di rischio

Non tutti sono ugualmente esposti al rischio di diventare vittime di cyberbullismo. Esistono fattori individuali e ambientali che aumentano la vulnerabilità, e conoscerli permette di intervenire in modo più mirato.

A livello individuale, i fattori di rischio includono una bassa autostima e una scarsa sicurezza in sé stessi, difficoltà nelle relazioni sociali, esperienze pregresse di vittimizzazione (chi è già stato vittima di bullismo tende a esserlo anche online) e una scarsa familiarità con le dinamiche digitali che rende difficile riconoscere e rispondere alle aggressioni. Anche le caratteristiche che rendono una persona diversa dalla norma percepita: l'aspetto fisico, l'orientamento sessuale, la provenienza, le difficoltà di apprendimento possono aumentare il rischio di essere presi di mira.

A livello ambientale, i fattori di rischio includono una scarsa supervisione e comunicazione in famiglia riguardo all'uso del digitale, un contesto scolastico o comunitario che tollera o minimizza le dinamiche di aggressione, e la mancanza di educazione digitale formale. Quest'ultimo fattore è di particolare importanza: chi non conosce le implicazioni legali e psicologiche dei propri comportamenti online, chi non sa come segnalare un contenuto offensivo, chi non conosce i propri diritti in quanto vittima è significativamente più vulnerabile.

Le conseguenze: il peso invisibile

Le conseguenze del cyberbullismo sono reali, profonde e spesso durature. Non si tratta di reazioni esagerate o di fragilità individuale: sono risposte psicologiche e fisiche documentate e studiate dalla ricerca scientifica, che possono manifestarsi con intensità diversa a seconda della gravità e della durata dell'aggressione.

I segnali comportamentali che possono indicare che qualcuno sta subendo cyberbullismo includono il ritiro sociale, il cambiamento improvviso nelle abitudini di uso del telefono o del computer, l'evitamento di eventi sociali, il calo del rendimento scolastico o lavorativo, la perdita di interesse per attività precedentemente piacevoli. Spesso la vittima inizia a evitare di usare i dispositivi digitali o, al contrario, non riesce a staccarsi da essi, in preda a un'ansia di controllo costante di ciò che viene detto di lei online.

I sintomi fisici possono includere disturbi del sonno, mal di testa, dolori addominali, stanchezza cronica. Questi sintomi sono la risposta del corpo a uno stato di stress prolungato: il cyberbullismo, per la sua natura pervasiva, mantiene la vittima in uno stato di allerta continua che ha conseguenze fisiche concrete.

L'impatto psicopatologico può essere molto grave: ansia, depressione, disturbi post-traumatici da stress, nei casi più gravi pensieri suicidari. La permanenza dei contenuti digitali amplifica questo impatto: a differenza di un'aggressione fisica che si esaurisce in un momento, il cyberbullismo può essere rivissuto ogni volta che si accede alla rete, ogni volta che qualcuno trova quel contenuto e lo ricondivide.

Segnale d'allarme: Un cambiamento brusco e inspiegabile nelle abitudini digitali o nel comportamento sociale di una persona (soprattutto di un giovane) è spesso il primo segnale che qualcosa non va. Prendersene cura, chiedere come sta e offrire ascolto senza giudicare può fare una differenza cruciale.

USO ETICO DELLA RETE: NETIQUETTE, PRIVACY E PENSIERO CRITICO

Obiettivi del modulo

Al termine di questo modulo conoscerai i principi fondamentali della netiquette e dell'impronta digitale, comprenderai il concetto di consenso nel contesto digitale e saprai come gestire attivamente la tua privacy online. Conoscerai le principali tecniche di phishing e saprai come difenderti. Avrai strumenti concreti per sviluppare il pensiero critico come antidoto ai bias cognitivi che alimentano le aggressioni online.

La netiquette: il galateo della rete

La netiquette – contrazione di network etiquette – è l'insieme delle norme di comportamento che regolano la comunicazione online. Non è un codice scritto con forza di legge, ma una serie di convenzioni condivise che permettono la convivenza civile negli spazi digitali. La sua regola fondamentale è semplice e potente: comportati online come vorresti essere trattato, e come ti comporteresti in un contesto pubblico reale.

Alcune norme di netiquette sono particolarmente rilevanti nel contesto di questa dispensa. Non condividere mai contenuti di altri (foto, messaggi privati, informazioni personali) senza il loro esplicito consenso. Non pubblicare informazioni su situazioni, luoghi o persone senza aver chiesto il permesso. Non usare un tono aggressivo, sarcastico o denigratorio nei commenti: la critica può essere diretta e onesta senza essere offensiva. Non alimentare le discussioni aggressive con la propria partecipazione: il silenzio attivo, ossia scegliere deliberatamente di non amplificare, è spesso la risposta più efficace.

L'impronta digitale: cosa lasci di te online

Ogni azione che compiamo online lascia una traccia: i commenti che pubblichiamo, le foto che carichiamo, i like che mettiamo, le ricerche che facciamo, i siti che visitiamo. L'insieme di queste tracce costituisce la nostra impronta digitale, una sorta di curriculum informale che ci precede e che ci segue in ogni contesto in cui qualcuno voglia cercarci.

La metafora del muro è utile per comprendere la portata di questo concetto: se tutto ciò che scrivi oggi restasse scolpito su un muro della tua città per i prossimi cinquant'anni, saresti fiero di averlo firmato? Molti comportamenti online che sembrano effimeri come un commento scritto di getto o una foto condivisa in un momento di rabbia, possono riemergere anni dopo con conseguenze che non si erano previste. I selezionatori del lavoro cercano i candidati online. I partner controllano i profili social. Le istituzioni possono richiedere l'accesso a contenuti digitali in caso di procedimenti legali. L'impronta digitale non è un concetto astratto: è parte della propria reputazione nel mondo reale.

La cultura del consenso

Il consenso è il principio fondamentale che regola l'uso etico dei contenuti che riguardano altre persone. Prima di condividere una foto in cui c'è qualcun altro, bisogna chiedere il permesso a quella persona. Prima di pubblicare informazioni su qualcuno, bisogna assicurarsi di averne il consenso. Prima di taggare qualcuno in un post, bisogna verificare che sia a proprio agio con quella visibilità.

Il consenso deve essere libero, informato e specifico: qualcuno che ha acconsentito a essere fotografato non ha necessariamente acconsentito a che quella foto venga pubblicata sui social network. Qualcuno che ha condiviso con te privatamente un'informazione non ha acconsentito a che tu la condivida con altri. Il consenso non è una burocrazia: è il rispetto fondamentale per l'autonomia e la dignità dell'altro.

Privacy e sicurezza: proteggersi attivamente

La gestione della privacy online non è una questione di paranoia: è una competenza fondamentale di cittadinanza digitale. Le piattaforme social raccolgono enormi quantità di dati sui propri utenti, e la configurazione predefinita tende a massimizzare la visibilità e la condivisione dei dati, non a proteggere la privacy. Chi non configura attivamente le impostazioni di privacy dei propri profili sta, di fatto, concedendo a chiunque l'accesso alle proprie informazioni personali. La configurazione attiva della privacy comprende alcune pratiche essenziali: controllare regolarmente le impostazioni di privacy di ogni account social, verificando chi può vedere i propri contenuti, chi può taggare la propria persona, chi può trovare il profilo tramite ricerca; usare password forti con non meno di dodici caratteri, con combinazione di lettere maiuscole e minuscole, numeri e simboli e diverse per ogni account; attivare l'autenticazione a due fattori, che richiede una seconda verifica — tipicamente un codice inviato al telefono — per accedere all'account anche se qualcuno conosce la password.

La difesa dal phishing è altrettanto importante. Il phishing è una tecnica truffaldina che cerca di ottenere dati personali, password o informazioni finanziarie fingendosi un'entità affidabile: una banca, un servizio online, un ente pubblico. Si manifesta tipicamente attraverso email o messaggi che sembrano provenire da fonti legittime e che contengono link a siti che imitano quelli originali. Riconoscerlo richiede attenzione: controllare il mittente reale dell'email, verificare l'URL del sito prima di inserire dati, non cliccare su link ricevuti in messaggi non attesi, non fornire mai password o dati bancari in risposta a richieste via email.

Il pensiero critico: l'antivirus contro i bias

Il pensiero critico è la capacità di valutare le informazioni e le situazioni con

metodo e consapevolezza, resistendo alle reazioni impulsive e alle distorsioni cognitive. Nell'ecosistema digitale, dove le informazioni si moltiplicano a velocità vertiginosa e dove i meccanismi di raccomandazione delle piattaforme tendono a rafforzare le posizioni già possedute, il pensiero critico è la difesa più efficace contro la disinformazione, i bias e le reazioni aggressive. La tecnica Wait and Think – aspetta e rifletti – è uno strumento semplice ma potente. Prima di rispondere a un commento che sembra offensivo, prima di condividere un contenuto che provoca indignazione, prima di reagire a ciò che sembra un attacco: aspetta. Prenditi trenta secondi, un minuto, un'ora. Chiedi ad almeno una persona di cui ti fidi cosa ne pensa. La maggior parte delle reazioni aggressive online nasce da reazioni impulsive che, con un minimo di tempo e riflessione, non verrebbero mai messe in atto.

La Peer Education (l'educazione tra pari) è una delle strategie più efficaci per diffondere questi strumenti nelle comunità. Chi impara a riconoscere i propri bias cognitivi, a praticare il pensiero critico, a distinguere fatti da opinioni e a gestire le reazioni emotive online ha una responsabilità: condividere questi strumenti con chi gli sta vicino. La cultura digitale responsabile non si costruisce attraverso decreti dall'alto: si costruisce attraverso le relazioni, le conversazioni, gli esempi.

COME RISPONDERE: PROTOCOLLO S.O.S., STRUMENTI E QUADRO LEGALE

Obiettivi del modulo

Al termine di questo modulo conoscerai il protocollo da adottare in caso di cyberbullismo: conservazione delle prove, non reazione, segnalazione istituzionale. Saprai utilizzare gli strumenti tecnologici di protezione disponibili, tra cui parental control, software di monitoraggio e strumenti delle piattaforme. Conoscerai il quadro normativo italiano, con particolare riguardo alla Legge 71/2017 e le principali responsabilità penali derivanti dai reati digitali.

Il protocollo S.O.S.: cosa fare quando succede

Quando si è vittima di cyberbullismo, o quando si è testimoni di un episodio che riguarda qualcuno vicino, sapere cosa fare concretamente fa una differenza enorme. Il protocollo S.O.S. (Salva, Osserva, Segnala) è uno schema operativo semplice che aiuta a non cedere al panico e a prendere le misure giuste.

La prima azione è non rispondere e non reagire. Qualsiasi risposta emotiva all'aggressore come insulti, minacce, difese appassionate, alimenta il conflitto, dà al bullo la soddisfazione della reazione e può essere usata contro di noi. La tentazione di rispondere è comprensibile, ma resistere è la scelta più efficace. Bloccare l'aggressore è la misura tecnica immediata da adottare.

La seconda azione è conservare le prove. Prima di eliminare qualsiasi contenuto, è fondamentale fare screenshot di tutto: i messaggi offensivi, i post, i commenti, le date e gli orari, i nomi dei profili coinvolti. Le prove digitali sono essenziali per qualsiasi procedimento legale o segnalazione istituzionale. Senza prove documentate, la parola della vittima è più difficile da sostenere davanti alle autorità.

La terza azione è la segnalazione istituzionale. Le piattaforme digitali hanno tutte strumenti di segnalazione dei contenuti offensivi: usarli è importante, anche se i tempi di risposta possono essere lunghi. Per i reati più gravi, è necessario rivolgersi alla Polizia Postale, che è l'organo specializzato nella gestione dei reati informatici. Il Garante per la Protezione dei Dati Personali ha poteri specifici per richiedere la rimozione di contenuti entro 48 ore: in caso di contenuti che violano la privacy (es. immagini diffuse senza consenso) è un'autorità fondamentale a cui rivolgersi.

Non aspettare che le cose si risolvano da sole. Il cyberbullismo, senza intervento, tende ad aggravarsi nel tempo. Agire prima segnalando, cercando supporto e coinvolgendo adulti di riferimento, è sempre meglio che aspettare.

Gli strumenti tecnologici di protezione

La tecnologia che può essere usata per fare del male può anche essere usata per proteggerci. Esistono strumenti specifici progettati per ridurre i rischi online, particolarmente utili nel contesto della tutela dei minori ma non esclusivi di quella fascia d'età.

Il parental control è un insieme di funzionalità software che permette di limitare l'accesso a determinati contenuti, di monitorare l'uso del dispositivo, di impostare limiti di tempo e di gestire le app installate. È disponibile come funzionalità nativa nei principali sistemi operativi (iOS, Android, Windows, macOS) e come applicazione dedicata. Non è uno strumento di sorveglianza invasiva: usato in modo trasparente, come parte di una conversazione aperta su sicurezza digitale, è un supporto prezioso per i genitori che vogliono proteggere i propri figli mantenendo un dialogo.

Le piattaforme digitali offrono anche strumenti specifici di protezione: la possibilità di bloccare utenti, di segnalare contenuti, di limitare chi può commentare i propri post o inviare messaggi privati, di filtrare i commenti con parole chiave specifiche. Usare attivamente questi strumenti è parte di una gestione responsabile della propria presenza online.

Il quadro normativo: la Legge 71/2017 e i reati digitali

L'Italia ha una legge specifica sul cyberbullismo: la Legge 71 del 29 maggio 2017, nota come Legge Mancini. È la prima legge italiana dedicata specificamente al fenomeno e ha introdotto strumenti importanti per la tutela dei minori e per la prevenzione e il contrasto del cyberbullismo nelle scuole.

La legge prevede che le scuole nominino un referente per le politiche di prevenzione e contrasto del cyberbullismo, con l'obbligo di attivare procedure di intervento in caso di episodi segnalati. Il preside/dirigente scolastico ha poteri e responsabilità specifiche: deve essere informato di qualsiasi episodio di cyberbullismo che riguardi la comunità scolastica e deve intervenire adottando le misure necessarie. La legge prevede anche uno strumento specifico per i minori: la possibilità di chiedere al Garante per la Protezione dei Dati Personali l'oscuramento, la rimozione o il blocco di contenuti che ritengono essere atti di cyberbullismo, senza necessariamente avviare un procedimento penale. Il Garante è tenuto a rispondere entro 48 ore.

Per quanto riguarda le responsabilità penali, è importante sapere che in Italia la responsabilità penale inizia a 14 anni. Un minore di 14 anni non è penalmente imputabile, ma chi esercita la responsabilità genitoriale può essere chiamato a rispondere civilmente del danno. Tra i 14 e i 18 anni, i minori sono penalmente imputabili ma con trattamento differenziato rispetto agli adulti.

Sopra i 18 anni, si risponde pienamente delle proprie azioni digitali.

I principali reati digitali perseguibili includono: la minaccia, articolo 612 del Codice Penale, fino a un anno di reclusione; la diffamazione aggravata tramite strumenti informatici, articolo 595, terzo comma, fino a tre anni di reclusione; la sostituzione di persona, articolo 494, fino a un anno; gli atti persecutori o cyberstalking, articolo 612-bis, da uno a sei anni, con aggravante in caso di uso di strumenti informatici; la diffusione illecita di immagini intime, legge 69 del 2019, da uno a sei anni.

Da sapere: Se sei vittima di un reato digitale, puoi presentare denuncia presso qualsiasi commissariato di Polizia o stazione dei Carabinieri. La Polizia Postale ha anche uno sportello online sul sito [commissariatodips.it](https://www.commissariatodips.it) per le segnalazioni di reati informatici.

Obiettivi del modulo

Al termine di questo modulo avrai sviluppato una comprensione più profonda del concetto di empatia digitale e della responsabilità collettiva nel contrasto al cyberbullismo. Saprai come passare da spettatore passivo ad alleato proattivo. Avrai un toolkit operativo che include le regole d'oro per un uso quotidiano consapevole della rete e che puoi applicare immediatamente e condividere con chi ti sta vicino.

L'empatia digitale: vedersi nell'altro

L'empatia è la capacità di comprendere e condividere i sentimenti di un'altra persona, di mettersi nei suoi panni. Nell'ambiente digitale, questa capacità è sistematicamente erosa dall'assenza di contatto fisico, dalla velocità della comunicazione e dall'effetto di disinibizione che riduce la percezione della realtà emotiva dell'altro. Coltivare l'empatia digitale significa lavorare deliberatamente contro questa erosione.

Un esercizio pratico di empatia digitale è chiedersi, prima di pubblicare qualsiasi contenuto che riguardi un'altra persona: come mi sentirei se questo fosse pubblicato su di me? Se la risposta è che mi sentirei a disagio, ferito, umiliato, o se non posso sapere come si sentirebbe quella persona, magari perché non l'ho mai chiesto, allora è il momento di fermarsi.

L'empatia digitale non riguarda soltanto il non fare del male: riguarda anche il fare del bene attivamente. Riconoscere il contributo di qualcuno in una discussione online, esprimere sostegno a qualcuno che si trova in difficoltà, segnalare un contenuto offensivo perché si tiene alla dignità della persona che coinvolge: questi sono atti di empatia digitale che costruiscono comunità online migliori.

La responsabilità collettiva: il cyberbullismo si vince con la cultura

Il cyberbullismo non è un problema che può essere risolto soltanto dalla legge, dai filtri tecnologici o dagli adulti di riferimento. È un problema culturale che richiede una risposta culturale. Le norme legislative sono necessarie ma non sufficienti: una norma senza una cultura che la sostenga non cambia i comportamenti reali.

La responsabilità collettiva significa che tutti (non solo le vittime e non solo i bulli) hanno un ruolo nella costruzione di spazi digitali più sicuri e più rispettosi. Chi sceglie di non condividere contenuti offensivi contribuisce. Chi segnala un post problematico contribuisce. Chi supporta una persona che sta subendo un'aggressione contribuisce. Chi parla apertamente di questi temi

con i propri figli, i propri studenti, i propri colleghi contribuisce. La transizione dall'esclusione sociale all'inclusione digitale non avviene automaticamente: è il risultato di scelte quotidiane, individuali e collettive, che sommandosi producono un cambiamento culturale reale. Ogni persona che legge questa dispensa e decide di applicare i principi che contiene è parte di questo cambiamento.

Il toolkit: le cinque regole d'oro

Al termine di questo percorso, è utile avere un promemoria operativo – un toolkit – che sintetizzi i principi fondamentali in regole concrete e applicabili ogni giorno. Queste regole d'oro non sostituiscono la complessità di ciò che si è discusso: la sintetizzano in azioni immediate.

1. Pensa prima di postare. Ogni contenuto che pubblichi è potenzialmente permanente e pubblico. Chiediti: se questo restasse online per sempre, sarei a mio agio? Se la risposta è no, non pubblicarlo.

2. Il consenso è sacro. Non condividere mai contenuti che riguardano altre persone senza il loro esplicito permesso. Questo vale per le foto, per le informazioni personali, per i messaggi privati. Il consenso non è una formalità: è rispetto.

3. Le parole hanno un peso. Anche online, anche in forma anonima, anche in una chat privata. Le parole che scrivi raggiungono persone reali con emozioni reali. Usa il tono che useresti guardando negli occhi la persona a cui ti stai rivolgendo.

4. Non restare in silenzio. Se sei testimone di un'aggressione online, non girare la testa. Segnala il contenuto, supporta la vittima, coinvolgi adulti di riferimento. Il silenzio degli spettatori è il carburante del cyberbullismo.

5. Proteggi i tuoi dati. Configura attivamente le impostazioni di privacy dei tuoi account. Usa password forti e diverse. Non condividere informazioni sensibili in risposta a richieste non verificate. La tua sicurezza online dipende in gran parte dalle tue scelte.

Queste regole non sono restrizioni alla libertà online: sono le fondamenta di una libertà digitale più autentica. Chi usa la rete con responsabilità e rispetto può fruire di tutti i suoi benefici senza le conseguenze legali, reputazionali, relazionali che derivano dai comportamenti irresponsabili.

Perché il dialogo è più efficace del controllo

Uno degli errori più comuni che gli adulti commettono nel tentativo di proteggere i giovani dal cyberbullismo è quello di affidarsi esclusivamente al controllo: sottrarre i dispositivi, installare filtri senza spiegarne il motivo, vietare l'accesso ai social network. Queste misure, adottate senza una comunicazione aperta e senza un lavoro educativo di accompagnamento, producono quasi sempre l'effetto contrario: il giovane impara a nascondere la propria vita digitale, e il problema si sposta in uno spazio in cui l'adulto non ha più alcuna visibilità.

La ricerca è chiara su questo punto: i giovani che affrontano meglio le situazioni difficili online sono quelli che hanno la certezza di poter parlare con un adulto di riferimento senza essere giudicati, puniti o privati del telefono. Questo non significa che i genitori e gli educatori debbano approvare qualsiasi comportamento: significa che devono costruire una relazione di fiducia sufficiente perché il giovane scelga di chiedere aiuto anziché affrontare da solo una situazione che lo sopraffà.

Il dialogo preventivo, parlare di questi temi prima che accada qualcosa, è molto più efficace di quello reattivo. Un genitore che discute apertamente con i propri figli di cosa fare se si riceve un messaggio offensivo, di come riconoscere il phishing, di quali contenuti non condividere: questo genitore sta costruendo un'armatura culturale che nessun software di parental control potrà mai replicare.

Come parlare di cyberbullismo con i giovani

Non esiste uno script perfetto per questa conversazione, ma esistono alcune linee guida che la rendono più efficace. La prima è partire dall'ascolto, non dalla norma: prima di spiegare cosa si deve o non si deve fare, chiedere cosa sa già il giovane di questi temi, cosa ha visto, cosa gli è capitato. Ascoltare senza interrompere, senza giudicare, senza reagire con allarme eccessivo: questi atteggiamenti creano lo spazio psicologico in cui la comunicazione diventa possibile.

La seconda linea guida è usare esempi concreti, non astratti. Non "il cyberbullismo fa male" ma "hai mai visto qualcuno essere trattato male in un gruppo WhatsApp? Come ti sei sentito? Cosa hai fatto?". I casi concreti, inclusi quelli che compaiono nelle notizie, sono strumenti educativi potenti se usati senza sensazionalismo e con un focus sull'analisi critica della situazione.

La terza linea guida è chiarire che chiedere aiuto non significa perdere il telefono. Questa è spesso la ragione principale per cui i giovani non parlano con gli adulti quando subiscono cyberbullismo: hanno paura che la reazione immediata dell'adulto sia quella di togliere il dispositivo, che per loro è anche lo strumento di connessione con gli amici, il mezzo di espressione, lo spazio di autonomia. Esplicitare che l'obiettivo è aiutare, non punire, è il primo passo per abbattere questa barriera.

Il ruolo della scuola: oltre la Legge 71/2017

La scuola ha un ruolo unico nel contrasto al cyberbullismo: è il luogo in cui la maggior parte delle dinamiche di gruppo tra adolescenti si forma e si manifesta, e in cui è possibile raggiungere tutti i giovani con un intervento sistematico ed educativo. La Legge 71/2017 ha formalizzato questo ruolo con obblighi specifici, ma l'efficacia dell'intervento scolastico va molto oltre l'adempimento normativo. I programmi di educazione digitale che funzionano non sono quelli che si limitano a elencare i rischi della rete: sono quelli che mettono al centro le competenze, il pensiero critico, la gestione delle emozioni, la capacità di riconoscere i propri bias e che usano metodologie attive come il role playing, la peer education e la discussione di casi reali. La dispensa che stai leggendo è concepita esattamente in quest'ottica: non come un testo da memorizzare ma come uno strumento per attivare riflessioni e cambiamenti di comportamento.

Il referente scolastico per il cyberbullismo (figura prevista dalla Legge 71/2017) ha un ruolo di coordinamento che va oltre la gestione degli episodi critici: include la promozione di una cultura digitale responsabile all'interno della comunità scolastica, il raccordo con le famiglie e le istituzioni esterne, e la formazione continua dei docenti su questi temi. Una scuola che forma adulti digitalmente consapevoli forma, indirettamente, famiglie e comunità più capaci di affrontare questi fenomeni.

La comunità come rete di protezione

Il cyberbullismo non è soltanto un problema che riguarda i giovani e le scuole. Coinvolge adulti – mobbing digitale, revenge porn tra ex partner, stalking online – e anziani – truffe, manipolazione, isolamento digitale. Una risposta culturale efficace deve coinvolgere l'intera comunità, non solo le fasce d'età più giovani.

Le biblioteche, i centri anziani, le associazioni di quartiere, le parrocchie, le organizzazioni di volontariato: sono tutti luoghi in cui si può fare educazione digitale e promuovere una cultura del rispetto online. Iniziative come il progetto Digita Facile Campania dimostrano che la formazione digitale rivolta agli adulti e agli anziani produce risultati concreti in termini di autonomia, sicurezza e

qualità della vita. Una comunità digitalmente consapevole è una comunità più resiliente di fronte ai rischi della rete.

Per i genitori: Se tuo figlio segnalasse di essere vittima di cyberbullismo, la prima risposta dovrebbe essere gratitudine per la fiducia dimostrata e ascolto attivo. Solo dopo, insieme, si valutano le azioni da intraprendere. Non togliere il telefono come prima reazione: è il modo più rapido per perdere la comunicazione.

Imparare dai casi: scenari e riflessioni

Uno degli strumenti più efficaci per comprendere davvero un fenomeno è confrontarsi con situazioni concrete. I seguenti scenari, costruiti a partire da tipologie reali di episodi di cyberbullismo, sono pensati per attivare la riflessione e per applicare i concetti discussi in questa dispensa a situazioni riconoscibili.

Scenario 1: il gruppo di classe

Giulia, 15 anni, viene esclusa dal gruppo WhatsApp della classe senza spiegazioni. I suoi compagni creano un gruppo parallelo in cui condividono screenshot di sue conversazioni private, aggiungendo commenti ironici sul suo aspetto e sul suo modo di parlare. Giulia lo scopre per caso attraverso un'amica. Nei giorni successivi, i commenti ironici si trasferiscono anche sui social network, sempre più pubblici. Giulia inizia a non voler andare a scuola.

Questo scenario illustra alcune caratteristiche tipiche del cyberbullismo tra adolescenti: la dimensione di gruppo, che amplifica la portata dell'aggressione; la transizione dal privato al pubblico, che ne aumenta la gravità; e il legame con la vita offline, che rende impossibile per la vittima separare le due sfere. In questo caso, cosa avrebbe potuto fare l'amica che ha scoperto la situazione? Come dovrebbe reagire un genitore informato? Cosa prevede la scuola in questo caso?

Scenario 2: l'ex partner

Marco, 23 anni, termina una relazione. L'ex partner, in risposta, pubblica sui social network screenshot di messaggi privati, commentandoli in modo da screditarlo agli occhi degli amici comuni. Successivamente, crea un profilo falso con il nome di Marco e inizia a inviare messaggi offensivi ai suoi contatti. Marco si trova a dover spiegare a tutti che non è lui il mittente di quei messaggi.

Questo scenario combina due reati distinti: la diffamazione (la pubblicazione dei messaggi con commenti offensivi) e la sostituzione di persona (il profi-

lo falso). Illustra come il cyberbullismo non riguardi soltanto i giovanissimi e come possa avere conseguenze concrete e immediate sulla vita reale, nelle relazioni sociali e professionali. Quali sono le prime azioni che Marco dovrebbe intraprendere? A quali autorità può rivolgersi?

Scenario 3: lo spettatore

Lucia, 17 anni, fa parte di un gruppo online in cui alcuni ragazzi iniziano a prendere in giro sistematicamente un compagno di scuola, condividendo foto modificate in modo ridicolo e inventando storie false sul suo conto. Lucia non conosce molto bene il compagno preso di mira, ma si rende conto che le cose stanno peggiorando. Non vuole essere coinvolta, ma sente che il silenzio la rende complice.

Questo scenario esplora il dilemma dello spettatore passivo: la tensione tra il desiderio di non complicarsi la vita e la consapevolezza che il silenzio ha un costo morale. Lucia non deve necessariamente confrontarsi direttamente con i ragazzi che stanno facendo del male: può segnalare il contenuto alla piattaforma, può contattare privatamente il compagno per fargli sapere che non è solo, può parlare con un adulto di riferimento. Anche il gesto più piccolo può fare la differenza.

Scenario 4: l'adulto e la truffa digitale

Antonio, 68 anni, riceve un'email che sembra provenire dalla sua banca, con il logo ufficiale e un tono formale. L'email lo informa di un'anomalia sul conto e lo invita a cliccare su un link per verificare i propri dati. Antonio clicca, inserisce le credenziali e si ritrova con il conto svuotato in poche ore. Quando lo racconta ai figli, si sente rispondere che "doveva stare più attento".

Questo scenario illustra due fenomeni distinti ma correlati: il phishing sofisticato, che non è più facilmente riconoscibile come in passato, e la tendenza a colpevolizzare le vittime di truffe digitali. Antonio non è caduto in una truffa per stupidità: è caduto in una truffa perché era ben costruita e perché non aveva ricevuto una formazione adeguata su come riconoscerla. La risposta giusta non è il rimprovero: è il supporto immediato, come contattare la banca, sporgere denuncia e la formazione preventiva per evitare che accada di nuovo.

I casi reali ci ricordano che il cyberbullismo e le aggressioni digitali non sono fenomeni astratti. Dietro ogni scenario c'è una persona reale con una vita reale che viene danneggiata. Tenere questa consapevolezza viva è il fondamento di qualsiasi cultura digitale responsabile.

Riepilogo dei concetti fondamentali

Questo percorso formativo ha affrontato il cyberbullismo e l'esclusione sociale digitale nella loro complessità: non come un problema di tecnologia ma come un problema umano, culturale e sociale che richiede risposte a più livelli. Il cyberbullismo si distingue dal bullismo tradizionale per quattro caratteristiche che lo rendono spesso più grave: la pervasività, non conosce orari né confini fisici; l'anonimato, che abbassa le difese psicologiche dell'aggressore; la risonanza pubblica, che moltiplica il danno; la permanenza, che lo rende difficile da archiviare. Molti comportamenti online non sono semplici mancanze di educazione ma reati penalmente perseguibili: revenge porn, cyberstalking, diffamazione aggravata, sostituzione di persona.

Comprendere gli attori del cyberbullismo significa andare oltre la coppia bullo-vittima. Gli spettatori sono i protagonisti più numerosi e, collettivamente, i più potenti: la loro scelta di essere attivi, passivi o alleati determina in misura cruciale l'evoluzione della situazione. Il cyberbullo smette quando smette di ricevere il rinforzo del gruppo. La decisione di trasformarsi da spettatore in alleato è una delle più importanti che si possa prendere online.

Un uso etico della rete richiede tre pilastri: la netiquette, comportarsi online come ci si comporterebbe in un contesto pubblico reale; il consenso, non condividere mai contenuti altrui senza permesso; il pensiero critico, resistere alle reazioni impulsive e ai bias cognitivi che alimentano i conflitti. La gestione attiva della propria privacy e la difesa dal phishing completano il quadro delle competenze di sicurezza digitale.

Quando si è vittime o testimoni di cyberbullismo, sapere come agire fa la differenza: non rispondere all'aggressore, conservare le prove con screenshot, segnalare alle piattaforme, alla Polizia Postale e al Garante per la Protezione dei Dati. La Legge 71/2017 offre strumenti specifici per i minori; il Codice Penale prevede sanzioni precise per i reati digitali a partire dai 14 anni.

La lotta al cyberbullismo si vince con la cultura. L'empatia digitale, la responsabilità collettiva, la scelta quotidiana di non essere spettatori passivi: sono questi gli ingredienti di una rete migliore. Ogni persona che applica le cinque regole d'oro (pensare prima di postare, rispettare il consenso, pesare le parole, non restare in silenzio, proteggere i propri dati) contribuisce a costruire spazi digitali più sicuri e più degni per tutti.

Il web non dimentica. Ma tu puoi scegliere cosa lasciare su quel muro. Ogni giorno, ogni post, ogni commento è una scelta. Scegli bene.

Test di autovalutazione

Indica la risposta corretta per ciascuna domanda. Le risposte si trovano in fondo alla sezione.

1. Come agisce l'effetto di disinibizione sull'aggressore online? a) Lo rende più timido e riservato. b) Riduce i freni inibitori e l'empatia perché la mancanza di contatto visivo "anestetizza" la percezione delle emozioni altrui. c) Rallenta la velocità di scrittura.
2. Interpretare negativamente le intenzioni di qualcuno sulla base di un messaggio ambiguo è un esempio di: a) Bias di conferma. b) Bias di ostilità. c) Effetto tunnel.
3. La Legge 71/2017 cosa prevede per le scuole? a) L'obbligo di sequestrare i telefoni. b) La nomina di un referente e procedure di prevenzione e intervento. c) L'installazione di telecamere.
4. Perché l'impronta digitale è rischiosa? a) Perché rovina lo smartphone. b) Perché incide sulla reputazione futura in modo difficile da controllare. c) Perché rallenta il wi-fi.
5. Qual è lo scopo principale della bias mitigation? a) Usare il pensiero critico per evitare reazioni aggressive alimentate da pregiudizi cognitivi. b) Bloccare i profili falsi. c) Migliorare la grafica dei post.
6. Qual è la prima azione da compiere se si riceve una minaccia online? a) Rispondere con tono fermo. b) Fare uno screenshot e non rispondere. c) Eliminare l'account.
7. Qual è la differenza tra spettatore attivo e alleato? a) Lo spettatore attivo aiuta il bullo; l'alleato aiuta la vittima. b) Sono sinonimi. c) L'alleato è un complice del bullo.

Risposte: 1-b / 2-b / 3-b / 4-b / 5-a / 6-b / 7-a

Glossario essenziale

Alleato: lo spettatore che sceglie di intervenire attivamente in difesa della vittima di cyberbullismo, supportandola e segnalando i contenuti offensivi.

Anonimato (online): la possibilità di agire online nascondendo la propria identità reale. Riduce i freni inibitori ma non protegge dalle conseguenze legali.

Bias cognitivo: distorsione sistematica nel modo in cui si elaborano le informazioni e si prendono decisioni. Il bias di conferma e il bias di ostilità sono particolarmente rilevanti nel contesto delle aggressioni online.

Body shaming: pratica di criticare, deridere o umiliare una persona per il suo aspetto fisico, online o offline.

Catfishing: costruzione di un'identità falsa online per instaurare relazioni ingannevoli con altri utenti.

Cyberbullismo: forma di bullismo perpetrata attraverso dispositivi digitali e piattaforme online. Si distingue dal bullismo tradizionale per pervasività, anonimato, risonanza pubblica e permanenza.

Cyberstalking: persecuzione sistematica attraverso mezzi digitali – messaggi ripetuti, minacce, monitoraggio dei profili social. È perseguibile come atto persecutorio ai sensi dell'art. 612-bis del Codice Penale.

Disinibizione (effetto): fenomeno psicologico per cui la mancanza di contatto visivo online riduce i freni inibitori e la percezione delle emozioni altrui, facilitando comportamenti aggressivi.

Dissing: divulgazione pubblica di informazioni riservate o umilianti riguardanti una persona con l'intento di danneggiarla. Può configurarsi come diffamazione aggravata.

Empatia digitale: la capacità di riconoscere e rispettare le emozioni altrui negli spazi digitali, nonostante l'assenza di contatto fisico diretto.

Garante per la Protezione dei Dati Personali: autorità italiana che tutela la privacy dei cittadini. Ha poteri specifici per richiedere la rimozione di contenuti digitali lesivi entro 48 ore.

Hate speech: discorso d'odio che incita alla discriminazione, all'ostilità o alla violenza verso persone o gruppi in base alla loro identità. Vietato dalla legge italiana e dalle politiche delle piattaforme digitali.

Impronta digitale: l'insieme delle tracce lasciate online dalle proprie attività digitali: post, commenti, like, ricerche, interazioni. Costituisce un curriculum informale che può influenzare la reputazione reale.

Legge 71/2017: prima legge italiana specificamente dedicata al contrasto del cyberbullismo. Prevede strumenti di tutela per i minori, obblighi per le scuole

e procedure di intervento istituzionale.

Netiquette: insieme di norme di comportamento che regolano la comunicazione civile negli spazi digitali. Deriva dall'unione di network ed etichette.

Peer Education: educazione tra pari: strategia formativa in cui persone con caratteristiche simili si trasmettono competenze e comportamenti, risultando spesso più efficace della comunicazione verticale adulto-giovane.

Permanenza (del contenuto digitale): caratteristica del web per cui i contenuti pubblicati sono difficili da eliminare completamente e possono riemergere anche a distanza di anni.

Phishing: tecnica truffaldina che finge di provenire da fonti affidabili per ottenere dati personali, password o informazioni finanziarie.

Polizia Postale: organo specializzato nella gestione dei reati informatici in Italia. È il riferimento principale per le denunce di cyberbullismo e reati digitali.

Revenge porn: diffusione illecita di immagini o video sessualmente espliciti senza il consenso della persona ritratta. È reato specifico in Italia dalla Legge 69/2019, punito con la reclusione da uno a sei anni.

Trolling: pratica di provocare deliberatamente altri utenti online con commenti offensivi o fuori luogo, con l'unico scopo di generare reazioni emotive negative.

Risorse e contatti utili

In caso di episodi di cyberbullismo o per ulteriori informazioni, è possibile rivolgersi alle seguenti risorse.

Polizia Postale: commissariatodips.it — sportello online per segnalare reati informatici e consultare informazioni su truffe e sicurezza digitale.

Garante per la Protezione dei Dati Personali: gdpd.it/cyberbullismo — per richiedere la rimozione di contenuti lesivi della privacy e ottenere informazioni sui propri diritti digitali.

Telefono Azzurro: 19696 — servizio di ascolto e supporto per bambini e adolescenti in difficoltà, operativo tutti i giorni.

Parole O_Stili: paroleostili.it — progetto culturale che promuove un uso responsabile e rispettoso delle parole online.

TEMA B
SICUREZZA E USO CONSAPEVOLE
DEI SERVIZI DIGITALI

-  **SICUREZZA DIGITALE E ALFABETIZZAZIONE**
SU INFORMAZIONE E DATI



Digita Facile
Campania

Presentazione del capitolo

Questo capitolo accompagna il percorso formativo dedicato alla Sicurezza Digitale e all'Alfabetizzazione su Informazione e Dati, sviluppato nell'ambito del progetto Digita Facile Campania. Si rivolge a chiunque voglia orientarsi con maggiore consapevolezza nel mondo digitale: capire come funziona la rete, riconoscere i siti sicuri da quelli pericolosi, valutare l'affidabilità di una notizia, gestire le proprie comunicazioni online e creare contenuti digitali in modo responsabile.

Il capitolo è articolato in due grandi moduli tematici. Il primo – Fondamentali della Navigazione Digitale – introduce gli strumenti di base per navigare in rete: browser, motori di ricerca, tecniche di ricerca avanzata, verifica della sicurezza dei siti web e valutazione dell'autorevolezza delle fonti. Il secondo – Fondamentali della Comunicazione Digitale – approfondisce gli strumenti di comunicazione online – email, messaggistica, social network – e le competenze per creare e condividere contenuti in modo efficace e rispettoso delle normative sul diritto d'autore. Non è richiesta alcuna competenza tecnica per seguire questa dispensa. È sufficiente la curiosità di capire meglio come funziona il mondo digitale e la voglia di usarlo in modo più sicuro, consapevole e creativo. Ogni strumento che imparerai a conoscere è qualcosa che puoi usare da subito nella tua vita quotidiana.

Questo capitolo è pensato per essere usato, non solo letto. Tienilo vicino quando navighi, quando ricevi un'email sospetta, quando devi valutare una notizia o quando vuoi creare un documento condiviso. È un manuale pratico di cittadinanza digitale.

La rete come opportunità: navigare con consapevolezza

Il digitale è ovunque: saper navigare è saper vivere

Internet ha smesso da tempo di essere uno strumento per specialisti o per giovani tecnologici. È diventato il canale principale attraverso cui si accede a una quantità enorme di servizi essenziali: la prenotazione di una visita medica, la consultazione dei propri documenti fiscali, la comunicazione con enti pubblici, la ricerca di un lavoro, l'accesso a informazioni di ogni tipo. Chi non sa orientarsi in questo spazio non è soltanto meno efficiente: è meno libero, perché dipende dagli altri per accedere a servizi che dovrebbero essere alla portata di tutti.

Ma la rete non è soltanto uno strumento di accesso ai servizi: è anche lo spazio in cui si forma l'opinione pubblica, in cui circolano notizie vere e false, in cui si costruiscono e si distruggono reputazioni, in cui si esprimono creatività e

cultura. Saper navigare bene significa non solo trovare quello che si cerca, ma anche saper valutare quello che si trova, riconoscere le trappole, proteggersi dai rischi e contribuire in modo positivo allo spazio comune digitale.

I rischi reali di una navigazione inconsapevole

La mancanza di competenze digitali di base non è soltanto una questione di disagio o di inefficienza: può avere conseguenze concrete e serie. Chi non sa riconoscere un sito falso può inserire i propri dati bancari su una pagina truffaldina e perdere denaro. Chi non sa valutare l'affidabilità di una notizia può contribuire alla diffusione di disinformazione. Chi non conosce le regole di base della privacy può condividere inconsapevolmente informazioni sensibili con persone o organizzazioni che non dovrebbero averle. Questi non sono rischi teorici: sono situazioni che accadono ogni giorno, a persone di ogni fascia d'età e di ogni livello di istruzione. Il phishing – le email o i messaggi che fingono di provenire da banche, corrieri o enti pubblici per ottenere dati personali – è aumentato in modo esponenziale negli ultimi anni e colpisce anche persone che si considerano abbastanza esperte. Le fake news circolano su piattaforme usate da miliardi di persone e influenzano decisioni politiche, sanitarie, economiche. La sicurezza digitale non è un argomento per tecnici: è una competenza di sopravvivenza nell'era contemporanea.

Obiettivi del modulo

Al termine di questo modulo conoscerai i principali browser e saprai scegliere quello più adatto alle tue esigenze. Comprenderai come funziona un motore di ricerca e saprai usare tecniche di ricerca avanzata per trovare informazioni più precise e affidabili. Sarai in grado di verificare la sicurezza di un sito web, riconoscere i principali tentativi di inganno attraverso URL falsificati e valutare l'affidabilità di una notizia senza cadere nelle trappole del clickbaiting e dei bias cognitivi.

Gli strumenti per navigare: i browser

Il browser è il programma attraverso cui accediamo al web: è la finestra attraverso cui guardiamo internet. La sua storia inizia nel 1990 grazie all'informatico britannico Tim Berners-Lee, il “padre” del World Wide Web. Per permettere alle persone di esplorare questa sua nuova invenzione, Berners-Lee sviluppò il primo software di navigazione della storia. Inizialmente battezzato proprio WorldWideWeb, il programma venne poco dopo rinominato in Nexus per evitare che il nome si confondesse con la rete stessa. Da quel primo, fondamentale strumento pionieristico, l'offerta si è moltiplicata. Oggi ne esistono diversi, ognuno con caratteristiche specifiche che lo rendono più o meno adatto a certi usi:

- **Google Chrome:** È il browser più diffuso al mondo, con una quota di mercato che supera il 60%. È veloce, compatibile con la quasi totalità dei siti web e fortemente integrato con gli altri servizi Google – Gmail, Drive, Maps. Il suo punto debole è la gestione dei dati: Chrome raccoglie molte informazioni sulle abitudini di navigazione degli utenti, che vengono utilizzate per personalizzare la pubblicità.
- **Apple Safari:** È il browser preinstallato su tutti i dispositivi Apple – iPhone, iPad, Mac – ed è ottimizzato per funzionare al meglio su questi dispositivi, con un'ottima gestione dell'autonomia della batteria. Offre buone funzionalità di privacy ed è la scelta naturale per chi è immerso nell'ecosistema Apple.
- **Microsoft Edge:** È il browser sviluppato da Microsoft e preinstallato su Windows. La versione attuale, basata sullo stesso motore di Chrome, è significativamente migliorata rispetto al passato e offre funzionalità interessanti come la modalità di lettura, l'integrazione con strumenti di Intelligenza Artificiale e una gestione discreta della privacy.

I paladini della privacy (Firefox, Brave, Opera): Se la priorità è la riservatezza online, esiste una schiera di browser dedicata alla protezione dei dati personali:

- **Mozilla Firefox:** Un browser open-source — il cui codice è pubblico e controllabile da chiunque — sviluppato da una fondazione senza scopo di lucro. Ha una solida reputazione in materia di privacy e offre moltissime estensioni per bloccare i tracker pubblicitari.
- **Brave:** Un browser che fa della privacy la sua missione principale. Blocca di default gli annunci invasivi e i tracciati di terze parti, garantendo una navigazione che risulta non solo protetta, ma anche molto più veloce.
- **Opera:** Si distingue in questa categoria per l'inclusione nativa di strumenti per l'anonimato, offrendo una comoda VPN gratuita integrata nel browser e un ad-blocker efficace senza bisogno di installare estensioni esterne.

Anatomia di un browser: gli strumenti essenziali

Indipendentemente dal browser che si usa, alcuni elementi sono comuni a tutti e vale la pena conoscerli bene perché si usano ogni giorno.

La barra degli indirizzi — detta URL bar — è la riga in alto in cui si digita l'indirizzo del sito che si vuole visitare. È anche il luogo in cui si può digitare direttamente una ricerca, che viene automaticamente elaborata dal motore di ricerca predefinito. Leggere con attenzione l'indirizzo che compare in questa barra è uno dei gesti più importanti per la sicurezza online: è lì che si nascondono molti tentativi di inganno.

La gestione delle schede permette di tenere aperte più pagine contemporaneamente nello stesso browser, passando dall'una all'altra con un clic. È uno strumento di produttività fondamentale, ma attenzione: troppo schede aperte consumano memoria e possono rallentare il dispositivo.

I segnalibri — o **preferiti** — permettono di salvare gli indirizzi dei siti che si visitano più spesso per trovarli rapidamente senza doverli cercare ogni volta. Organizzarli in cartelle tematiche è un'abitudine semplice che fa risparmiare molto tempo.

La navigazione in incognito — chiamata anche navigazione privata — è una modalità in cui il browser non salva la cronologia delle pagine visitate, i cookie e i dati inseriti nei moduli. È utile quando si usa un dispositivo condiviso o quando si vuole fare una ricerca senza che influenzi le raccomandazioni future. Attenzione però: la navigazione in incognito non rende anonimi su internet — il fornitore di connessione e i siti visitati possono comunque registrare l'attività — ma impedisce soltanto che quella sessione venga salvata localmente sul dispositivo.

Come funziona un motore di ricerca

Un motore di ricerca – come Google, Bing o DuckDuckGo – è un sistema automatizzato che esplora continuamente il web alla ricerca di nuovi contenuti, li cataloga e li rende ricercabili dagli utenti. Il processo si articola in tre fasi fondamentali.

Il web crawling è la fase di esplorazione: programmi automatici detti spider o crawler percorrono continuamente la rete seguendo i link da una pagina all'altra, raccogliendo il contenuto di ogni pagina che visitano.

L'indexing è la fase di catalogazione: i contenuti raccolti vengono analizzati, classificati e inseriti in un archivio gigantesco – l'indice del motore di ricerca – organizzato in modo da permettere ricerche veloci. Il ranking è la fase di classificazione dei risultati: quando si inserisce una query – una richiesta di ricerca – il motore analizza l'indice e restituisce i risultati in ordine di pertinenza, usando algoritmi complessi che valutano decine di fattori (ranking). Tra i principali motori di ricerca, Google è il leader assoluto con una quota di mercato superiore al 90% a livello mondiale. Bing, sviluppato da Microsoft, è il secondo più usato e si distingue per la progressiva integrazione con strumenti di Intelligenza Artificiale. DuckDuckGo è il motore di ricerca che non traccia i dati degli utenti: non crea profili personali, non personalizza i risultati in base alla cronologia e non vende dati a inserzionisti pubblicitari. È la scelta ideale per chi vuole proteggere la propria privacy nelle ricerche.

Tecniche di ricerca avanzata

Sapere come si costruisce una buona query di ricerca è una competenza preziosa che fa risparmiare tempo e produce risultati molto più precisi. Alcune tecniche semplici ma efficaci permettono di sfruttare al meglio i motori di ricerca. Gli operatori logici sono simboli o parole che modificano la logica della ricerca. Le virgolette – “parola esatta” – costringono il motore a cercare esattamente quella sequenza di parole, non le singole parole separate. Il segno meno – parola -esclusione – esclude dai risultati le pagine che contengono una certa parola. L'operatore site: – site: governo.it parola – limita la ricerca a un sito specifico. L'operatore filetype: – filetype: pdf argomento – cerca soltanto file di un tipo specifico. **Inquadra il QR code per scaricare la guida su tutti i principali operatori logici.**



La ricerca inversa per immagini permette di trovare la fonte originale di una foto o di verificare se un'immagine è stata usata in contesti diversi da quello in

cui viene presentata. È uno strumento potente per smascherare le fake news che usano foto decontestualizzate: si carica l'immagine sul motore di ricerca – su Google Immagini c'è l'icona a forma di fotocamera nella barra di ricerca – e si vedono tutti i contesti in cui quella foto è stata pubblicata. Google Lens è uno strumento di riconoscimento visivo disponibile sugli smartphone Android e tramite l'app Google: puntando la fotocamera su un oggetto, un testo o un'immagine, è in grado di identificarlo, tradurlo, fornire informazioni su di esso o trovarne versioni simili online. È uno strumento particolarmente utile per tradurre testi in lingue straniere in tempo reale o per identificare prodotti, piante, monumenti.

Consiglio pratico: La prossima volta che ricevi una notizia con una foto che sembra strana o improbabile, prova la ricerca inversa per immagini. In pochi secondi puoi scoprire se quella foto è davvero collegata alla notizia o se è stata presa da un contesto completamente diverso.

Verificare la sicurezza di un sito web

Non tutti i siti web sono quello che sembrano. Ogni anno milioni di persone vengono truffate inserendo i propri dati personali o finanziari su siti falsi che imitano quelli originali. Sapere come verificare la sicurezza di un sito prima di inserirvi qualsiasi dato sensibile è una delle competenze digitali più importanti.

Il primo indicatore da controllare è il protocollo: HTTPS o HTTP? La sigla HTTPS – **HyperText Transfer Protocol Secure** – indica che la connessione tra il browser e il sito è cifrata tramite un protocollo di sicurezza chiamato SSL/TLS. In pratica, significa che i dati che si inseriscono nel sito non possono essere intercettati durante il loro percorso. Il lucchetto che compare nella barra degli indirizzi accanto all'URL certifica che la connessione è cifrata. La regola è semplice: non inserire mai dati sensibili – password, numero di carta di credito, codice fiscale – su un sito il cui indirizzo non inizia con HTTPS.

Il secondo elemento da controllare è il dominio, ovvero la parte centrale dell'URL – quella che precede il .com, .it, .org e così via. I truffatori usano alcune tecniche specifiche per ingannare gli utenti. Il typosquatting consiste nel registrare domini con piccoli errori tipografici rispetto a quelli originali: amazOn.it con uno zero invece della "o", arrazon.it con due "r" che a prima vista sembrano una "m". I sottodomini ingannevoli sfruttano la struttura degli URL per confondere: paypal.conferma-dati.com sembra contenere la parola PayPal, ma in realtà il sito è conferma-dati.com, non paypal.com. Le estensioni insolite – .xyz, .top, .click – sono spesso usate per siti fraudolenti perché costano pochissimo da registrare.

Regola d'oro: Prima di inserire qualsiasi dato sensibile su un sito, controlla l'URL con attenzione. Leggi il dominio da destra verso sinistra: l'ultimo punto prima del / è dove si trova il dominio principale. Se non è quello che ti aspetti, non procedere.

Obiettivi del modulo

Al termine di questo modulo padroneggerai le funzionalità essenziali dell'e-mail, incluse le regole di privacy per l'invio a più destinatari. Conoscerai le principali app di messaggistica e saprai usarle in modo sicuro. Comprenderai le differenze tra social network e forum e saprai creare e condividere contenuti digitali in modo efficace e responsabile. Conoscerai le basi del diritto d'autore e delle licenze Creative Commons.

COMUNICAZIONE ASINCRONA: L'EMAIL

Molto più di un semplice messaggio

L'email — posta elettronica — è lo strumento di comunicazione digitale più formale e più longevo: esiste dagli anni Settanta e continua a essere il canale principale per le comunicazioni professionali e istituzionali. A differenza dei messaggi istantanei, è uno strumento asincrono — non richiede che entrambi i partecipanti siano connessi nello stesso momento — e si presta a comunicazioni strutturate, con allegati, riferimenti e archivio.

L'anatomia base di una casella email include la cartella Posta in arrivo, dove arrivano i messaggi ricevuti; la cartella Posta inviata, che conserva i messaggi spediti; le Bozze, dove vengono salvati automaticamente i messaggi iniziati ma non ancora inviati; e la cartella Spam, dove finiscono i messaggi che il sistema giudica indesiderati o potenzialmente pericolosi. Controllare periodicamente la cartella Spam è importante: a volte vi finiscono messaggi legittimi che meritano attenzione.

A, CC e CCN: privacy nella comunicazione di gruppo

Quando si invia un'email a più persone, la scelta del campo in cui inserire i destinatari ha implicazioni importanti per la privacy.

Il campo A — **destinatario principale** — è per chi deve leggere il messaggio e rispondere. Tutti i destinatari inseriti in questo campo sono visibili a tutti gli altri.

Il campo CC — **Copia Conoscenza** — è per chi deve essere tenuto informato ma non deve necessariamente rispondere. Anche in questo caso, tutti i destinatari in CC sono visibili a tutti i destinatari del messaggio, compresi quelli nel campo A.

Il campo CCN — **Copia Conoscenza Nascosta** — è lo strumento fondamentale per proteggere la privacy nelle comunicazioni di gruppo. I destinatari inseriti in CCN ricevono il messaggio ma il loro indirizzo non è visibile agli altri desti-

natari. È essenziale usare CCN quando si invia un'email a un gruppo di persone che non necessariamente si conoscono tra loro: usare il campo A o CC in queste situazioni significa rivelare a tutti i presenti gli indirizzi email degli altri, il che può violare la loro privacy.

Usare il campo A o CC per inviare un'email a un gruppo di persone che non si conoscono tra loro è una violazione della privacy di tutti i destinatari. Usa sempre CCN in questi casi. È una questione di rispetto e, in certi contesti professionali, di conformità al GDPR.

Regole di etichetta e sicurezza nell'uso dell'email

Alcune regole semplici rendono la comunicazione email più efficace, più professionale e più sicura. Inserire sempre un oggetto chiaro e specifico è la prima regola. Un'email senza oggetto, o con un oggetto generico come "Info" o "Ciao", rischia di non essere aperta o di finire nello spam. L'oggetto dovrebbe riassumere in modo preciso il contenuto del messaggio. Non scrivere tutto in maiuscolo. Su internet – e in particolare nelle email – scrivere in maiuscolo equivale a urlare. È percepito come aggressivo e poco professionale, anche quando non è l'intenzione. Allegati e dimensioni: la maggior parte dei provider email impone un limite massimo alle dimensioni degli allegati – tipicamente 25 MB. Per inviare file più grandi, è preferibile usare un servizio di condivisione cloud – come Google Drive o WeTransfer – e inserire il link nell'email.

Il **phishing** via email è la minaccia più frequente che si incontra nella gestione della posta elettronica. Le email di phishing fingono di provenire da banche, corrieri, servizi di pagamento, enti pubblici o aziende tecnologiche e cercano di convincere il destinatario a cliccare su un link o a fornire dati personali. I segnali da cercare sono: mittente con indirizzo sospetto, tono di urgenza artificiale, link che non corrispondono al dominio indicato, richieste di informazioni che nessuna banca o istituzione legittima farebbe via email.

COMUNICAZIONE SINCRONA: APP DI MESSAGGISTICA

Comunicare in tempo reale

Le **app di messaggistica** – WhatsApp, Telegram, Messenger e simili – hanno rivoluzionato la comunicazione quotidiana. Basate su connessione internet anziché su rete telefonica tradizionale come gli SMS, permettono di inviare testo, foto, video, documenti e messaggi vocali in tempo reale, individualmente o in gruppo, a costo praticamente nullo. Le funzionalità principali di queste app includono i gruppi – conversazioni con più persone contemporaneamente, molto utili per famiglie, gruppi di lavoro, associazioni – le broadcast list – che permettono di inviare lo stesso messaggio a più contatti senza creare un gruppo – i messaggi vocali e le videochiamate.

La sicurezza nelle app di messaggistica (si definisce **Smishing** l'attività fraudolenta legata a questi strumenti) richiede alcune precauzioni specifiche. Il livello di confidenza che caratterizza queste comunicazioni — spesso si scrive ad amici e familiari, in un tono informale — abbassa naturalmente la guardia. Ma i rischi esistono: link ingannevoli possono arrivare anche da contatti fidati — se il loro account è stato compromesso o se hanno ricevuto a loro volta un messaggio virale senza verificarlo; le catene virali — messaggi che invitano a condividere con tutti i propri contatti — diffondono spesso informazioni false o allarmistiche; i profili clonati — qualcuno che si finge un tuo contatto creando un profilo simile — possono tentare di estorcere denaro o informazioni.

Regola pratica: Prima di cliccare su un link ricevuto via WhatsApp o Telegram — anche da un numero conosciuto — chiediti: me lo aspettavo? Ha senso che questa persona me lo mandi? Se hai il minimo dubbio, verifica direttamente con il contatto tramite una telefonata o un messaggio separato.

AGORÀ VIRTUALI: I SOCIAL NETWORK

Social network e forum: spazi diversi per scopi diversi

I social network — Facebook, Instagram, LinkedIn, X — sono piattaforme orizzontali costruite intorno al profilo personale. Ognuno ha un profilo che rappresenta la propria identità online, una rete di contatti, e un feed — un flusso di contenuti — personalizzato dall'algoritmo. Sono ambienti ad alta visibilità e ad alto impatto emotivo: i contenuti possono raggiungere migliaia o milioni di persone, e le interazioni — like, commenti, condivisioni — hanno un peso sociale percepito.

I forum sono comunità verticali organizzate intorno a un argomento specifico. La struttura è diversa: si organizzano in thread — discussioni su un tema preciso — e la partecipazione è motivata dall'interesse per l'argomento più che dalla costruzione di un'identità pubblica. I forum specializzati — su salute, tecnologia, cucina, hobby specifici — sono spesso fonte di informazioni molto più approfondite e affidabili dei social network sugli stessi temi, perché il livello di competenza dei partecipanti è mediamente più alto e il tono è meno emotivo.



RISCHI E VANTAGGI DELL'INFORMAZIONE DIGITALE

Verificare l'affidabilità di una notizia

Nell'era dell'informazione digitale, la capacità di distinguere le notizie affidabili da quelle false o manipolate è diventata una competenza fondamentale. La disinformazione — la diffusione intenzionale di informazioni false — non è un problema marginale: influenza elezioni, alimenta odio, mina la fiducia nelle istituzioni e può avere conseguenze concrete sulla salute pubblica.

Il primo criterio di valutazione è la **gerarchia delle fonti**. Le fonti primarie sono quelle che riportano i dati direttamente — studi scientifici originali, comunicati ufficiali di enti o governi, testimonianze dirette. Le fonti secondarie — articoli giornalistici, analisi, commenti — elaborano le informazioni delle fonti primarie. Più ci si allontana dalla fonte primaria, maggiore è il rischio di distorsioni, semplificazioni o manipolazioni. Quando si legge una notizia importante, cercare la fonte primaria da cui proviene è sempre il passo più utile.

Il secondo criterio è **l'anatomia della fonte**: chi ha scritto il contenuto? È un esperto riconosciuto nel settore di cui si parla? Il sito ha uno scopo informativo o ha un interesse a presentare le cose in un certo modo? Quando è stato pubblicato il contenuto? La data di pubblicazione è fondamentale: un articolo del 2018 presentato come notizia di oggi è già di per sé una forma di manipolazione. Le informazioni sono verificabili su altre fonti indipendenti?

Il **clickbaiting** è una tecnica di manipolazione emotiva ampiamente usata per aumentare i clic su contenuti di scarsa qualità. Si basa su titoli che sfruttano il curiosity gap — ti dicono che c'è qualcosa di interessante senza rivelartelo subito, costringendoti a cliccare — o che usano emozioni intense come la paura, la rabbia, l'indignazione, per attivare reazioni impulsive. Titoli come “Non crederai mai a quello che ha fatto il governo” o “Il rimedio che le case farmaceutiche non vogliono che tu sappia” sono esempi classici. Imparare a riconoscerli e a non reagire automaticamente è una difesa fondamentale contro la disinformazione.

Le dinamiche cognitive dei social network

I social network non sono soltanto strumenti di comunicazione: sono ambienti progettati per massimizzare il tempo che gli utenti trascorrono al loro interno. Gli algoritmi che decidono quali contenuti mostrare sono ottimizzati per l'engagement — il coinvolgimento — non per la verità o la qualità dell'informazione. Questo ha conseguenze cognitive importanti che vale la pena comprendere.

La **filter bubble** — bolla dei filtri — è il fenomeno per cui l'algoritmo, imparando progressivamente cosa ci piace, ci mostra sempre più contenuti simili a quelli

con cui abbiamo già interagito. Il risultato è che la nostra visione del mondo online diventa progressivamente più ristretta e omogenea: vediamo sempre le stesse voci, sempre le stesse opinioni, sempre le stesse prospettive. Questo non soltanto limita la nostra comprensione della realtà: favorisce la polarizzazione, perché non ci espone mai a punti di vista diversi dai nostri.

La **polarizzazione** è la tendenza a spostarsi progressivamente verso posizioni sempre più estreme su un argomento controverso. I contenuti che generano più engagement – cioè più reazioni, commenti, condivisioni – sono quasi sempre quelli emotivamente carichi, quelli che suscitano indignazione o entusiasmo intenso. Gli algoritmi li amplificano. Il risultato è che le posizioni moderate vengono progressivamente silenziose, mentre quelle estreme diventano sempre più visibili e percepite come rappresentative.

Le **cascate informative** descrivono la tendenza a condividere contenuti senza leggerli o verificarli, semplicemente perché lo stanno facendo molte altre persone. Questo meccanismo – simile al comportamento di gregge – è uno dei principali vettori di diffusione delle fake news: una notizia falsa ma emotivamente coinvolgente può essere condivisa milioni di volte in poche ore da persone che non l'hanno mai letta per intero.

Il **rinforzo positivo** è il meccanismo psicologico più potente che le piattaforme usano per creare dipendenza. Ogni like, ogni commento, ogni condivisione che riceviamo genera un piccolo rilascio di dopamina – il neurotrasmettitore associato alla ricompensa. Il cervello si abitua a cercare questi rinforzi, modificando progressivamente il comportamento online in direzione di ciò che li produce. Comprendere questo meccanismo non significa smettere di usare i social network: significa usarli con consapevolezza, sapendo che il loro design è ottimizzato per tenerci incollati agli schermi più a lungo possibile.

Il fatto che tu stia leggendo questa dispensa – invece di scorrere passivamente un feed di social network – è già un atto di consapevolezza digitale. La conoscenza di questi meccanismi non li disattiva automaticamente, ma ti dà gli strumenti per riconoscerli quando li senti agire su di te.

Creare contenuti digitali: strumenti e opportunità

Internet non è soltanto un luogo in cui si consumano contenuti: è un luogo in cui si possono creare. Gli **User Generated Content** – UGC, contenuti creati dagli utenti – sono il motore che dà valore alle piattaforme digitali. Post, video, foto, recensioni, blog, podcast: sono tutti contenuti che qualcuno ha creato e che contribuiscono a costruire la conoscenza collettiva accessibile in rete.

Il **cloud computing** ha rivoluzionato la creazione di contenuti digitali. Strumenti come Google Workspace – che comprende Google Documenti, Fogli e Presentazioni – permettono di creare, modificare e condividere documenti direttamente nel browser, senza installare alcun software, con salvataggio automatico e accessibilità da qualsiasi dispositivo. La possibilità di lavorare simultaneamente sullo stesso file – il co-editing – elimina il problema delle versioni multiple e dei file allegati nelle email, semplificando enormemente la collaborazione.

Per la **grafica e il design**, Canva è lo strumento più accessibile: offre migliaia di modelli preconfezionati per creare presentazioni, post social, locandine, curriculum e molto altro, con un'interfaccia drag-and-drop che non richiede competenze grafiche. Per chi vuole andare oltre, Photopea è un editor di immagini professionale – simile a Photoshop – accessibile gratuitamente via browser. Per il montaggio video, DaVinci Resolve è un software professionale usato anche nelle produzioni cinematografiche e disponibile gratuitamente; Shotcut è un'alternativa più intuitiva per chi si avvicina per la prima volta al montaggio.

Condividere in sicurezza: la gestione dei permessi

Quando si condividono documenti o file tramite servizi cloud, è fondamentale gestire correttamente i permessi di accesso. Condividere un file senza le giuste impostazioni può renderlo accessibile a persone non autorizzate.

Tutti i principali servizi di condivisione cloud – Google Drive, OneDrive, Dropbox – offrono tre livelli di permesso. Il permesso di lettura permette all'utente di vedere il contenuto del file ma non di modificarlo. Il permesso di commento permette di aggiungere note e suggerimenti ma non di alterare il testo originale. Il permesso di modifica dà pieno controllo sul file: l'utente può cambiarne il contenuto, cancellare parti, aggiungere sezioni. È importante assegnare sempre il livello di permesso minimo necessario: se qualcuno deve solo leggere un documento, non dargli il permesso di modifica.

Attenzione anche alle impostazioni di condivisione generale: un link di con-

divisione impostato su “chiunque abbia il link” significa che chiunque riceva quel link – anche per sbaglio – può accedere al file. Per contenuti sensibili, è sempre meglio condividere direttamente con gli indirizzi e-mail delle persone autorizzate, non attraverso un link pubblico. I file in cloud sono al sicuro da guasti del dispositivo locale, ma non da cancellazioni accidentali o da accessi non autorizzati all'account. Per i dati più importanti è buona norma mantenere copie su più supporti. La regola 3-2-1 suggerita dai professionisti della sicurezza prevede tre copie dei dati, su due supporti diversi, di cui uno conservato in luogo diverso dalla sede principale.

Diritto d'autore e licenze Creative Commons

Ogni contenuto creato da un essere umano – testo, immagine, video, musica, software – è protetto automaticamente dal diritto d'autore nel momento stesso in cui viene creato. Non è necessario registrarlo, non è necessario apporvi alcun simbolo: la protezione è automatica e dura per tutta la vita dell'autore e per un periodo variabile dopo la sua morte.

Il **copyright** – simboleggiato dal simbolo © – significa “tutti i diritti riservati”: non è possibile usare, riprodurre o modificare il contenuto senza esplicita autorizzazione da parte del titolare dei diritti, che può essere l'autore o chi ha acquisito i diritti per contratto. Usare immagini, musica o testi protetti da copyright senza autorizzazione – anche solo in un post sui social o in una presentazione – è una violazione della legge, anche se sembra un gesto innocuo.

Il **dominio pubblico** comprende le opere non più soggette a restrizioni d'uso perché la protezione del copyright è scaduta – in Italia, settant'anni dopo la morte dell'autore – o perché l'autore ha esplicitamente rinunciato ai diritti. Le opere in dominio pubblico possono essere usate, riprodotte e modificate liberamente.

Le **licenze Creative Commons** sono uno strumento intermedio creato per permettere agli autori di concedere alcuni diritti d'uso delle proprie opere mantenendo altri. Esistono diverse combinazioni di condizioni: l'Attribuzione – BY – richiede di citare l'autore; Non Commerciale – NC – impedisce l'uso a scopo di lucro; Non Opere Derivate – ND – impedisce di modificare l'opera; Condividi allo stesso modo – SA – richiede che le opere derivate siano distribuite con la stessa licenza. Le licenze Creative Commons sono ampiamente usate nel mondo della formazione, della ricerca e della cultura open source.

Dove trovare immagini libere: Unsplash, Pixabay e Pexels offrono fotografie di alta qualità gratuite e libere da copyright per uso personale e commerciale. Google Immagini permette di filtrare i risultati per tipo di licenza nella sezione Strumenti. Wikimedia Commons è il repository di media dell'enciclopedia Wikipedia e contiene milioni di immagini, video e audio liberamente utilizzabili.

La password: prima linea di difesa

Le password sono le chiavi di accesso ai nostri spazi digitali: e-mail, servizi bancari, profili social, documenti cloud. Eppure, la maggior parte delle persone gestisce le proprie password in modo pericolosamente superficiale. Secondo le ricerche sulla sicurezza informatica, le password più usate al mondo continuano ad essere combinazioni elementari come sequenze numeriche semplici, il proprio nome o la data di nascita. Questi dati non sono sorprendenti — creare e ricordare password sicure è scomodo — ma le conseguenze di una password debole o riutilizzata possono essere molto serie.

Una password sicura ha almeno dodici caratteri e include lettere maiuscole e minuscole, numeri e simboli. Non contiene parole di senso compiuto in nessuna lingua, non include informazioni personali facilmente reperibili — nome, data di nascita, nome di animali domestici — e non è la stessa usata su altri account. Quest'ultimo punto è cruciale: se si usa la stessa password su dieci siti diversi e uno di quei siti subisce una violazione dei dati, tutti e dieci gli account sono compromessi. Il modo più pratico per gestire password sicure e diverse per ogni servizio è usare un gestore di password: un programma che le crea, le memorizza e le inserisce automaticamente. Bitwarden, 1Password e i gestori integrati nei browser sono opzioni valide. Il gestore di password è a sua volta protetto da un'unica password maestra — quella si deve ricordare davvero bene — o da un sistema biometrico come l'impronta digitale.

L'autenticazione a due fattori

Anche la password più robusta può essere compromessa attraverso violazioni di dati, phishing sofisticato o software di intercettazione. Per questo motivo, la sicurezza moderna raccomanda di aggiungere un secondo livello di verifica: l'autenticazione a due fattori, detta 2FA. Il principio è semplice: per accedere a un account non basta sapere la password, bisogna anche avere accesso a un secondo elemento — tipicamente uno smartphone. La 2FA è disponibile su quasi tutti i principali servizi online ed è gratuita. Attivarla sugli account più importanti — e-mail, banca, profili di lavoro — è una delle misure di sicurezza con il miglior rapporto tra semplicità ed efficacia.

I dati personali: cosa proteggere e come

Nell'ecosistema digitale, i dati personali hanno un valore economico reale. Le piattaforme gratuite — social network, motori di ricerca, servizi e-mail — non sono davvero gratuite: il loro modello di business si basa sulla raccolta, l'analisi e la vendita di dati sugli utenti a inserzionisti pubblicitari. I dati più sensibili — credenziali di accesso, dati bancari, codice fiscale, informazioni sanitarie — non vanno mai condivisi in canali non verificati e vanno protetti con partico-

lare attenzione. Il GDPR garantisce a ogni cittadino europeo il diritto di sapere quali dati possiede un'organizzazione su di lui e di richiederne la cancellazione: una protezione legale importante, che si affianca alla consapevolezza individuale.

Consiglio: Controlla periodicamente le app collegate ai tuoi account Google o Facebook. Nelle impostazioni dell'account, cerca la sezione dedicata alle app di terze parti e revoca l'accesso a quelle che non usi più o che non riconosci.

LE TRUFFE ONLINE: RICONOSCERLE E DIFENDERSI

Il panorama delle truffe digitali

Le truffe online sono cresciute in modo esponenziale negli ultimi anni. Secondo i dati della Polizia Postale, ogni anno in Italia vengono denunciate centinaia di migliaia di reati informatici, con danni economici miliardari. Le vittime non sono soltanto anziani o persone poco istruite: chiunque può essere truffato, specialmente quando la truffa è ben costruita e sfrutta momenti di distrazione o di stress emotivo. Le truffe digitali sfruttano principalmente tre leve psicologiche: l'urgenza artificiale – bisogna agire subito, senza tempo per riflettere – l'autorità percepita – il messaggio sembra provenire da una banca, un corriere, un ente pubblico – e la ricompensa promessa – un pacco da ritirare, un rimborso, un premio. Riconoscere queste leve è il primo passo per non cadere nella trappola.

Il phishing nelle sue forme moderne

Il phishing avanzato non si limita più alle email scritte in italiano stentato. Le versioni moderne sono sofisticate: usano loghi ufficiali riprodotti fedelmente, toni formali, indirizzi email che si distinguono dall'originale solo per un carattere, e link che puntano a siti che copiano quasi perfettamente quelli reali. Lo smishing è la versione via SMS, il vishing è la versione telefonica. Il principio per difendersi è sempre lo stesso: nessuna banca, nessun ente pubblico e nessun servizio legittimo chiede mai credenziali, password o dati bancari via email, SMS o telefono. Mai.

Le truffe sugli acquisti online

Le piattaforme di vendita secondaria – marketplace, gruppi social, annunci su siti dedicati – sono terreno fertile per chi vende prodotti che non esistono o che non verranno mai spediti. I segnali di allarme da riconoscere: prezzi significativamente inferiori al mercato, venditori senza storia verificabile, richieste di pagamento con metodi non tracciabili – ricariche telefoniche, criptovalute, bonifici a privati – e pressione a concludere rapidamente la transazione.

Per ridurre il rischio: usare metodi di pagamento che offrono protezione all'acquirente come carte di credito o PayPal, verificare la reputazione del venditore su più fonti indipendenti come Trustpilot o Google Reviews, e cercare online il nome del venditore accompagnato dalla parola 'truffa' prima di procedere all'acquisto.

Le truffe romantiche

Le truffe romantiche sfruttano il desiderio di connessione emotiva. Un profilo falso costruisce progressivamente una relazione affettiva – spesso per mesi – prima di presentare una richiesta di denaro motivata da un'emergenza

improvvisa. La distanza geografica presentata come motivo dell'assenza di incontri reali è quasi sempre un segnale di allarme. Il segnale principale rimane sempre lo stesso: qualcuno che non si è mai incontrato di persona chiede denaro.

Cosa fare se si è vittime di una truffa

La reazione più comune è la vergogna: si tende a nascondere l'accaduto per paura di essere giudicati ingenui. Ma le truffe sfruttano vulnerabilità psicologiche universali: essere stati truffati non è un segno di stupidità, e non denunciare aiuta i truffatori a colpire altre persone. Le azioni da compiere nell'ordine: bloccare immediatamente la carta e avvertire la banca, cambiare le password degli account coinvolti, raccogliere prove – screenshot, ricevute – e sporgere denuncia alla Polizia Postale in presenza o su [commissariatodips.it](https://www.commissariatodips.it).

Non trasferire mai denaro a qualcuno conosciuto solo online. Non inserire dati bancari su siti non verificati. Non chiamare numeri comparsi in avvisi a schermo. Non concedere accesso remoto al proprio dispositivo a chi lo richiede. I truffatori creano urgenza artificiale: fermarsi e verificare è sempre la scelta giusta.

L'AI nella vita quotidiana: già presente, spesso invisibile

L'Intelligenza Artificiale è diventata in pochi anni uno strumento di uso quotidiano. I suggerimenti personalizzati dei servizi streaming, la correzione automatica dello smartphone, il riconoscimento facciale nelle foto, la traduzione istantanea, i filtri antispam dell'email: sono tutti alimentati da sistemi di AI. Più recentemente, i modelli linguistici di grande scala hanno portato queste tecnologie a un livello di accessibilità e capacità senza precedenti: strumenti come ChatGPT o Gemini sono in grado di scrivere testi coerenti su qualsiasi argomento, rispondere a domande complesse, generare immagini realistiche. Queste capacità aprono opportunità straordinarie — e aprono anche scenari inediti per la produzione di contenuti falsi con un livello di verosimiglianza mai visto prima.

I deepfake: quando vedere non è più credere

I deepfake sono contenuti audiovisivi generati o modificati dall'AI in modo da sembrare autentici. Fino a pochi anni fa creare un deepfake convincente richiedeva attrezzature costose e competenze avanzate. Oggi è accessibile a chiunque, e i risultati sono spesso indistinguibili da video reali. Un video deepfake può mostrare un politico fare dichiarazioni che non ha mai fatto, o falsificare prove in contesti legali e giornalistici. La rapidità di diffusione sui social network — dove milioni di persone vedono il contenuto prima che qualcuno lo verifichi — rende il problema urgente e di impatto reale sulle elezioni, sulla reputazione delle persone e sulla fiducia nelle istituzioni. Alcuni segnali visivi possono aiutare a riconoscere i deepfake meno sofisticati: movimenti degli occhi innaturali o lampeggiamento irregolare, sincronizzazione imperfetta tra labbra e audio, bordi del viso sfumati in modo anomalo, texture della pelle troppo uniforme. Ma la difesa più efficace resta la verifica della fonte: prima di condividere un video rilevante, confrontarlo con i canali ufficiali del soggetto coinvolto.

Le allucinazioni dei modelli linguistici

I modelli linguistici di AI generano testo statisticamente plausibile: sono bravi a produrre testo che suona corretto e autorevole, ma questo non significa che le informazioni contenute siano necessariamente vere. Il fenomeno delle allucinazioni — in cui il modello produce informazioni false presentandole con la stessa sicurezza di quelle corrette — è documentato e ben noto. Citazioni di studi che non esistono, dati numerici inventati ma precisi, date errate di eventi storici, nomi attribuiti a dichiarazioni mai fatte: per questi motivi usare l'AI per informazioni fattuali specifiche richiede sempre verifica su fonti primarie indipendenti.

Usare l'AI con consapevolezza

Nonostante i rischi, l'AI offre opportunità concrete e immediate: tradurre documenti, spiegare concetti complessi, generare bozze di testo, sintetizzare documenti lunghi. La chiave è trattare l'output dell'AI come punto di partenza, non come risposta definitiva. Per contenuti generati dall'AI destinati a essere condivisi, è buona pratica segnalare esplicitamente che si tratta di contenuto generato automaticamente e verificato dall'autore. Questa trasparenza contribuisce a mantenere un ecosistema informativo più onesto.

IDENTITÀ DIGITALE E REPUTAZIONE ONLINE

La tua presenza online: costruirla o subirla

Ogni persona che usa internet ha, volente o nolente, una presenza digitale: un insieme di informazioni, contenuti e tracce accessibili online che formano un'immagine di sé nei confronti di chiunque faccia una ricerca. Questa presenza può essere costruita consapevolmente – curando il proprio profilo LinkedIn, scegliendo cosa pubblicare, partecipando in modo costruttivo alle comunità online – oppure può essere subita: costruita da altri attraverso tag non richiesti, menzioni, contenuti condivisi senza consenso. Un datore di lavoro, un potenziale partner, un cliente: tutti cercano informazioni online prima di prendere decisioni. Quello che trovano ha un peso reale.

L'impronta digitale e le sue conseguenze

Ogni azione che compiamo online lascia una traccia: i commenti che pubblichiamo, le foto che carichiamo, i like che mettiamo, le ricerche che facciamo. L'insieme di queste tracce costituisce la nostra impronta digitale – una sorta di curriculum informale che ci precede in ogni contesto. A differenza di una conversazione dal vivo che si esaurisce nel momento, un post digitale può essere trovato mesi o anni dopo, fuori dal contesto originale, da persone che non conoscevano quando l'abbiamo scritto. La regola pratica è semplice: prima di pubblicare qualsiasi contenuto, immaginare che sia visibile a tutti – datori di lavoro, familiari, colleghi. Se il contenuto non supera questo test mentale, è meglio non pubblicarlo.

Il diritto all'oblio: come esercitarlo

Il GDPR riconosce a ogni cittadino europeo il diritto alla cancellazione dei propri dati – detto anche diritto all'oblio. Significa che si può richiedere a un'organizzazione di cancellare le informazioni personali che la riguardano, a condizione che non ci siano motivi legittimi prevalenti per conservarle. Per i contenuti presenti sui motori di ricerca, Google offre uno strumento specifico per richiedere la rimozione di risultati che contengono informazioni personali sensibili – numeri di documenti, dati bancari, indirizzi privati. Per i contenuti sui social network, ogni piattaforma offre procedure specifiche di segnalazione e richiesta di rimozione.

Costruire una reputazione digitale positiva

La reputazione digitale non si costruisce soltanto evitando contenuti negativi: si costruisce attivamente contribuendo in modo positivo agli spazi digitali. Partecipare a discussioni professionali con commenti pertinenti. Condividere contenuti utili e affidabili. Produrre materiali originali – articoli, tutorial, recensioni oneste – che dimostrano competenza e affidabilità. Queste azioni, nel tempo, costruiscono una presenza digitale che apre porte invece di chiuderle.

Azione concreta: Cerca il tuo nome su Google e osserva cosa appare. Se trovi contenuti indesiderati, valuta come intervenire: modificare le impostazioni di privacy del profilo, richiedere la rimozione, oppure costruire contenuti positivi che ne scalzino la visibilità nei risultati di ricerca.

Riepilogo dei concetti fondamentali

Questo percorso formativo ha costruito le basi per una navigazione digitale consapevole, sicura e produttiva, coprendo due grandi aree di competenza: la navigazione e la comunicazione digitale.

Nella navigazione digitale, abbiamo imparato che i browser sono le finestre attraverso cui accediamo al web, ognuno con caratteristiche specifiche in termini di velocità, privacy e compatibilità. I motori di ricerca funzionano attraverso tre fasi – crawling, indexing, ranking – e possono essere usati in modo molto più efficace con tecniche semplici come gli operatori logici e la ricerca inversa per immagini. La sicurezza di un sito si verifica controllando il protocollo HTTPS e leggendo attentamente il dominio nell'URL, prestando attenzione alle tecniche di inganno come il typosquatting e i sottodomini falsi. L'affidabilità di una notizia si valuta risalendo alle fonti primarie, verificando l'autorevolezza di chi scrive e resistendo alle trappole emotive del clickbaiting.

Nella comunicazione digitale, abbiamo imparato che l'email è lo strumento di comunicazione formale per eccellenza, e che usare correttamente i campi A, CC e CCN è una questione di privacy e professionalità. Le app di messaggistica sono potenti e comode, ma richiedono attenzione ai link ricevuti e alle catene virali. I social network e i forum sono ambienti diversi con dinamiche diverse, e la consapevolezza degli effetti cognitivi degli algoritmi – filter bubble, polarizzazione, rinforzo positivo – è la difesa più efficace contro la manipolazione involontaria. La creazione di contenuti digitali è oggi accessibile a tutti, con strumenti gratuiti e potenti, a patto di gestire correttamente i permessi di condivisione e rispettare le normative sul diritto d'autore.

La sicurezza digitale non è un prodotto che si acquista: è una competenza che si costruisce. Ogni volta che verifichi l'URL di un sito prima di inserire i tuoi dati, ogni volta che controlli la fonte di una notizia prima di condividerla, ogni volta che usi CCN per proteggere la privacy dei tuoi contatti: stai esercitando la tua cittadinanza digitale. Fallo sempre.

Test di autovalutazione

Indica la risposta corretta per ciascuna domanda. Le risposte si trovano in fondo alla sezione.

1. Quale di questi indirizzi è sicuro per accedere a Facebook? a) <https://facebook-login.com> b) <http://www.facebook.com> c) <https://m.facebook.com> d) <https://faceboook.com>
2. Cosa garantisce il lucchetto HTTPS nella barra del browser? a) Che il sito è onesto e non ti trufferà. b) Che la connessione è cifrata – i dati non possono essere intercettati durante il trasferimento. c) Che il sito non contiene pubblicità.
3. Se vuoi inviare un'email a un gruppo di persone che non si conoscono tra loro proteggendo la loro privacy, quale campo devi usare? a) Campo A. b) Campo CC. c) Campo CCN.
4. Cos'è la filter bubble? a) Un filtro che blocca i contenuti per adulti. b) Il fenomeno per cui l'algoritmo mostra progressivamente contenuti sempre più simili a quelli con cui abbiamo già interagito. c) Un software antivirus per browser.
5. Qual è la tecnica di inganno che sfrutta piccoli errori tipografici nei domini web? a) Phishing. b) Typosquatting. c) Clickbaiting.
6. Una licenza Creative Commons con la condizione NC significa che: a) L'opera non può essere usata senza citare l'autore. b) L'opera non può essere usata a scopo commerciale. c) L'opera non può essere modificata.
7. Cosa permette di fare la ricerca inversa per immagini? a) Trovare immagini simili esteticamente a una data fotografia. b) Trovare la fonte originale di un'immagine e tutti i contesti in cui è stata usata. c) Riconoscere automaticamente le fake news.

Risposte: 1-c / 2-b / 3-c / 4-b / 5-b / 6-b / 7-b

Glossario essenziale

Browser: programma utilizzato per navigare su internet (es. Chrome, Firefox, Safari, Edge). Permette di visualizzare pagine web e accedere a servizi online.

CCN (Copia Conoscenza Nascosta): campo email che permette di inviare un messaggio a più destinatari mantenendo nascosti i loro indirizzi reciprocamente. Strumento fondamentale per la privacy nelle comunicazioni di gruppo.

Clickbaiting: tecnica di manipolazione che usa titoli sensazionalistici o emotivamente coinvolgenti per indurre gli utenti a cliccare su un contenuto, spesso di scarsa qualità o fuorviante.

Co-editing: modifica simultanea dello stesso documento da parte di più utenti in tempo reale, resa possibile da strumenti cloud come Google Workspace.

Creative Commons: sistema di licenze che permette agli autori di concedere alcuni diritti d'uso delle proprie opere mantenendone altri, alternativo al copyright tradizionale.

Copyright (©): protezione legale automatica che garantisce all'autore di un'opera esclusività d'uso e distribuzione. 'Tutti i diritti riservati'.

Dominio pubblico: insieme delle opere non più soggette a restrizioni di copyright, liberamente utilizzabili da chiunque.

Filter bubble: fenomeno per cui gli algoritmi delle piattaforme mostrano contenuti sempre più coerenti con le preferenze espresse dall'utente, creando una bolla informativa che esclude punti di vista diversi.

HTTPS: protocollo di sicurezza che cifra i dati scambiati tra browser e sito web. La 'S' sta per Secure. Condizione necessaria (ma non sufficiente) per inserire dati sensibili su un sito.

Motore di ricerca: sistema che esplora, cataloga e rende ricercabile il contenuto del web. I principali sono Google, Bing e DuckDuckGo.

Navigazione in incognito: modalità del browser che non salva cronologia, cookie e dati di navigazione sul dispositivo. Non garantisce l'anonimato online.

Phishing: tecnica truffaldina che finge di provenire da fonti affidabili per ottenere dati personali, password o informazioni finanziarie.

Ricerca inversa per immagini: tecnica che permette di trovare la fonte originale di un'immagine e tutti i contesti in cui è stata usata, utile per verificare l'autenticità delle foto nelle notizie.

Rinforzo positivo (online): meccanismo psicologico per cui i like e le interazioni social generano un rilascio di dopamina, potenzialmente creando dipendenza dalle piattaforme.

SSL/TLS: protocollo crittografico che garantisce la sicurezza della connessione HTTPS, cifrando i dati durante il loro trasferimento.

Typosquatting: tecnica di inganno che sfrutta piccoli errori tipografici nei nomi di dominio (es. 'faceboook.com') per indirizzare gli utenti verso siti fraudolenti.

UGC (User Generated Content): contenuti creati dagli utenti delle piattaforme digitali: post, video, recensioni, blog, podcast. Costituiscono il valore principale delle piattaforme social.

URL (Uniform Resource Locator): indirizzo univoco di una risorsa su internet, visibile nella barra degli indirizzi del browser. Leggere correttamente un URL è fondamentale per riconoscere i siti fraudolenti.

Web crawling: processo automatico con cui i motori di ricerca esplorano il web seguendo i link da una pagina all'altra, raccogliendo contenuti da indicizzare.

Risorse utili

Agid – Agenzia per l'Italia Digitale: agid.gov.it – informazioni ufficiali sulla trasformazione digitale della PA italiana, SPID e servizi digitali.

Garante per la Protezione dei Dati Personali: gdpd.it – per informazioni sui propri diritti digitali e sulla privacy online.

Polizia Postale: commissariatodips.it – segnalazioni di reati informatici, truffe online e phishing.

DuckDuckGo: duckduckgo.com – motore di ricerca privacy-first, non traccia i dati degli utenti.

Unsplash / Pixabay / Pexels: immagini gratuite e libere da copyright per uso personale e professionale.

Google Digital Garage: grow.google/intl/it_it/courses – corsi gratuiti di Google su competenze digitali, marketing online e sicurezza informatica.

TEMA B
SICUREZZA E USO CONSAPEVOLE
DEI SERVIZI DIGITALI

 **NETI-QUIET COME COMUNICARE ONLINE**
CON RISPETTO E SICUREZZA



Digita Facile
Campania

A chi è rivolto questo capitolo

Questo capitolo accompagna il percorso formativo NETI-QUIET: Come comunicare online con rispetto e sicurezza, sviluppato nell'ambito del progetto Digita Facile Campania, Tema B – Sicurezza e Uso Consapevole dei Servizi Digitali. Si rivolge a chiunque usi internet nella vita quotidiana e voglia migliorare il modo in cui comunica negli spazi digitali: dalle chat familiari alle e-mail di lavoro, dai gruppi WhatsApp ai documenti condivisi, dai social network alle piattaforme di collaborazione.

Il capitolo si articola in una sezione introduttiva e quattro moduli tematici. L'introduzione "Welcome to the Digital Village" apre il percorso esplorando perché la comunicazione online è così diversa da quella dal vivo e perché servono regole condivise. Il Modulo 1 "Digital Fair Play" introduce le fondamenta della convivenza digitale con le regole d'oro della netiquette. Il Modulo 2 "Impronte Digitali" sviluppa la consapevolezza sull'identità digitale e sui rischi reputazionali. Il Modulo 3 "Write Don't Fight" insegna a scrivere e rispondere in modo efficace e rispettoso, prevenendo conflitti. Il Modulo 4 "Digital Teampay" affronta la collaborazione in ambienti digitali condivisi. Il percorso è accompagnato da una protagonista narrativa – Lina Link, la guardiana delle buone connessioni nel Digital Village – che rende i contenuti più accessibili e coinvolgenti, specialmente per i partecipanti con minore familiarità con i temi digitali. Non è richiesta alcuna competenza tecnica pregressa: è sufficiente utilizzare anche saltuariamente canali digitali nella vita di tutti i giorni.

Questo capitolo non è solo un testo da leggere: è un manuale da tenere vicino. Torna a consultarlo quando un messaggio ti mette in difficoltà, quando un gruppo si scalda, quando stai per pubblicare qualcosa e non sei sicuro. Il Kit Netiquette in fondo raccoglie gli strumenti pratici più utili per la vita reale.

Online ci capiamo davvero?

Quante volte, nelle ultime settimane, hai frainteso un messaggio o sei stato frainteso? Quante volte hai pensato che il tono di un WhatsApp fosse scortese, per poi scoprire che non era così? Quante volte hai riletto una e-mail e ti sei chiesto: ma perché l'ha scritta così?

Se hai risposto “spesso” almeno a una di queste domande, sei nel posto giusto. Non perché tu abbia sbagliato qualcosa: ma perché la comunicazione digitale è genuinamente più difficile di quanto sembri. Non perché le persone vogliono litigare o ferirsi (nella maggior parte dei casi non è così) ma perché online manca tutto ciò che nella vita di tutti i giorni ci aiuta a capirci: la faccia, la voce, il tono, il contesto, lo sguardo. Quando parliamo di persona, il 70 per cento della comunicazione passa attraverso elementi non verbali: l'espressione del viso, la postura, il volume della voce, il ritmo delle parole.

Online, questi elementi scompaiono. Restano solo le parole, spesso scritte di fretta, spesso lette nel momento sbagliato e gli emoji, che cercano di compensare ma non sempre ci riescono.

Le parole corrono più veloci delle intenzioni

Il digitale ha introdotto una nuova fragilità nella comunicazione umana: la velocità. Un messaggio che online si scrive in trenta secondi viene letto in due, senza tono, senza contesto, senza la possibilità di aggiustare l'impressione in tempo reale. E chi legge, magari stanco, magari nervoso, magari con aspettative diverse dalle nostre, interpreta. E quando interpretiamo, spesso sbagliamo.

Tre messaggi apparentemente innocenti illustrano perfettamente questo problema. “Ok.” sembra secco, quasi infastidito. “Ah ok...” sembra deluso, quasi ferito. “Come preferisci.” sembra indifferente, quasi passivo-aggressivo. Nessuno di questi messaggi contiene parole offensive.

Eppure, tutti e tre possono creare tensione, incomprensione, conflitti e non perché chi scrive voglia farlo, ma perché chi legge deve interpretare, e lo fa attraverso il filtro del proprio stato emotivo del momento. È qui che entra in gioco la netiquette. Non come una lista di divieti, non come un corso di galateo digitale, non come un modo per censurare la propria espressione. Ma come uno strumento per comunicare in modo più efficace, per essere capiti meglio, per evitare fraintendimenti inutili, per proteggere le proprie relazioni (e la propria reputazione) negli spazi digitali.

Cos'è la netiquette

Il termine netiquette nasce dalla fusione di network/rete e netiquette/galateo. È l'insieme delle regole, spesso non scritte ma largamente condivise, che regolano la comunicazione civile negli spazi digitali. Non è un codice di legge: è una serie di convenzioni che, quando vengono rispettate, rendono la vita online più piacevole, più produttiva e più sicura per tutti.

La netiquette serve a non ferire gli altri involontariamente, a non creare drammi inutili, a non rovinarsi la reputazione con un messaggio scritto di getto, a comunicare meglio anche quando si è di fretta, arrabbiati o stressati. Non serve per stare in silenzio, serve per farsi capire. Non è essere deboli: è essere strategici.

“Nel Digital Village non vince chi urla di più. Vince chi sa comunicare meglio. La netiquette non serve a limitarti: serve a farti stare meglio online.” – Lina Link

Obiettivi del modulo

Al termine di questo modulo conoscerai le fondamenta della convivenza digitale. Saprai applicare le regole d'oro della netiquette nei diversi contesti in cui comunichi online, ossia chat, email, social, gruppi. Saprai riconoscere i comportamenti scorretti più comuni come spam, flame, trolling e avrai strumenti concreti per gestirli senza alimentare conflitti.

Il fair play nella comunicazione digitale

Nello sport, il fair play non è solo rispettare le regole scritte: è un atteggiamento. È sapere che dall'altra parte c'è un avversario o un compagno che ha gli stessi diritti tuoi, gli stessi obiettivi tuoi, gli stessi limiti tuoi. È capire che le regole non servono a limitarti, ma a rendere possibile il gioco. Senza regole, il gioco si ferma.

Online funziona esattamente allo stesso modo. La maggior parte dei problemi nelle comunicazioni digitali non nasce perché qualcuno vuole fare del male: nasce perché scriviamo di fretta, rispondiamo di pancia, diamo per scontato che l'altro capisca cosa intendiamo. La netiquette è il fair play della comunicazione digitale: serve a far continuare il gioco, la conversazione, la collaborazione, la relazione.

Le 10 regole d'oro della netiquette

Queste regole non sono un decalogo da memorizzare. Sono strumenti pratici da usare ogni volta che ti trovi davanti a uno schermo con qualcosa da comunicare.

1. Ricorda che dall'altra parte c'è una persona. Dietro ogni messaggio, ogni commento, ogni email c'è qualcuno che legge: magari stanco, magari nervoso, magari insicuro. Il modo in cui scrivi ha un impatto reale su quella persona. Scrivere come se ti stessero leggendo in faccia è il primo filtro naturale contro le comunicazioni offensive o maldestre.

2. Pensa prima di inviare. Dieci secondi prima di premere Invia valgono più di dieci messaggi di scuse dopo. Questa non è un'iperbole: è una realtà verificata ogni giorno in ogni chat e in ogni gruppo. Il tasto Invia è più potente di quanto sembri: una volta premuto, le parole non tornano indietro.

3. Non rispondere a caldo. Quando un messaggio ti fa arrabbiare o ti ferisce, la risposta immediata è quasi sempre la peggiore. Aspetta cinque minuti, un'ora, anche un giorno se necessario. La maggior parte delle escalation digitali nasce da risposte impulsive a interpretazioni — spesso sbagliate — di messaggi ambigui.

4. Sii chiaro, non criptico. L'ironia, il sarcasmo, i sottintesi che funzionano perfettamente dal vivo sono tra le principali cause di malintesi online. Se non sei sicuro che il tono venga percepito correttamente, scrivi in modo esplicito. Meglio essere leggermente ridondante che lasciare spazio a interpretazioni sbagliate.

5. Evita ironia quando non sei sicuro. L'ironia online è un rischio calcolato. Funziona solo quando chi legge conosce bene il tuo stile comunicativo. Con persone che non conosci molto, o in contesti professionali, è meglio evitarla o accompagnarla con un segnale esplicito.

6. In gruppo, pensa due volte. I gruppi amplificano tutto: le incomprensioni diventano conflitti, i toni diventano schieramenti, le opinioni diventano faziosità. Prima di scrivere in un gruppo, chiediti: questo messaggio serve al gruppo, o serve solo a me in questo momento?

7. Critica le idee, non le persone. La differenza tra un feedback costruttivo e un attacco personale è spesso solo grammaticale. “Questa parte del progetto potrebbe essere più chiara” è completamente diverso da “non si capisce niente di quello che hai scritto”. Il contenuto del messaggio è identico; l'effetto su chi lo riceve è opposto.

8. Usa i commenti per collaborare. Nei documenti condivisi, nelle discussioni online, nelle revisioni di lavoro: i commenti sono strumenti di collaborazione, non di giudizio. Un commento che propone, spiega e chiede confronto fa avanzare il lavoro. Un commento che giudica e non spiega crea tensione.

9. Proteggi la tua reputazione digitale. Ogni messaggio che scrivi, ogni commento che lasci, ogni foto che condividi è parte della tua impronta digitale. Contribuisce, nel bene o nel male, all'immagine che gli altri si formano di te online. Trattala come un bene prezioso.

10. Se hai un dubbio, fermati. Quando stai per inviare qualcosa e hai anche solo un piccolo dubbio (se vale la pena, se verrà capito, se è il momento giusto) quel dubbio è informazione. Ascoltalo. Se “sembra così così”, probabilmente lo è.

Comportamenti scorretti: riconoscerli per non perpetuarli

Conoscere i comportamenti scorretti più diffusi online non serve per giudicare chi li pratica, ma per riconoscerli quando li si subisce e per non metterli in atto inconsapevolmente.

Lo spam è l'invio di messaggi non richiesti e non pertinenti: catene di Sant'Antonio, pubblicità non richiesta, messaggi ripetitivi nei gruppi. È una delle forme di mancanza di rispetto più diffuse e meno percepite come tali, perché chi la pratica spesso non è consapevole del disturbo che crea agli altri.

Il Flame (letteralmente fiamma) è una risposta aggressiva, emotivamente intensa e sproporzionata rispetto al contenuto del messaggio originale. Nasce quasi sempre da una risposta a caldo a qualcosa che ha infastidito, e innesca quasi inevitabilmente una escalation: risposta aggressiva produce risposta aggressiva, il tono si alza, la conversazione perde ogni utilità.

Il Trolling è la pratica di provocare deliberatamente altri utenti con commenti fuori luogo, offensivi o contraddittori, con l'unico scopo di generare reazioni emotive negative. La risposta più efficace al trolling è il non rispondere: privare il troll della reazione che cerca è l'unico modo per disinnescarlo. Come dice la saggezza digitale: "Non dare da mangiare ai troll."

Regola pratica: Prima di rispondere a un messaggio che ti ha dato fastidio, rileggilo fingendo che sia stato scritto con buone intenzioni. Molto spesso la lettura cambia. Se rimane problematico anche dopo questa riscrittura mentale, allora sì, merita una risposta. Ma una risposta consapevole, non impulsiva.

IMPRONTE DIGITALI: TRACCE, RISCHI E POTERE DELL'IMMAGINE ONLINE

Obiettivi del modulo

Al termine di questo modulo avrai sviluppato una consapevolezza più profonda sulla tua identità digitale e sull'impronta che lasci ogni giorno negli spazi online. Saprai distinguere tra tracce volontarie e involontarie, riconoscere gli errori più comuni come oversharing, commenti impulsivi e capire come costruire e proteggere la tua reputazione digitale.

Identità digitale: cos'è e da cosa è composta

L'identità digitale è l'insieme delle informazioni, dei contenuti e delle tracce che definiscono chi sei negli spazi online. Non è soltanto ciò che scrivi di proposito su un profilo social: è tutto ciò che ti riguarda e che è accessibile in rete, indipendentemente dal fatto che tu ne sia consapevole.

Si compone di elementi diversi. I profili ufficiali, account sui social network, profilo LinkedIn, profilo su piattaforme professionali, sono la parte più consapevole e controllabile della tua identità digitale. I contenuti pubblicati (post, commenti, foto, video, recensioni) costituiscono una storia digitale che si accumula nel tempo. Le menzioni altrui (quando qualcuno ti tagga in una foto, scrive il tuo nome in un commento, ti cita in un articolo) aggiungono elementi alla tua identità digitale su cui hai meno controllo diretto. I dati comportamentali (i siti che visiti, i prodotti che cerchi, i contenuti con cui interagisci) formano un profilo invisibile che le piattaforme usano per personalizzare la tua esperienza e, molto spesso, per venderti come prodotto agli inserzionisti.

L'impronta digitale: volontaria e involontaria

L'impronta digitale o digital footprint è l'insieme delle tracce che lasci online. Si divide in due categorie che è importante distinguere.

L'impronta volontaria è tutto ciò che pubblichi deliberatamente: i post sui social, le foto che carichi, le recensioni che scrivi, i commenti che lasci, i like che metti. È la parte dell'impronta su cui hai pieno controllo, o almeno, sulla quale hai la possibilità di esercitare controllo, se ci pensi prima di agire.

L'impronta involontaria è costituita dalle tracce che lasci senza rendertene conto: i cookie dei siti visitati, i dati di geolocalizzazione registrati dai tuoi dispositivi, le ricerche effettuate sui motori di ricerca, le app che hai autorizzato ad accedere alla tua rubrica o alla tua posizione. Questa parte dell'impronta è meno visibile ma non meno reale, e alimenta l'enorme industria della raccolta e commercializzazione dei dati personali.

La caratteristica più importante dell'impronta digitale, che spesso viene sottovalutata, è la sua permanenza. Il web ha una memoria lunghissima: un contenuto pubblicato online è estremamente difficile da eliminare completamente. Può essere salvato, ricondiviso, archiviato da sistemi automatici, riemerso attraverso i risultati dei motori di ricerca anni dopo la pubblicazione originale. Questo vale per i post pubblici, ma anche, in molti casi, per i messaggi privati, se qualcuno decide di fare uno screenshot.

Gli errori più comuni: oversharing e commenti impulsivi

L'oversharing, ossia la condivisione eccessiva di informazioni personali, è uno degli errori più diffusi e meno percepiti come tali. Condividere la propria posizione in tempo reale, pubblicare foto dei documenti di identità, raccontare dettagli della propria vita privata o familiare a un pubblico molto ampio, condividere informazioni sullo stato di salute o su situazioni finanziarie delicate: sono tutte pratiche che possono avere conseguenze non previste.

L'oversharing non è sempre intenzionale. Spesso nasce dal desiderio comprensibile di condividere momenti belli o difficili con la propria rete sociale. Il problema sorge quando non si considera chi fa parte di quella rete, che può includere conoscenti, colleghi, superiori o persone che non si sono mai incontrate di persona e quando non si riflette su come quelle informazioni potrebbero essere usate da chi le legge.

I commenti impulsivi sono l'altra grande fonte di danni reputazionali online. Un commento scritto in un momento di rabbia, di frustrazione o di eccessiva sicurezza può sembrare irrilevante nel momento in cui viene scritto, ma può avere conseguenze durature. Casi documentati mostrano persone che hanno perso opportunità di lavoro, rapporti professionali o relazioni personali a causa di commenti pubblicati online, anche anni prima, e ritrovati attraverso una semplice ricerca del nome.

Reputazione online: come si costruisce e come si protegge

La reputazione digitale non si costruisce soltanto evitando i contenuti negativi: si costruisce attivamente, nel tempo, attraverso la qualità e la coerenza di ciò che si pubblica e di come ci si comporta negli spazi digitali. Come nella vita reale, la reputazione online è la somma delle impressioni che gli altri si formano di te attraverso ogni interazione.

Costruirla consapevolmente significa chiedersi, prima di ogni pubblicazione: questo contenuto riflette chi voglio essere online? È coerente con i valori e l'immagine che voglio trasmettere? Può essere letto da qualcuno che non conosco senza creare impressioni che non voglio dare?

Proteggerla significa anche essere attivi nella gestione delle informazioni che altri pubblicano su di te. Se qualcuno pubblica una foto che ti riguarda senza chiedere il tuo consenso, hai il diritto di chiederne la rimozione. Se trovi contenuti su di te che ritieni lesivi della tua immagine, il GDPR ti garantisce il diritto di richiederne la cancellazione, il cosiddetto diritto all'oblio. E se noti che la tua impronta digitale contiene elementi che non vorresti ci fossero, è possibile lavorare per ridurne la visibilità, anche se non sempre è possibile eliminarli completamente.

Esercizio pratico: Cerca il tuo nome e cognome su Google. Cosa compare? I risultati rispecchiano l'immagine che vuoi dare di te? Se trovi qualcosa che non ti piace, questo è il momento per capire come gestirla, non quando quella informazione viene trovata da un datore di lavoro o da qualcuno con cui vuoi costruire una relazione.

WRITE DON'T FIGHT: COMUNICARE SENZA CREARE CONFLITTI

Obiettivi del modulo

Al termine di questo modulo saprai scrivere email efficaci e rispettose, gestire chat e gruppi in modo da prevenire e risolvere le tensioni, riconoscere le cinque trappole comunicative più diffuse online e applicare le basi della comunicazione assertiva negli scambi digitali.

L'email: lo strumento più frainteso del web

L'email è lo strumento di comunicazione digitale più formale e più antico, eppure è anche quello in cui si commettono più errori di comunicazione. Forse proprio perché la sua struttura sembra semplice (c'è un mittente, c'è un destinatario, c'è un messaggio) si tende a sottovalutare quanto sia facile farla male.

Un'email efficace ha alcune caratteristiche fondamentali. Inizia con un oggetto chiaro e specifico: una delle cause più frequenti di fraintendimenti nelle comunicazioni professionali è ricevere un'email con oggetto "Ciao" o "Informazioni" o, peggio, con nessun oggetto. Il destinatario non sa cosa aspettarsi, non sa se è urgente, non sa se deve agire o solo leggere. Un oggetto come "Richiesta di appuntamento per la prossima settimana" o "Domanda sul progetto X - risposta entro venerdì" elimina ambiguità in partenza.

Il corpo dell'email dovrebbe essere chiaro, conciso e organizzato. Paragrafi brevi, una sola richiesta per email quando possibile e, fondamentale, una chiusura che indichi chiaramente cosa ci si aspetta dall'altro: risposta? azione? semplice lettura? Senza questa indicazione, il destinatario deve indovinare, e spesso indovina male.

Alcune regole di etichetta email sono così radicate da essere universalmente riconosciute, ma vale la pena ribadirle. Non scrivere in MAIUSCOLO: su internet equivale a urlare, ed è percepito come aggressivo anche quando l'intenzione non è tale. Rispettare i tempi dell'altro: un'email non è un messaggio istantaneo, e aspettarsi una risposta nell'arco di pochi minuti è una forma di pressione non richiesta. Inserire saluti e firma: anche in contesti informali, un minimo di struttura formale è segno di rispetto.

Chat e gruppi: le regole del flusso

Le app di messaggistica come WhatsApp, Telegram, Messenger hanno caratteristiche comunicative molto diverse dall'email, e richiedono regole diverse. Sono più veloci, più informali, più immediate. E proprio per questo sono l'ambiente in cui le tensioni nascono più facilmente.

I gruppi WhatsApp sono forse l'ambiente digitale in cui si concentrano più

problemi comunicativi nella vita quotidiana delle persone. Messaggi inviati nelle ore sbagliate, discussioni che si animano su argomenti divisivi, notifiche continue che disturbano il sonno o il lavoro, conversazioni che esplodono per fraintendimenti che dal vivo si sarebbero risolti in trenta secondi: il gruppo WhatsApp di famiglia, di lavoro o di quartiere è diventato un campo minato comunicativo per moltissime persone. Alcune regole semplici aiutano a navigarlo meglio.

Rispettare gli orari: inviare messaggi non urgenti nelle ore notturne o nelle prime ore del mattino è mancanza di rispetto, anche se chi riceve ha la modalità silenziosa attivata. Non inondare il gruppo con contenuti non pertinenti come video, meme, catene, specialmente se il gruppo ha uno scopo specifico. Evitare di fare discussioni private in gruppo: se il problema riguarda una persona sola, affrontarlo in privato. Non rispondere alle provocazioni nel gruppo: se qualcuno è aggressivo o scorretto, affrontarlo in privato, oppure non rispondere affatto.

Le cinque trappole comunicative

Esistono cinque pattern di comunicazione online che, più di altri, portano ai conflitti. Riconoscerli in sé stessi e negli altri è il primo passo per evitarli.

1. La risposta reattiva. Rispondere immediatamente a un messaggio che ha generato una reazione emotiva intensa, senza aspettare che l'emozione si calmi. Il risultato è quasi sempre un messaggio che si pente subito dopo, ma che non si può più riprendere.

2. L'interpretazione negativa di default. Interpretare automaticamente come ostile o aggressivo qualsiasi messaggio ambiguo, invece di chiedere chiarimenti. Se un messaggio potrebbe essere letto in due modi (uno neutro e uno offensivo) è quasi sempre meglio assumere il neutro e, se necessario, chiedere.

3. Il “Come mai non rispondi?” digitale. Leggere troppo nel silenzio dell'altro. La doppia spunta blu che rimane senza risposta per ore può avere mille spiegazioni: il telefono era in tasca, la persona era impegnata, stava aspettando di avere una risposta migliore. Spesso, però, viene interpretata come un segnale di disagio o di rifiuto.

4. L'ironia senza segnali. Usare ironia o sarcasmo in contesti dove non è chiaro che sia ironia, e con persone che non conoscono abbastanza bene il proprio stile comunicativo. Senza il tono della voce e l'espressione del viso, l'ironia è spesso indistinguibile da un'affermazione letterale.

5. Il messaggio di gruppo al posto del messaggio privato. Affrontare in un gruppo un problema che riguarda una persona sola, mettendola in difficoltà di fronte a tutti. Anche quando non è l'intenzione, questo comportamento viene quasi sempre percepito come un attacco pubblico.

Comunicazione assertiva: la terza via

Tra l'aggressività (dire tutto quello che si pensa senza filtri, a qualsiasi costo) e la passività (non dire nulla per evitare conflitti) esiste una terza via: la comunicazione assertiva. È la capacità di esprimere le proprie opinioni, esigenze ed emozioni in modo chiaro e diretto, rispettando allo stesso tempo quelle dell'altro. Online, la comunicazione assertiva si traduce in alcune scelte linguistiche specifiche. Usare la prima persona invece dell'accusa: "Mi sono sentito escluso dalla decisione" invece di "Tu mi hai sempre escluso". Descrivere il comportamento invece di giudicare la persona: "Questo commento mi ha fatto stare male" invece di "Sei sempre così scortese".

Fare richieste specifiche invece di lamenti generici: "Ti chiedo di avvisarmi prima di modificare il documento" invece di "Non rispetti mai il lavoro degli altri".

La comunicazione assertiva non garantisce che ogni conflitto si risolva, ma aumenta significativamente la probabilità che l'altro la recepisca come un tentativo di dialogo piuttosto che come un attacco, e questo cambia quasi tutto.

"Nel Digital Village, Lina Link sa che la netiquette non è essere deboli. È essere strategici. Dire le cose in modo che l'altro possa ascoltarle è intelligenza comunicativa, non rinuncia."

Obiettivi del modulo

Al termine di questo modulo saprai collaborare efficacemente in ambienti digitali condivisi: documenti in cloud, piattaforme di project management, gruppi di lavoro digitali. Saprai usare i commenti in modo costruttivo, gestire le versioni dei documenti senza creare confusione, dare feedback utili e riceverli senza conflitti, e assegnare responsabilità in modo chiaro ed equo.

Il documento condiviso come spazio comune

Un documento condiviso è una stanza comune. Se entri in una stanza comune e sposti i mobili senza dire nulla, qualcuno si arrabbia e non perché la modifica sia necessariamente sbagliata, ma perché non si sa perché è stata fatta, e questo crea disagio. Online accade lo stesso: non è la modifica che dà fastidio, è non capire perché è stata fatta.

Lavorare bene in un documento condiviso significa rispettare alcune regole semplici ma spesso ignorate. Non cancellare di pancia: prima di eliminare una parte del lavoro altrui, commenta e spiega il motivo. Se cambi qualcosa, spiega: un commento vale più di dieci scuse dopo. Rispetta le versioni: se non sei sicuro di cosa fa una parte del documento, chiedi prima di toccarla. In pratica: non riscrivere sopra, ma proponi e spiega.

I commenti: strumenti di collaborazione, non di giudizio

I commenti nei documenti condivisi sono uno degli strumenti più potenti della collaborazione digitale e uno di quelli usati peggio. Un commento che funziona ha tre caratteristiche: indica cosa c'è da migliorare in modo specifico, propone una strada o chiede confronto, e si rivolge al lavoro, non alla persona che lo ha fatto.

La differenza tra un commento costruttivo e uno distruttivo è spesso solo grammaticale. “Qui potremmo rendere questo punto più chiaro: propongo di...” è collaborazione. “Non si capisce niente” è un attacco. “Questa sezione è la più debole: scegliamo insieme cosa tenere e cosa riscrivere” è costruttivo. “Rifai tutto” è demotivante e inutile. Il contenuto del messaggio, ossia che c'è qualcosa da migliorare, è identico in entrambe le coppie: l'effetto su chi lo riceve è, però, opposto. Una regola utile per i commenti: il feedback utile indica cosa migliorare, propone una strada, e non colpisce la persona. Se il commento non soddisfa questi tre criteri, probabilmente non è pronto per essere inviato.

Gli errori più comuni che fanno litigare i team digitali

Lavorare insieme online senza regole condivise produce quasi inevitabilmente

gli stessi problemi, in quasi tutti i gruppi. Conoscerli in anticipo è il modo più efficace per prevenirli.

Modificare senza avvisare è l'errore più frequente: qualcuno cambia una parte importante del documento senza spiegare perché, e chi aveva lavorato su quella parte si trova davanti a qualcosa di diverso senza capire cosa è successo. La soluzione è semplice: un commento, anche brevissimo, che spieghi la modifica cambia completamente la percezione.

Cancellare parti altrui senza spiegare è una variante dello stesso errore, ma con un impatto emotivo maggiore: chi vede il proprio lavoro scomparire senza una parola lo vive quasi sempre come un gesto irrispettoso, anche quando non è questa l'intenzione. Usare la funzione di revisione, che tiene traccia delle modifiche invece di applicarle direttamente, è la soluzione tecnica a questo problema.

Non assegnare compiti chiari è il problema strutturale più comune nei team digitali. Quando non è chiaro chi fa cosa, nasce la frase peggiore della collaborazione di gruppo: "Pensavo lo facesse qualcun altro." Un responsabile per ogni pezzo di lavoro, con una scadenza chiara e un luogo dove aggiornare lo stato (una chat, un commento nel documento, uno strumento di project management) trasforma un gruppo di persone in un team.

Usare feedback aggressivi come "fa schifo", "rifai", "non si capisce niente" non è soltanto scortese: è controproducente. Un feedback che colpisce la persona invece del lavoro attiva quasi inevitabilmente una risposta difensiva, che blocca la possibilità di migliorare davvero il risultato. Il tempo speso a formulare un feedback costruttivo non è cortesia: è efficienza.

Il patto di collaborazione

I team digitali che funzionano bene non lo fanno per caso: hanno regole condivise su come lavorare insieme. Non necessariamente regole formali scritte in un documento ufficiale, spesso sono accordi impliciti, stabiliti nelle prime interazioni del gruppo. Ma sono regole, e tutti sanno quali sono.

Prima di iniziare un lavoro di gruppo digitale, vale la pena dedicare dieci minuti a rispondere a queste domande insieme: chi fa cosa? Dove lavoriamo, quale piattaforma, quale documento? Come ci aggiorniamo, tramite chat, commenti, riunioni? Come gestiamo i conflitti, chi decide se c'è un disaccordo? Come facciamo i feedback? Questi dieci minuti preventivi possono fare risparmiare ore di conflitti e confusione in seguito.

Dal corso alla vita reale: La prossima volta che inizi un lavoro di gruppo online (che sia un progetto professionale, l'organizzazione di un evento o la gestione di un documento condiviso) proponi al gruppo di stabilire queste regole prima di iniziare. Noterai la differenza.

Conclusione: Il Patto delle Buone Connessioni

Siamo arrivati alla fine del viaggio nel Digital Village. Non alla fine dei social. Non alla fine delle chat. Ma alla fine di un percorso dentro il modo in cui comunichiamo online, con più consapevolezza, con più strumenti, con più capacità di scegliere invece di semplicemente reagire.

Abbiamo capito che le parole online pesano, e spesso più di quanto immaginiamo. Che i messaggi possono essere fraintesi anche con le migliori intenzioni. Che le tracce digitali restano e contribuiscono all'immagine che gli altri si formano di noi. Che collaborare senza regole condivise crea caos, frustrazione e conflitti che si potevano evitare.

E soprattutto abbiamo capito una cosa fondamentale: la netiquette non serve a limitarci. Serve a farci stare meglio online. Non è un insieme di divieti imposti dall'esterno: è una forma di intelligenza comunicativa che, quando diventa un'abitudine, rende la vita digitale più piacevole, più produttiva, più rispettosa, per noi e per gli altri.

Da domani continuerai a scrivere messaggi, a stare nei gruppi, a commentare, a lavorare online. La differenza è che ora sai riconoscere quando una conversazione sta prendendo una brutta piega, e sai dove intervenire. Sai quando una parola può ferire. Sai quando basta poco per cambiare il tono di una chat. E quando non sai se inviare o no un messaggio, ricorda: online non puoi controllare tutto, non puoi controllare le reazioni degli altri. Ma puoi sempre scegliere come comunicare.

“Da adesso, il Digital Village continua con te.” – Lina Link

Riepilogo dei concetti fondamentali

La comunicazione online è più difficile di quanto sembri perché mancano gli elementi non verbali che nella vita dal vivo ci aiutano a capirci: la faccia, la voce, il tono, il contesto. Le parole corrono più veloci delle intenzioni, e chi legge interpreta attraverso il filtro del proprio stato emotivo. La netiquette è la risposta a questa fragilità: non un insieme di divieti, ma uno strumento per comunicare meglio.

Il fair play digitale parte dal riconoscere che dall'altra parte di ogni messaggio c'è una persona. Le dieci regole d'oro da "pensa prima di inviare" a "se hai un dubbio fermati" non sono regole teoriche: sono strumenti pratici che cambiano la qualità della comunicazione quotidiana. I comportamenti scorretti quali spam, flame, trolling si riconoscono e si gestiscono senza alimentarli.

L'impronta digitale è reale e duratura: ogni post, commento, like contribuisce all'identità digitale che gli altri trovano quando cercano il tuo nome. L'oversharing e i commenti impulsivi sono le principali cause di danni reputazionali online. La reputazione digitale si costruisce attivamente, nel tempo, attraverso la coerenza tra ciò che si pubblica e i valori che si vuole trasmettere.

Nella comunicazione scritta via email, chat o messaggi le cinque trappole più frequenti sono la risposta reattiva, l'interpretazione negativa di default, il silenzio come segnale, l'ironia senza segnali, e il messaggio di gruppo invece di quello privato. La comunicazione assertiva (usare la prima persona, descrivere il comportamento invece di giudicare la persona, fare richieste specifiche) è la terza via tra aggressività e passività.

La collaborazione digitale funziona quando ci sono regole condivise: chi fa cosa, come si usano i commenti, come si gestiscono le modifiche, come si dà feedback. Un commento utile indica cosa migliorare, propone una strada e non colpisce la persona. Assegnare responsabilità chiare evita la frase peggiore del lavoro di gruppo: "Pensavo lo facesse qualcun altro."

Kit Netiquette: strumenti per la vita reale

Questo kit raccoglie gli strumenti più pratici del percorso formativo. Non è un decalogo da memorizzare: è qualcosa da tenere a portata di mano e consultare nei momenti in cui la comunicazione online si fa difficile.

Le 10 regole d'oro della netiquette

1. Ricorda che dall'altra parte c'è una persona.
2. Scrivi come se ti stessero leggendo in faccia.
3. Non rispondere a caldo.
4. Sii chiaro, non criptico.
5. Evita ironia quando non sei sicuro.
6. In gruppo, pensa due volte.
7. Critica le idee, non le persone.
8. Usa i commenti per collaborare.
9. Proteggi la tua reputazione digitale.
10. Se hai un dubbio...fermati.

Checklist “Prima di inviare”

Prima di premere Invia su qualsiasi messaggio – email, WhatsApp, commento, post – chiediti:

- ☐ Lo direi dal vivo?
- ☐ È chiaro?
- ☐ Può essere frainteso?
- ☐ Sto reagendo o rispondendo?
- ☐ Migliora o peggiora la situazione?

Se hai dubbi su almeno una di queste domande: aspetta. Rileggi tra qualche minuto o qualche ora. La risposta giusta arriva quasi sempre dopo, non durante.

Mini-guida alla collaborazione digitale

1. Decidete chi fa cosa prima di iniziare.
2. Usate commenti e revisioni invece di modificare direttamente.
3. Spiegate sempre le modifiche che fate al lavoro degli altri.
4. Date feedback utili: indica cosa migliorare + proponi una strada + non colpisci la persona.
5. Rispettate il lavoro degli altri: non cancellate senza spiegare.

Collaborare bene non è più difficile. È solo più intelligente.

Identità e reputazione online: cosa tenere a mente

Ogni post, commento e messaggio lascia una traccia. Non per spaventarti, ma per renderti consapevole. La reputazione digitale si costruisce un messaggio alla volta.

Condividi: idee, progetti, rispetto, contributi utili alla comunità.

Evita: dati personali sensibili, screenshot di chat private, post scritti nella rabbia, informazioni su altri senza il loro consenso.

Guida tascabile alla Netiquette

COS'È? Il modo di stare bene online. 5 REGOLE BASE: non scrivere a caldo – sii chiaro – rispetta gli altri – pensa prima di condividere – ricorda che online resta. **5 COSE DA EVITARE:** risposte aggressive – ironia poco chiara – messaggi vaghi – critiche personali – screenshot di chat private. Se ti sembra “così così”... probabilmente lo è.

Test di autovalutazione finale

Rispondi a queste domande per verificare ciò che hai imparato. Le risposte corrette si trovano in fondo alla sezione.

1. 1. Cos'è la netiquette? a) Un software per la sicurezza informatica. b) Il galateo della comunicazione online. c) Un social network professionale.
2. 2. Scrivere in MAIUSCOLO online equivale a: a) Dare enfasi positiva al messaggio. b) Urlare – ed è percepito come aggressivo. c) Segnalare l'urgenza del messaggio.
3. 3. Quale informazione NON va mai condivisa online? a) Il nome di un libro che hai letto. b) Il numero della carta di credito o di documenti di identità. c) Una foto di un tramonto.
4. 4. Cos'è il digital footprint? a) Un programma per tracciare i virus informatici. b) Le tracce lasciate online dalle proprie attività digitali. c) Un tipo di firma digitale per i documenti.
5. 5. Nei documenti condivisi, qual è la pratica corretta quando si vuole fare una modifica importante? a) Modificare direttamente senza avvisare, per non perdere tempo. b) Lasciare un commento che spiega la modifica proposta e chiede confronto. c) Inviare un messaggio privato all'autore e aspettare il suo accordo.
6. 6. Cosa fare se si riceve un messaggio aggressivo in un gruppo WhatsApp? a) Rispondere immediatamente in modo altrettanto deciso. b) Non rispondere nel gruppo – affrontare la questione in privato o ignorare. c) Aggiungere altre persone al gruppo per avere supporto.
7. 7. La comunicazione assertiva consiste nel: a) Dire sempre esattamente quello che si pensa senza filtri. b) Non dire nulla per evitare conflitti. c) Esprimere le proprie esigenze in modo chiaro e diretto, rispettando l'altro.
8. 8. Pubblicare foto di altre persone senza il loro consenso è: a) Accettabile se la foto è bella. b) Un rischio per la privacy e la reputazione di chi è ritratto. c) Consentito se si tratta di un'occasione pubblica.

Risposte: 1-b / 2-b / 3-b / 4-b / 5-b / 6-b / 7-c / 8-b

Autovalutazione delle competenze DigComp 2.2

Compila questa scheda prima e dopo il corso per misurare i tuoi progressi. Per ciascuna competenza, indica il tuo livello su una scala da 1 a 5: 1 = non mi sento ancora in grado, 5 = mi sento completamente autonomo.

Competenza DigComp 2.2	Area	Prima (1-5)	Dopo (1-5)
So comunicare in modo rispettoso online.	2.1		
So scegliere cosa condividere o meno.	2.2		
So comportarmi correttamente negli spazi pubblici online.	2.3		
So tutelare la mia immagine e reputazione digitale.	4.3		
So riconoscere quando devo migliorare le mie competenze digitali.	5.4		
Mi sento più sicuro/a nella comunicazione digitale.	Generale		

Glossario essenziale

Assertività: stile comunicativo che permette di esprimere le proprie opinioni ed esigenze in modo chiaro e diretto, rispettando allo stesso tempo quelle dell'altro. La terza via tra aggressività e passività.

Digital footprint (Impronta digitale): l'insieme delle tracce lasciate online da ogni attività digitale: post, commenti, like, ricerche, interazioni. Si divide in volontaria – ciò che si pubblica consapevolmente – e involontaria – dati generati automaticamente.

Diritto all'oblio: diritto garantito dal GDPR che permette di richiedere la cancellazione dei propri dati personali a un'organizzazione, o la rimozione di risultati dai motori di ricerca.

Flame: risposta aggressiva e sproporzionata a un messaggio online, che innesci quasi inevitabilmente una escalation del conflitto.

GDPR: Regolamento Generale sulla Protezione dei Dati dell'Unione Europea. Garantisce ai cittadini europei diritti sulla propria privacy e sui propri dati personali.

Identità digitale: l'insieme delle informazioni, dei contenuti e delle tracce che definiscono chi si è negli spazi online. Include profili ufficiali, contenuti pubblicati, menzioni altrui e dati comportamentali.

Netiquette: insieme delle regole di comportamento civile negli spazi digitali. Il termine nasce dalla fusione di network ed etichette. Non è un codice di legge: è un insieme di convenzioni condivise.

Oversharing: condivisione eccessiva di informazioni personali online, spesso senza considerare le potenziali conseguenze sulla propria privacy e reputazione.

Reputazione digitale: l'immagine che gli altri si formano di una persona attraverso la sua presenza e il suo comportamento online. Si costruisce nel tempo e può essere difficile da modificare una volta consolidata.

Spam: invio di messaggi non richiesti e non pertinenti. È una delle forme di mancanza di rispetto più diffuse nelle comunicazioni digitali di gruppo.

Trolling: pratica di provocare deliberatamente altri utenti online con commenti offensivi o fuori luogo, con l'unico scopo di generare reazioni emotive negative.

Gestire i conflitti digitali: dalla teoria alla pratica

Quando la comunicazione diventa conflitto

Anche con le migliori intenzioni e la migliore netiquette, i conflitti digitali accadono. Non sono il segnale che qualcosa è andato irrimediabilmente storto: sono parte normale della comunicazione tra esseri umani, che porta con sé incomprensioni, aspettative diverse, momenti difficili. La differenza non è evitare i conflitti, ma saperli gestire.

Un conflitto digitale segue quasi sempre la stessa traiettoria: un messaggio ambiguo o percepito come offensivo innesca una risposta reattiva, che a sua volta genera una contro-risposta altrettanto reattiva, e il tono si alza progressivamente fino a trasformare una conversazione normale in un litigio. Questa escalation segue una logica prevedibile, il che significa che può essere interrotta, se si riconosce in tempo a che punto del processo ci si trova.

Il protocollo di de-escalation

Quando ci si trova nel mezzo di un conflitto digitale, esistono alcune azioni che aiutano quasi sempre a uscirne senza danni.

La prima è fermarsi. Non rispondere. Anche se la risposta sembra urgente, anche se l'altro sta aspettando: fermarsi. Ogni secondo di pausa tra la lettura di un messaggio provocatorio e la scrittura della risposta è un secondo in cui la reazione emotiva si raffredda e la risposta razionale prende il sopravvento.

La seconda è rileggere il messaggio cercando attivamente un'interpretazione alternativa a quella che ha generato la reazione negativa. Chiediti: questo messaggio potrebbe avere un significato diverso? Se la risposta è sì, o anche solo 'forse', quella lettura alternativa è probabilmente la più vicina alla realtà. La maggior parte dei messaggi che sembrano offensivi sono semplicemente mal scritti.

La terza, se il conflitto è reale, è spostarlo dal canale scritto a quello verbale. Una telefonata di cinque minuti risolve spesso ciò che dieci messaggi non risolveranno mai. La voce trasmette tono, emozione, intenzione: tutto ciò che manca nella comunicazione scritta.

La quarta è usare la formula del 'io mi sono sentito + richiesta specifica' invece dell'accusa. 'Ho letto il tuo messaggio e mi sono sentito escluso dalla decisione, ti chiedo di coinvolgermi la prossima volta' è un'apertura al dialogo. 'Decidi sempre tutto tu senza consultarmi' è un attacco che genera difese.

I conflitti nei gruppi: regole specifiche

La prima regola è non risolvere conflitti privati in uno spazio pubblico. Se hai un problema con una persona del gruppo, affrontalo in privato. Portare il conflitto nel gruppo amplifica il danno per entrambe le parti e per il clima del gruppo nel suo insieme.

La seconda regola è non chiedere supporto nel gruppo prima di aver parlato direttamente con la persona interessata. Scrivere in un gruppo 'qualcuno sa perché X non ha fatto Y?' quando il messaggio è chiaramente diretto a X (che è nel gruppo) è una forma di pressione pubblica che si sostituisce al dialogo diretto.

La terza regola riguarda chi ha un ruolo di moderazione. Se sei l'amministratore di un gruppo e noti che la conversazione sta degenerando, hai la responsabilità di intervenire. Un messaggio breve, neutro e diretto come 'Restiamo in topic' o 'Propongo di continuare questa discussione in privato' è spesso sufficiente per spegnere una miccia prima che diventi un incendio.

Il benessere digitale

La netiquette riguarda il modo in cui comunichiamo con gli altri. Ma c'è un altro aspetto della vita digitale che merita attenzione: il modo in cui gli spazi digitali influenzano il nostro benessere. Non è un tema accessorio: è strettamente legato alla qualità della comunicazione. Chi è stressato, sovraccarico di notifiche, dipendente dalla validazione dei like scrive messaggi peggiori, reagisce in modo più impulsivo, è più vulnerabile ai conflitti.

Il benessere digitale si costruisce attraverso alcune scelte consapevoli: impostare limiti di tempo per le app che tendono a diventare compulsive, disattivare le notifiche non urgenti, non controllare il telefono nei primi e negli ultimi minuti della giornata, fare pause digitali regolari. Queste pratiche creano le condizioni di lucidità e calma in cui è più facile comunicare in modo consapevole.

L'ultimo consiglio: La prossima volta che ti trovi davanti a un messaggio difficile, ricorda: online non puoi controllare tutto, non puoi controllare le reazioni degli altri. Ma puoi sempre scegliere come comunicare. Questa è la netiquette.

TEMA B
**SICUREZZA E USO CONSAPEVOLE
DEI SERVIZI DIGITALI**

 **OPPORTUNITÀ DELLA RETE
E CYBERSECURITY**



Digita Facile
Campania

A chi è rivolto questo capitolo

Questo capitolo accompagna il percorso formativo dedicato alle Opportunità della Rete e alla Cybersecurity, sviluppato nell'ambito del progetto Digita Facile Campania. Si rivolge a chiunque voglia capire come funziona davvero internet, dalle sue origini alla sua evoluzione in corso, e come proteggersi efficacemente dai rischi digitali più concreti: i malware, i furti di dati, le truffe online, la perdita di informazioni preziose.

Il percorso è strutturato in quattro moduli. Il primo introduce la storia e l'evoluzione del web e dello smartphone, spiegando come queste tecnologie abbiano trasformato l'accesso alla rete e creato nuove opportunità e nuovi rischi. Il secondo esplora la difesa passiva del dispositivo: firewall, antimalware, aggiornamenti, e una guida dettagliata ai diversi tipi di malware. Il terzo si concentra sulla sicurezza attiva: i tre fattori di autenticazione, le password sicure e il riconoscimento biometrico. Il quarto conclude con la strategia di backup, l'unica vera difesa contro la perdita definitiva dei dati.

Non è richiesta alcuna competenza tecnica per seguire questa dispensa. I concetti sono spiegati con analogie della vita reale, esempi concreti e un linguaggio accessibile a chiunque. L'obiettivo non è formare esperti di informatica, ma costruire l'abitudine alla sicurezza digitale: quella serie di comportamenti quotidiani che, se interiorizzati, riducono drasticamente il rischio di diventare vittime della cybercriminalità.

La sicurezza digitale non è un prodotto da comprare: è un comportamento da adottare. Il lucchetto più sicuro al mondo è inutile se si lascia la porta aperta. Questa dispensa ti aiuta a capire dove sono le porte aperte e come chiuderle.

I numeri della cybercriminalità in Italia

La cybercriminalità non è un problema che riguarda solo le grandi aziende o i governi. Nel 2024, le truffe digitali, soprattutto legate a pagamenti elettronici e phishing, hanno colpito circa 2,9 milioni di italiani, con un danno economico stimato di 880 milioni di euro. Sono numeri che rendono la criminalità informatica una delle forme di crimine più diffuse nel paese, molto più presenti nella vita quotidiana di quanto si percepisca.

In Campania, nel 2024-2025, sono stati sequestrati oltre 2.000 SIM card utilizzate per frodi digitali e risultano 23 indagati per phishing e furto di dati personali. Il fenomeno è locale quanto globale: le stesse tecniche di inganno usate dai cybercriminali di tutto il mondo vengono impiegate anche nei comuni e nelle città campane, colpendo persone di ogni età e condizione.

Questi dati non sono citati per spaventare: sono citati per rendere concreto un rischio che spesso viene percepito come astratto o lontano. La domanda non è se potreste essere colpiti, ma quando e quanto sarete preparati quando accadrà.

La cybersicurezza è soprattutto comportamento

La cybersicurezza è l'insieme di tecnologie, ma soprattutto di comportamenti, che servono a proteggere la nostra vita digitale da furti, danni o accessi non autorizzati. La parola più importante di questa definizione non è "tecnologie", bensì "comportamenti". Gli strumenti di protezione quali antivirus, firewall, autenticazione a due fattori, funzionano solo se vengono attivati e usati correttamente. E il modo in cui si sceglie di comportarsi online (quale link si clicca, che password si sceglie, che informazioni si condividono) determina la sicurezza molto più di qualsiasi software.

Questo non significa che gli strumenti tecnici non contino: contano eccome, e li vedremo in dettaglio. Ma significa che la sicurezza digitale non è qualcosa che si 'compra' una volta e poi si dimentica: è qualcosa che si 'pratica' ogni giorno, con le scelte che si fanno ogni volta che si usa un dispositivo connesso a Internet.

OPPORTUNITÀ DELLA RETE: WEB, SMARTPHONE E CYBERSICUREZZA

Obiettivi del modulo

Al termine di questo modulo comprenderai come lo smartphone ha democratizzato l'accesso a internet, riducendo il gap digitale anche nelle fasce della popolazione storicamente più escluse. Conoscerai l'evoluzione del web nelle sue tre fasi fondamentali e capirai perché il passaggio dal Web 1.0 al Web 3.0 ha creato nuove opportunità ma anche nuove responsabilità per ciascun utente.

Lo smartphone: la rivoluzione in tre passi

Prima dello smartphone, internet era uno strumento per chi aveva un computer e che costava, ingombrava, richiedeva una certa familiarità tecnica, nonché una connessione stabile a casa o in ufficio. La tecnologia digitale era potente, ma non era per tutti. Lo smartphone ha cambiato questa equazione in modo radicale, attraverso tre trasformazioni fondamentali.

La prima trasformazione è stata l'abolizione dell'intermediario fisico. Il touchscreen ha eliminato la tastiera e il mouse, strumenti che richiedevano un apprendimento specifico, sostituendoli con il gesto naturale del tocco. Per la prima volta nella storia della tecnologia, l'interfaccia di un computer è diventata intuitiva per persone che non avevano mai usato un mouse, che non sapevano dove mettere le mani su una tastiera, che si sentivano estranee di fronte a uno schermo tradizionale. Il tap, lo swipe, la doppia pressione: sono gesti che si imparano in minuti, non in settimane.

La seconda trasformazione è stata la semplificazione del software attraverso il modello delle app. Prima degli smartphone, un programma informatico era un oggetto complesso che faceva molte cose, di cui non necessariamente si avesse bisogno, ma di cui era necessario imparare, comunque, l'interfaccia completa per trovare quella che ti serviva. Le app hanno introdotto un principio opposto: ogni icona fa una cosa sola, e la fa nel modo più semplice possibile. Vuoi chiamare qualcuno? C'è un'app. Vuoi guardare una mappa? C'è un'app. Vuoi prenotare una visita medica? C'è un'app. Questa frammentazione funzionale ha reso la tecnologia accessibile a persone che non avrebbero mai imparato a usare un software tradizionale.

La terza trasformazione è stata la mobilità assoluta. Per la prima volta, un computer potente con connessione internet, fotocamera, GPS, microfono, sensori è diventato qualcosa che si porta in tasca ovunque, disponibile in ogni momento. Questo ha significato che non serve più avere un computer a casa per accedere ai servizi digitali: basta avere uno smartphone.

I dati: chi ha guadagnato di più dalla rivoluzione smartphone

L'impatto della rivoluzione smartphone sull'inclusione digitale è documentato e straordinario. I dati parlano chiaro. Tra il 2009-2010 (era del PC come strumento principale di accesso a internet) e il 2024-2025, la quota di italiani over 65 con accesso a internet è passata dal 5,8% al 68,1%: un incremento di oltre il 1.000%. Tra gli over 75, dal 2,7% al 31,4%. Nel Sud Italia, l'accesso a internet è passato dal 43% al 77,5% della popolazione.

Questi numeri raccontano una storia di inclusione digitale senza precedenti. Lo smartphone ha raggiunto persone che il computer non aveva mai raggiunto: anziani che trovavano il PC troppo complicato, famiglie a basso reddito che non potevano permettersi un computer di buona qualità, abitanti di aree geografiche con scarsa infrastruttura tecnologica. Il fenomeno del mobile-only (il 69% degli italiani accede alla rete prevalentemente o esclusivamente tramite smartphone) è la conferma che lo smartphone non è semplicemente un'alternativa al PC: per molti è l'unico dispositivo con cui si entra in internet.

Lo smartphone ha anche contribuito a ridurre il divario tra Nord e Sud Italia nell'accesso digitale: da una differenza del 12% nel 2010 a una differenza del 7% nel 2024. Non è ancora zero, ma la direzione è chiara.

Dato da ricordare: Solo il 21% degli italiani non sa usare lo smartphone, contro il 34% di chi non sa usare il PC. Lo smartphone è diventato il dispositivo digitale più accessibile che sia mai esistito.

L'evoluzione del Web: da biblioteca a piazza a ecosistema di valore

Il World Wide Web — inventato da Tim Berners-Lee nel 1991 — è il sistema che permette la condivisione di documenti ipertestuali multimediali attraverso l'infrastruttura di internet. È importante distinguere web e internet: internet è la rete fisica di connessioni tra computer; il web è uno dei servizi che si può usare attraverso quella rete, il più diffuso e il più conosciuto. Quando apriamo un browser e visitiamo un sito, stiamo usando il web. Quando mandiamo un'e-mail, stiamo usando internet ma non necessariamente il web.

Il web ha attraversato tre fasi evolutive fondamentali, ognuna delle quali ha cambiato il modo in cui gli utenti interagiscono con la rete.

Web 1.0 — La Grande Biblioteca (Solo Lettura): la prima fase del web, dalla metà degli anni Novanta alla fine degli anni Novanta, era essenzialmente un'enciclopedia digitale globale. I siti web esistevano, ma erano statici: chiunque poteva leggerli, ma quasi nessuno poteva scriverci. Gli utenti erano visitatori passivi di una biblioteca immensa, non lineare e senza confini geografici. La rivoluzione era enorme: accesso immediato a informazioni da qualsiasi parte del mondo, ma la partecipazione era zero.

Web 2.0 – La Piazza Partecipativa (Lettura e Scrittura): a partire dai primi anni Duemila, il web si è trasformato in uno spazio partecipativo. I blog hanno permesso a chiunque di pubblicare. I social network hanno creato spazi di connessione e condivisione. Le piattaforme di video come YouTube hanno democratizzato la produzione e distribuzione di contenuti audiovisivi. I contenuti generati dagli utenti (UGC, User Generated Content) sono diventati il cuore del web. Internet non è più soltanto un medium alternativo ai libri e ai giornali: è diventato un ambiente digitale in cui si vive, si comunica, si lavora, ci si esprime.

Web 3.0 – L'Internet del Valore (Possesso e Sicurezza): la fase attuale e in evoluzione del web introduce un cambiamento fondamentale: il web non gestisce più solo informazioni, ma valore, sia economico che personale. Le tecnologie blockchain permettono la creazione di beni digitali scarsi e unici, non duplicabili come i file tradizionali. I dati personali possono restare in possesso dell'utente invece di essere ceduti alle piattaforme. Il concetto di intermediario digitale (l'azienda che gestisce le transazioni tra utenti) viene messo in discussione da sistemi decentralizzati. Questa evoluzione porta opportunità enormi, ma anche nuove responsabilità: nel Web 3.0, la sicurezza digitale dipende ancora di più dalle azioni individuali di ciascun utente.

La cybersicurezza: perché è diventata urgente

L'evoluzione del web da biblioteca a piazza partecipativa a ecosistema di valore ha portato con sé una crescita parallela dei rischi. Nel Web 1.0, si poteva al massimo perdere tempo su siti inaffidabili. Nel Web 2.0, i dati personali sono diventati la moneta del web, e quindi un bene da proteggere. Nel Web 3.0, con l'introduzione di valore economico direttamente gestibile online, i rischi di furto e frode sono diventati ancora più concreti e immediati.

La cybersicurezza risponde a questa evoluzione con un approccio su due livelli. Il primo è la protezione passiva: gli strumenti che lavorano in background, come sentinelle silenziose, per bloccare le minacce prima che raggiungano l'utente, attraverso firewall, antivirus, filtri antispam. Il secondo è la sicurezza attiva: le scelte e i comportamenti dell'utente che determinano il livello di rischio a cui si espone, come la scelta della password, l'attivazione dell'autenticazione a due fattori, la gestione del backup dei dati. Entrambi i livelli sono necessari: uno senza l'altro è insufficiente.

Obiettivi del modulo

Al termine di questo modulo conoscerai i tre strumenti fondamentali di protezione passiva del dispositivo: il firewall, l'antimalware e gli aggiornamenti del sistema operativo e delle app. Saprai come funzionano e perché ciascuno è indispensabile. Conoscerai i principali tipi di malware (ransomware, trojan, virus, worm, spyware) e le strategie per proteggersi da ciascuno.

L'analogia della casa: proteggere il digitale come la vita reale

La sicurezza digitale è spesso percepita come qualcosa di astratto e tecnico. In realtà, si basa sugli stessi principi della sicurezza fisica che usiamo ogni giorno senza pensarci. Chiudiamo la porta a chiave quando usciamo di casa/ blocchiamo il dispositivo con PIN o impronta. Non apriamo la porta a degli sconosciuti/non clicchiamo su link sconosciuti. Installiamo un allarme/ usiamo un antivirus. Facciamo manutenzione alla serratura, alle finestre o al muro di cinta/aggiorniamo il sistema operativo. Teniamo i documenti importanti in cassaforte/ usiamo password sicure e backup.

Ogni strumento di sicurezza digitale ha un equivalente fisico intuitivo. Usare questo parallelismo aiuta a capire non solo come funziona ogni strumento, ma anche perché è importante e cosa succede quando lo si trascura.

Il Firewall: il muro di cinta digitale

Il firewall è un sistema che può essere un software, un hardware, o entrambi e che controlla tutto il traffico che entra e che esce dal dispositivo. Come un muro di cinta con un cancello presidiato, decide chi può passare e chi deve essere fermato.

In entrata, il firewall blocca chi cerca di connettersi al dispositivo senza esserne stato invitato: hacker che scansionano la rete alla ricerca di dispositivi vulnerabili, programmi automatizzati che tentano accessi non autorizzati, traffico sospetto proveniente da indirizzi noti come pericolosi. In uscita, blocca i programmi che cercano di comunicare con l'esterno senza che l'utente ne sia consapevole: un malware che ha infettato il dispositivo potrebbe cercare di inviare dati rubati a un server criminale, il firewall può intercettare e bloccare questa comunicazione.

Esistono due tipi principali di firewall. Il firewall di rete è quello integrato nel modem/router di casa: protegge tutti i dispositivi collegati alla rete domestica, lavorando come un unico punto di controllo per l'intera casa. Il firewall personale è il software installato direttamente sul singolo dispositivo, come Windows Defender su Windows, ed equivalenti su Mac e smartphone. En-

trambi sono utili e si completano a vicenda.

Non disattivare mai il firewall quando sei connesso a Internet, specialmente su reti Wi-Fi pubbliche, come ad esempio quelle attivate nei bar, stazioni, aeroporti. Queste reti sono ambienti ad alto rischio in cui le probabilità di incontrare traffico malevolo sono molto più alte che nella rete domestica.

L'antimalware: dalla lista nera all'analisi comportamentale

L'antivirus tradizionale funzionava come una lista nera: cercava i programmi malevoli noti e li bloccava. Se il programma era nuovo e non ancora nella lista, passava. Oggi, gli antimalware moderni usano un approccio molto più sofisticato, basato sull'analisi comportamentale: invece di cercare programmi già conosciuti come pericolosi, osservano il comportamento di ogni programma e bloccano qualsiasi cosa si comporti in modo sospetto, anche se non era mai stata vista prima.

Il principio è elegante: se un programma sconosciuto sta cercando di cifrare tutti i file del disco, di disattivare l'antivirus, di connettersi a un server sconosciuto all'estero e di cancellare i log di sistema, si sta comportando esattamente come si comporterebbe un malware — anche se non è mai stato visto prima. L'antimalware moderno lo blocca preventivamente.

La funzione di scansione in tempo reale è quella che rende l'antimalware davvero efficace: non si aspetta che l'utente lanci manualmente una scansione, ma lavora costantemente in background, analizzando ogni file che viene aperto o scaricato nel momento stesso in cui avviene. È la differenza tra un medico che visita il paziente solo quando ha già la febbre alta e uno che monitora i parametri vitali in modo continuo. Scansiona il QR code in calce al Modulo 2 per avere una panoramica dei migliori Antimalware in circolazione

Consiglio pratico: Windows Defender, l'antimalware integrato in Windows 10 e 11, è gratuito e già installato. Molti pensano che non sia abbastanza, ma le valutazioni indipendenti lo collocano costantemente tra i migliori strumenti disponibili. Attivarlo e tenerlo aggiornato è il primo e più importante passo.

Gli aggiornamenti: chiudere le finestre rotte

I criminali informatici non scassinano la porta blindata: cercano le finestre rotte. Ogni software, che sia Windows, Android, iOS, le app bancarie, il browser, nasce con dei piccoli difetti tecnici chiamati vulnerabilità o bug. Non perché i programmatori siano incompetenti, ma perché qualsiasi sistema complesso ha imperfezioni che non vengono scoperte finché qualcuno non le cerca atti-

vamente. Gli hacker scoprono queste vulnerabilità e le usano per entrare nei dispositivi: questo processo si chiama exploit. Gli sviluppatori del software, quando vengono informati di una vulnerabilità, rilasciano un aggiornamento che la corregge, chiamato patch e che significa, letteralmente, “toppa”. Se non si installa l’aggiornamento, la vulnerabilità resta aperta, anche se tutti sanno che esiste e come sfruttarla.

Ritardare gli aggiornamenti è una delle abitudini più rischiose in ambito di sicurezza digitale. Non è raro che nel giro di ore o giorni dalla scoperta di una vulnerabilità, i cybercriminali inizino a sfruttarla su scala massiccia. Aggiornare prontamente è l’equivalente di riparare una serratura rotta prima che qualcuno la noti.

Attiva gli aggiornamenti automatici su tutti i tuoi dispositivi. Sia per il sistema operativo – Windows, Android, iOS – sia per le app più critiche, come browser e app bancarie. Questo piccolo gesto automatizzato è una delle misure di sicurezza più efficaci disponibili.

I tipi di malware: conoscere il nemico

Il termine malware (contrazione di malicious software) indica qualsiasi programma progettato per arrecare danni al sistema su cui viene eseguito o per sottrarre informazioni all’insaputa dell’utente. Non tutti i malware sono uguali: ognuno ha un obiettivo specifico e funziona in modo diverso. Conoscerli aiuta a capire quali comportamenti evitare e quali strumenti usare per proteggersi.

- **Il Ransomware** – Il Sequestratore: è la minaccia più temuta oggi. Il nome viene dall’inglese ransom, che significa riscatto. Il ransomware non ruba i dati per portarli via: li blocca sul posto, cifrandoli con una chiave che solo l’attaccante conosce, rendendoli completamente illeggibili. Sullo schermo appare un conto alla rovescia e una richiesta di pagamento, spesso in criptovalute per rendere il pagamento difficile da tracciare. La triste verità è che pagare il riscatto non garantisce di ricevere la chiave per sbloccare i file. L’unica vera difesa contro il ransomware non è l’antivirus: è il backup regolare dei dati. Se si ha una copia recente dei propri file in un luogo separato, si può semplicemente ripristinare dal backup senza dover pagare nulla.
- **Il Trojan** – Il Cavallo di Troia: prende il nome dal leggendario inganno della guerra di Troia. Si presenta come un programma utile, innocuo o desiderabile, un gioco gratuito, una fattura da scaricare, un aggiornamento di software e, una volta installato volontariamente dall’utente, apre una porta di servizio nel sistema che permette all’attaccante di entrare liberamente. La caratteristica fondamentale del Trojan è che non entra da solo: deve essere invitato. È sempre l’utente ad aprire la porta, credendo di fare qualcos’altro.

- **Virus vs Worm** — Il Parassita e il Viaggiatore: spesso usiamo “virus” come sinonimo di qualsiasi malware, ma tecnicamente ha un significato preciso. Il virus informatico funziona come quello biologico: ha bisogno di un ‘ospite’ per diffondersi, di fatti, infetta un file un documento, un programma e si diffonde solo se quell’utente passa quel file ad altri, via email o su una chiavetta USB. Il worm (verme) è invece completamente autonomo: si clona da solo e salta da un computer all’altro sfruttando la connessione internet, senza che l’utente faccia nulla. Può infettare migliaia di dispositivi in poche ore, intasando reti e causando danni su scala massiccia.
- **Spyware, Keylogger e Rootkit** — Le Spie Silenziose: questi malware non vogliono distruggere o bloccare: vogliono restare nascosti il più a lungo possibile, raccogliendo informazioni. Lo spyware registra le attività dell’utente, come ad esempio i siti visitati, le app usate, le abitudini digitali e le invia a terzi. Il keylogger è ancora più specifico e più pericoloso: registra ogni singolo tasto premuto sulla tastiera, intercettando automaticamente password, numeri di carta di credito, messaggi privati. Il rootkit è il più sofisticato e difficile da rimuovere: si nasconde nel nucleo più profondo del sistema operativo, a livello amministratore, e può disattivare altri programmi di sicurezza (incluso l’antivirus) senza che l’utente se ne accorga. Spesso l’unico modo per eliminarlo è reinstallare completamente il sistema operativo.

Filtri Antispam: il sistema di Vigilanza attiva

Se l’Antimalware è l’antifurto di casa, che entra in azione quando un ladro (un virus o un hacker) cerca di forzare la porta per rubare i tuoi dati o distruggere i mobili, i filtri Antispam per email e chiamate sono come la Vigilanza del quartiere, che agisce al di fuori delle mura domestiche.

Bloccare alla radice queste comunicazioni significa non farsi distrarre continuamente dallo smartphone che squilla a vuoto, mantenere la casella di posta ordinata e, soprattutto, evitare di cadere in truffe (phishing) mascherate da finte offerte commerciali.

Se ricevi una chiamata sospetta, l’intelligenza artificiale può rispondere per te, chiedere a chi chiama cosa vuole e mostrarti la trascrizione sullo schermo, oppure bloccare la chiamata in automatico se il numero è noto per essere spam, come fanno Google (sui telefoni Android, in particolare Pixel e Samsung) e app di terze parti (come Truecaller o Hiya, installabili su qualsiasi smartphone). Per evitare di finire nelle liste degli spammer, puoi impedire ai mittenti di sapere se hai aperto la loro email, oppure creare indirizzi fittizi temporanei quando ti iscrivi a siti di dubbia affidabilità, come permette di fare Apple (con la Protezione della privacy in Mail e la funzione “Nascondi la mia email” di iCloud+). Puoi “insegnare” al tuo provider cosa è spam segnalando i messag-

gi manualmente (invece di cancellarli e basta), oppure impostare regole che bloccano a priori chi non è tra i tuoi contatti.

Infine, è possibile attivare il blocco del telemarketing autorizzato. Ci si iscrive a un database nazionale per revocare i consensi commerciali dati in passato ed evitare chiamate dai call center legali, iscrivendosi al Registro Pubblico delle Opposizioni.

Inquadrando il QR code è possibile avere una guida per i Filtri Antispam.



I FATTORI DI SICUREZZA: PASSWORD, 2FA E BIOMETRIA

Obiettivi del modulo

Al termine di questo modulo comprenderai i tre fattori fondamentali di autenticazione e saprai come combinarli per proteggere i propri account. Saprai creare password sicure usando il metodo della passphrase e capirai perché la lunghezza è più importante della complessità. Conoscerai il funzionamento del riconoscimento biometrico e saprai come attivare l'autenticazione a due fattori sui principali servizi online.

I tre fattori di sicurezza

Qualsiasi sistema di autenticazione, cioè qualsiasi sistema che verifica che sei davvero chi dici di essere, si basa su tre categorie fondamentali di prove. Conoscerle aiuta a capire perché certi sistemi di protezione sono più sicuri di altri e come costruire una difesa efficace.

Qualcosa che SAI – la Conoscenza: è la categoria più classica e più diffusa: password, PIN, domande di sicurezza. Il vantaggio è che non si può rubare fisicamente. Lo svantaggio è che può essere indovinata, intercettata da malware, rubata attraverso il phishing, o ceduta ingenuamente dall'utente stesso. Ogni giorno milioni di persone inseriscono la propria password su siti falsi convinte di essere sul sito originale.

Qualcosa che HAI – il Possesso: è un oggetto fisico che dimostra la tua identità. Un tempo erano le chiavette bancarie che generavano codici numerici; oggi è quasi sempre lo smartphone. Il vantaggio rispetto alla sola password è fondamentale: un cybercriminale può rubare la tua password stando dall'altra parte del mondo, ma non può prendere il tuo telefono che è fisicamente nella tua tasca nello stesso momento. Questa è la base dell'autenticazione a due fattori: anche se qualcuno ha la tua password, senza il tuo telefono non può accedere al tuo account.

Qualcosa che SEI – la Biometria: sono le tue caratteristiche fisiche uniche: l'impronta digitale, il riconoscimento del volto, la scansione dell'iride. Il vantaggio è che non puoi dimenticarla a casa e non può essere indovinata. Il limite è che, a differenza di una password, non puoi cambiarla se viene compromessa, non puoi cambiare le tue impronte digitali.

La sicurezza ideale combina almeno due di questi tre fattori: è questo il principio dell'autenticazione a due fattori (2FA) che vedremo a breve.

Le password: lunghezza batte complessità

La saggezza convenzionale sulla sicurezza delle password dice di usare **caratteri speciali, numeri, maiuscole e minuscole**. Questa indicazione non è sbagliata, ma nasconde un punto più importante: la lunghezza di una password è il fattore che più influenza la sua resistenza agli attacchi automatizzati.

Consideriamo due password. La prima è una stringa casuale di 8 caratteri: K9#mP_2\$. Sembra sicura, visto che ha caratteri speciali, numeri, lettere di diverso tipo. Ma ha solo 8 caratteri. La seconda è una frase di senso compiuto: Estate24-Korfù@love1. Ha 20 caratteri, è facile da ricordare perché racconta qualcosa (una vacanza del 2024) e include comunque numeri e caratteri speciali. Quale è più sicura? La seconda, in modo netto. Un attacco automatizzato che prova miliardi di combinazioni al secondo impiega secondi a craccare una password di 8 caratteri, anche complessa. Una passphrase di 20 caratteri richiede diversi anni anche con i computer più potenti.

Il metodo della passphrase, una frase o una serie di parole che hanno un senso per te ma non per nessun altro, è oggi considerato dai professionisti della sicurezza il modo migliore per creare password che siano al tempo stesso sicure e memorizzabili. Una passphrase efficace racconta qualcosa di personale e specifico, usa maiuscole e caratteri speciali naturalmente, e si colloca tra i 15-20 caratteri.

Alcune regole aggiuntive completano il quadro. Non usare mai la stessa password su più account: se un servizio viene violato e la tua password viene rubata, tutti gli account che usano la stessa password sono immediatamente a rischio. Non usare dati personali facilmente reperibili — nome, data di nascita, nome degli animali domestici — che possono essere indovinati da chi ti conosce o da chi cerca informazioni su di te online. Usare un password manager, ossia un programma che crea, memorizza e inserisce automaticamente password sicure e diverse per ogni servizio, è la soluzione più pratica per gestire decine di account diversi senza dover ricordare decine di password diverse.



Esercizio pratico: Crea adesso una passphrase usando questo schema: [Stagione/Anno]–[Luogo]@[Parola]N. Ad esempio: Inverno2023–Napoli@mare7. È lunga, memorizzabile e sicura. Usa questo schema per proteggere i tuoi account più importanti.

L'autenticazione a due fattori: il doppio lucchetto

L'autenticazione a due fattori – **2FA** – combina il primo fattore (qualcosa che sai: la tua password) con il secondo fattore (qualcosa che hai: il tuo smartphone). Il principio è semplice: anche se qualcuno riesce a ottenere la tua password, senza accesso fisico al tuo telefono non può entrare nel tuo account.

In pratica, quando si attiva la 2FA su un account e si cerca di accedere da un dispositivo nuovo o non riconosciuto, dopo aver inserito la password il sistema chiede un secondo codice di verifica, generalmente un numero a 6 cifre che arriva via SMS o viene generato da un'app dedicata come Google Authenticator o Authy. Questo codice è valido solo per pochi secondi: anche se qualcuno lo intercettasse, non avrebbe il tempo di usarlo.



La 2FA è disponibile su quasi tutti i principali servizi online. Su Google/Gmail: Account Google → Sicurezza → Verifica in due passaggi. Su Facebook/Meta: Impostazioni e Privacy → Password e Sicurezza → Autenticazione a due fattori. Su Amazon: Il mio account → Accesso e sicurezza → Verifica in due fasi. Su WhatsApp: Impostazioni → Account → Verifica in due passaggi. Sulle app bancarie: cercare la voce Sicurezza o Privacy nelle impostazioni dell'app.

Attivare la 2FA sugli account più importanti, come email principale, conto bancario, account Google o Apple, social network, è la misura di sicurezza con il miglior rapporto tra facilità di implementazione e livello di protezione. Lo si fa una volta e poi funziona automaticamente. Fallo oggi.

Il riconoscimento biometrico: come funziona davvero

I sistemi di riconoscimento biometrico (impronta digitale, riconoscimento facciale, scansione dell'iride) sono oggi integrati in quasi tutti gli smartphone moderni e in molte app, incluse le app bancarie. La loro adozione è cresciuta rapidamente perché sono comodi: sbloccare il telefono con il dito è più veloce che digitare un PIN. Inoltre, sono genuinamente sicuri, se usati correttamente.

Ma come funzionano esattamente? Il telefono non salva la foto del vostro dito o del vostro viso. Quando registrate l'impronta o il viso per la prima volta, il dispositivo trasforma quell'informazione fisica in un codice matematico, una stringa numerica molto lunga, attraverso un processo a senso unico: dal dito si crea il codice, ma dal codice non si può ricostruire il dito. Questo è fondamentale: significa che anche se qualcuno riuscisse a rubare i dati dal vostro telefono, non potrebbe estrarne una 'copia' della vostra impronta.

Questo codice matematico non viene mai inviato ai server di Apple, Google o Samsung. Non viaggia su internet. Resta chiuso in un chip speciale all'interno del dispositivo, chiamato Secure Enclave su iOS o TrustZone su Android, completamente isolato dal resto del sistema. Quando posate il dito sul sensore, il sistema legge l'impronta, genera il codice e chiede al chip: 'I codici corrispondono?'. Il chip risponde solo 'Sì' o 'No'. Il codice originale non esce mai dal chip.

Un aspetto importante da capire: la biometria è una comodità che sblocca la vera chiave di sicurezza, che è il PIN o la password principale. Quando si riavvia il telefono dopo averlo spento, il sistema chiede il PIN e non l'impronta: è una misura di sicurezza deliberata. Dopo il riavvio, il chip che contiene il codice biometrico viene 'resettato' e serve la chiave maestra (PIN) per riattivarlo. Questo significa che chiunque trovasse il vostro telefono spento non potrebbe sbloccarlo con la vostra impronta senza conoscere anche il PIN.

Obiettivi del modulo

Al termine di questo modulo comprenderai perché il backup è l'unica vera difesa contro la perdita definitiva dei dati. Conoscerai la regola 3-2-1 e saprai come applicarla nella vita quotidiana. Saprai distinguere tra i diversi tipi di backup e scegliere la combinazione più adatta alle tue esigenze.

Perché il backup è la misura di sicurezza più importante

Tutti gli strumenti di sicurezza che abbiamo discusso (firewall, antimalware, autenticazione a due fattori, password sicure) servono a prevenire che qualcosa vada storto. Il backup serve per quando qualcosa va storto comunque. E, nella sicurezza digitale, il 'quando' non è un'ipotesi: è una certezza.

Un dispositivo può rompersi. Può essere rubato. Può essere colpito da un ransomware che cifra tutti i file. Può essere danneggiato dall'acqua, dalla caduta, da un fulmine. Può essere accidentalmente formattato. Può subire un guasto hardware improvviso. Per ognuno di questi scenari, che sono tutti scenari reali e che capitano ogni giorno a milioni di persone, l'unica soluzione è avere una copia dei dati in un luogo separato.

Senza backup, la perdita è definitiva. Con un backup recente, è un inconveniente temporaneo. La differenza tra i due scenari è enorme sia in termini economici, ma soprattutto in termini emotivi, quando si tratta di foto, video, documenti personali che non si possono ricreare.

La regola 3-2-1: il gold standard del backup

I professionisti della sicurezza informatica hanno codificato decenni di esperienza in un principio semplice e memorizzabile: la regola 3-2-1. Tre copie dei dati. Due supporti diversi. Una copia fuori sede.

3 copie totali: non basta l'originale, e non basta una sola copia. L'obiettivo è avere tre istanze dei propri dati: l'originale sul dispositivo principale, più due copie di sicurezza. Il motivo è semplice: i dischi si rompono, i backup falliscono silenziosamente, gli incidenti capitano. Con tre copie, se anche due si perdono simultaneamente, la terza salva tutto.

2 supporti diversi: le due copie di sicurezza non devono stare sullo stesso tipo di supporto. Una su hard disk esterno e una su cloud, ad esempio. Oppure una su DVD e una su NAS di rete. Perché? Perché ogni tecnologia ha le sue vulnerabilità specifiche: un hard disk meccanico si rompe se cade, un DVD si graffia e diventa illeggibile, una chiavetta USB si smagnetizza nel tempo. Usare tecnologie diverse riduce il rischio che lo stesso tipo di guasto distrugga entrambe le copie.

1 copia fuori sede: questa è la componente più importante e più spesso trascurata. Una copia deve stare fisicamente lontana dal dispositivo originale. Se tutte le copie sono nello stesso posto – nel cassetto di casa con il computer – un furto, un allagamento, un incendio le distrugge tutte contemporaneamente. La copia fuori sede può essere un disco esterno a casa di un familiare fidato, oppure, molto più semplicemente, il cloud.

Applicare la regola 3-2-1 a un esempio concreto: le foto del battesimo del nipotino. Copia 1 – originale: nella galleria del telefono. Copia 2 – locale: su un hard disk esterno tenuto in casa. Copia 3 – fuori sede: caricata automaticamente su Google Foto o iCloud. Anche se il telefono cade nel mare, anche se l'hard disk si rompe, anche se viene rubata la borsa con entrambi i dispositivi, le foto sono al sicuro nel cloud.

I tipi di backup: scegliere quello giusto

Non tutti i backup sono uguali. Esistono diverse tipologie, ognuna con vantaggi e limiti specifici.

Backup locale – il disco esterno: un hard disk USB esterno collegato al computer. Il vantaggio è la velocità: il trasferimento dei dati avviene alla velocità della connessione USB, che è molto rapida per grandi quantità di dati. Lo svantaggio è che il disco fisico può rompersi, essere rubato o danneggiato insieme al computer originale. È ideale come prima copia di sicurezza, da usare in combinazione con il cloud.

Backup su cloud: i dati vengono copiati automaticamente su server remoti attraverso internet. I servizi più diffusi sono Google Foto e Google Drive, iCloud di Apple, Microsoft OneDrive, Dropbox. Il vantaggio è l'accessibilità, di fatti i dati sono disponibili da qualsiasi dispositivo connesso e la protezione geografica: i dati sono fisicamente lontani dal dispositivo originale, protetti da incidenti locali. Lo svantaggio è che richiede una connessione internet sufficiente per caricare i dati, e che si dipende dalla continuità del servizio.

Backup dei file vs immagine di sistema: il backup dei file copia solo i dati che si vuole proteggere – documenti, foto, video. È sufficiente per la maggior parte delle esigenze quotidiane e richiede meno spazio. Il backup dell'immagine di sistema crea una copia completa di tutto il disco, del sistema operativo, dei programmi installati, di configurazioni e dati e permette di ripristinare il computer esattamente com'era prima di un guasto grave, senza dover reinstallare tutto da zero. È più pesante e più lento, ma prezioso in caso di guasti hardware gravi.

Azione immediata: Se non hai ancora un backup dei tuoi dati, attiva Google Foto sul tuo smartphone adesso. Va in Impostazioni → Google Foto → Backup e attiva la sincronizzazione automatica. Tutte le foto e i video del telefono verranno copiati automaticamente nel cloud ogni volta che sei connesso al Wi-Fi. È gratuito per le foto in qualità standard ed è la singola azione più utile che puoi fare oggi per proteggere i tuoi dati.

Riepilogo dei concetti fondamentali

Questo percorso formativo ha costruito una comprensione completa della sicurezza digitale, dalle sue fondamenta storiche agli strumenti pratici di protezione quotidiana.

La rivoluzione dello smartphone ha democratizzato l'accesso a internet, portando online fasce della popolazione che il PC non aveva mai raggiunto. Il web si è evoluto dalla biblioteca statica del Web 1.0, attraverso la piazza partecipativa del Web 2.0, fino all'ecosistema di valore del Web 3.0, in cui la sicurezza individuale è diventata più importante che mai perché i rischi di furto e frode sono cresciuti insieme alle opportunità.

La protezione passiva del dispositivo si basa su tre strumenti fondamentali: il firewall, che controlla il traffico in entrata e in uscita; l'antimalware, che analizza il comportamento dei programmi per bloccare le minacce; gli aggiornamenti regolari, che chiudono le vulnerabilità prima che vengano sfruttate. I diversi tipi di malware hanno obiettivi e comportamenti specifici: il ransomware sequestra i dati chiedendo un riscatto; il trojan entra mascherandosi da programma utile; il worm si diffonde autonomamente di rete in rete; lo spyware e il keylogger spierebbero silenziosamente raccogliendo dati preziosi.

La sicurezza attiva si costruisce sui tre fattori di autenticazione (qualcosa che sai, qualcosa che hai, qualcosa che sei) e sulla loro combinazione. Le password sicure usano il metodo della passphrase: una frase lunga e memorizzabile battuta in sicurezza qualsiasi stringa breve e casuale. L'autenticazione a due fattori aggiunge un secondo livello di protezione che rende praticamente impossibile accedere a un account anche conoscendo la password. Il riconoscimento biometrico è sicuro perché il codice non esce mai dal chip del dispositivo.

Il backup — nella sua forma 3-2-1 — è l'unica vera difesa contro la perdita definitiva dei dati. Tre copie, su due supporti diversi, di cui una fuori sede: questa regola semplice protegge anche dai peggiori scenari, quali ransomware, furto, incendio, guasto hardware.

La sicurezza digitale non richiede di diventare esperti. Richiede di adottare poche abitudini quotidiane: aggiornare il dispositivo, usare password diverse e sicure, attivare la 2FA sugli account importanti, fare il backup dei dati. Chi fa queste quattro cose è già molto più sicuro della media degli utenti digitali.

Test di autovalutazione

Indica la risposta corretta per ciascuna domanda. Le risposte si trovano in fondo alla sezione.

1. Cosa ha reso lo smartphone più accessibile del PC per le fasce della popolazione meno tecnologiche? a) Il costo più basso. b) Il touchscreen che ha eliminato la necessità di imparare tastiera e mouse. c) La connessione Wi-Fi più veloce.
2. Qual è la fase del web in cui gli utenti sono diventati anche produttori di contenuti? a) Web 1.0. b) Web 2.0. c) Web 3.0.
3. Cos'è un firewall? a) Un software per navigare su internet. b) Un sistema che controlla il traffico che entra e esce dal dispositivo. c) Un tipo di anti-virus per gli smartphone.
4. Qual è la vera difesa contro il ransomware? a) Un buon antivirus aggiornato. b) Non aprire mai email da sconosciuti. c) Il backup regolare dei dati in un luogo separato.
5. Tra queste due password, quale è più sicura? a) K9#mP_2\$ (8 caratteri, complessa). b) Estate24-Korfù@love1 (20 caratteri, passphrase). c) Sono equivalenti in sicurezza.
6. Cosa verifica il 'qualcosa che HAI' nell'autenticazione a tre fattori? a) La conoscenza di una password. b) La presenza di un oggetto fisico come lo smartphone. c) Le caratteristiche biometriche come l'impronta.
7. Nella regola 3-2-1 del backup, cosa significa l'1? a) Fare il backup una volta alla settimana. b) Tenere una copia dei dati fuori sede, fisicamente separata dal dispositivo originale. c) Usare un solo tipo di supporto per semplicità.
8. Il riconoscimento biometrico è sicuro principalmente perché: a) L'impronta viene salvata crittografata nei server del produttore. b) Il codice matematico non esce mai dal chip del dispositivo. c) Nessun malware può accedere alla fotocamera.

Risposte: 1-b / 2-b / 3-b / 4-c / 5-b / 6-b / 7-b / 8-b

Autovalutazione delle competenze DigComp 2.2

Compila questa scheda prima e dopo il corso. Per ciascuna competenza, indica il tuo livello su una scala da 1 a 5: 1 = non mi sento ancora in grado, 5 = mi sento completamente autonomo.

Area di Competenza	Prima del corso	Dopo il corso
Conosco i rischi principali della navigazione online		
So riconoscere un tentativo di phishing o un sito sospetto		
So scegliere e gestire password sicure		
Ho attivato o so come attivare la 2FA		
Ho un sistema di backup attivo per i miei dati		
So riconoscere i principali tipi di malware		
Capisco la differenza tra Web 1.0, 2.0 e 3.0		

Glossario essenziale

2FA (Autenticazione a due fattori): sistema di sicurezza che richiede due prove di identità per accedere a un account: tipicamente password (fattore ‘conosco’) più un codice inviato allo smartphone (fattore ‘possiedo’).

Antimalware: software che protegge il dispositivo dai programmi malevoli, usando analisi comportamentale per bloccare minacce nuove non ancora conosciute.

App: software ‘monouso’ ottimizzato per dispositivi mobili, progettato per svolgere un singolo compito in modo semplice e intuitivo. Il modello app ha democratizzato l'accesso alla tecnologia digitale.

Backup: copia di sicurezza dei dati in un luogo separato dal dispositivo originale. La regola 3-2-1 prevede 3 copie su 2 supporti diversi di cui 1 fuori sede.

Biometria: sistema di identificazione basato su caratteristiche fisiche uniche – impronta digitale, volto, iride. Nell'autenticazione biometrica, il dispositivo

non salva l'immagine ma un codice matematico irreversibile.

Bug/Vulnerabilità: difetto tecnico in un software che può essere sfruttato da un attaccante per accedere al sistema. Gli aggiornamenti (patch) servono a chiudere questi buchi.

Firewall: sistema che controlla il traffico di rete in entrata e in uscita dal dispositivo, bloccando connessioni non autorizzate.

Keylogger: tipo di malware che registra silenziosamente ogni tasto premuto sulla tastiera, intercettando password, numeri di carta di credito e messaggi privati.

Malware: termine generico per qualsiasi software progettato per danneggiare un sistema o sottrarre informazioni. Include ransomware, trojan, virus, worm, spyware, keylogger, rootkit.

Passphrase: password basata su una frase o sequenza di parole invece che su una stringa di caratteri casuali. Più lunga e memorizzabile, offre maggiore sicurezza grazie alla lunghezza.

Password manager: programma che genera, memorizza e inserisce automaticamente password sicure e diverse per ogni account, eliminando la necessità di ricordarle tutte manualmente.

Patch: aggiornamento software rilasciato per correggere una vulnerabilità o un bug. Il termine viene dall'inglese 'toppa'.

Ransomware: malware che cifra tutti i file del dispositivo rendendoli inaccessibili, chiedendo un riscatto in criptovalute per fornire la chiave di decifrazione.

Rootkit: malware avanzato che si nasconde nel nucleo del sistema operativo, spesso in grado di disattivare l'antivirus. Richiede generalmente la reinstallazione completa del sistema per essere eliminato.

Secure Enclave / TrustZone: chip speciale all'interno dei dispositivi mobili che conserva i dati biometrici in modo completamente isolato dal resto del sistema. Il codice biometrico non esce mai da questo chip.

Trojan: malware che si maschera da programma utile o innocuo. Deve essere installato volontariamente dall'utente per funzionare, dopodiché apre una porta di accesso agli attaccanti.

Web 1.0 / 2.0 / 3.0: le tre fasi evolutive del World Wide Web. Dal web solo lettura (1.0) al web partecipativo con contenuti generati dagli utenti (2.0) all'internet del valore con dati e proprietà digitale gestiti dagli utenti stessi (3.0).

Worm: malware che si clona e si diffonde autonomamente di rete in rete, senza bisogno di essere scaricato o aperto dall'utente.

TEMA B
SICUREZZA E USO CONSAPEVOLE
DEI SERVIZI DIGITALI
 TRAPPOLE DIGITALI E TRUFFE ONLINE



Digita Facile
Campania

A chi è rivolto questo capitolo

Questo capitolo accompagna il percorso formativo dedicato alle Trappole Digitali e alle Truffe Online, sviluppato nell'ambito del progetto Digita Facile Campania, Tema B – Sicurezza e Uso Consapevole dei Servizi Digitali. Si rivolge a chiunque usi internet nella vita quotidiana per fare acquisti, gestire il conto corrente, comunicare con amici e istituzioni e vuole imparare a riconoscere e a evitare le insidie digitali più diffuse.

Il percorso è organizzato in due grandi blocchi tematici. Il primo, Navigare in Piena Consapevolezza e Sicurezza, esplora i meccanismi invisibili che accompagnano la navigazione quotidiana: i cookie e le loro implicazioni sulla privacy, le tracce visibili che lasciamo nel browser, la navigazione in incognito e i suoi limiti reali, la VPN come strumento di protezione avanzata, e le tecniche per verificare l'autenticità di siti e notizie. Il secondo, Truffe e Trappole in Ambiente Digitale, smonta le principali tecniche di manipolazione psicologica usate dai cybercriminali e descrive in dettaglio gli scenari di truffa più diffusi, da quelli più semplici ai più sofisticati, ognuno con la strategia di difesa specifica.

Questo capitolo è costruito attorno a un principio fondamentale: la migliore difesa non è tecnica, è culturale. Chi conosce le trappole difficilmente ci cade. Chi sa come funziona il phishing non clicca il link. Chi riconosce il social engineering si ferma prima di agire. La conoscenza è lo strumento più potente che abbiamo contro la cybercriminalità e questa dispensa è pensata per renderla accessibile a tutti, indipendentemente dal livello di competenza digitale di partenza.

Il messaggio centrale di questo percorso è che le truffe digitali sfruttano sempre le stesse tre leve emotive: paura, urgenza e avidità. Ogni volta che un messaggio online ti fa sentire una di queste emozioni in modo intenso e improvviso, fermati un momento per verificare meglio.

Navigare lascia tracce: cosa succede davvero online

Truffe online: fenomeno in crescita

I soldi fisici stanno scomparendo. I nostri risparmi, la pensione, lo stipendio sono solo “numeri” su un server bancario accessibile via app. Ma non solo. Anche la nostra identità è sempre più “digitale” con SPID e CIE che permettono l'accesso ai servizi della Pubblica Amministrazione.

Tutto questo rende i nostri dati “il nuovo oro”. Lo sono per le Agenzie di Marketing, che studiano sistemi sempre più sofisticati per venire incontro agli

interessi degli utenti e aumentare la conversione in acquisti. Lo sono per i Cybercriminali, il cui obiettivo è trovare un modo per derubarci.

Nel 2024 le truffe digitali — soprattutto legate a pagamenti elettronici — hanno colpito circa 2,9 milioni di italiani, con un danno economico stimato in 880 milioni di euro. In Campania, nel 2024-2025, sono stati sequestrati oltre 2.000 SIM card utilizzate per frodi digitali, e risultano 23 indagati per phishing e furto di dati personali.

Alla base di questo fenomeno, ci siamo noi e il nostro comportamento. Utilizzare consapevolmente la tecnologia digitale e navigare sul web sapendo individuare le trappole digitali, resta la prima arma contro le truffe.

I nostri dati sono il “nuovo oro”

Nel 2024 è emerso che la società americana Cox Media Group aveva dichiarato ai propri clienti di offrire una tecnologia chiamata Active Listening, basata sull'analisi dei dati vocali degli utenti attraverso i microfoni dei dispositivi smart. L'episodio, pur smentito da Meta e Google che hanno rimosso CMG dai loro programmi pubblicitari, dimostra che la prudenza nella gestione dei permessi delle app non è paranoia, ma buon senso.

Quante volte accettiamo i cookie senza valutarne i termini? Quante volte scarichiamo un'app e concediamo autorizzazioni sensibili come l'accesso al microfono e alla geolocalizzazione nostro smartphone? Stiamo rivelando informazioni preziose su di noi, che oggi possono migliorare l'offerta pubblicitaria, ma domani?

Il Regolamento Generale sulla Protezione dei Dati, entrato in vigore nel 2018 per sostituire le vecchie leggi sulla privacy degli anni Novanta, ha cercato di restituire ai cittadini europei il pieno controllo sulle proprie informazioni digitali, imponendo a tutte le aziende, compresi i giganti del web extra-europei, di raccogliere i dati in modo trasparente e solo dopo aver ottenuto un consenso esplicito. Il ruolo del Garante è quello di far applicare concretamente il regolamento europeo in Italia, operando come un vero e proprio “arbitro” che vigila sul comportamento di aziende e pubbliche amministrazioni.

Ma la protezione dei dati personali e dei nostri conti passa inevitabilmente dal nostro comportamento.

COOKIE, TRACCE E PRIVACY NELLA NAVIGAZIONE

Obiettivi

Al termine di questa sezione saprai cosa sono i cookie e come gestirli in modo consapevole. Comprenderai la differenza tra tracce visibili e invisibili lasciate durante la navigazione. Conoscerai i limiti reali della navigazione in incognito e il funzionamento di una VPN.

Le tracce invisibili: i cookie. Biscotti dolci o amari?

Il cookie informatico (dal termine inglese che significa letteralmente “biscotto”) è un piccolo file di testo che un sito web salva nel browser dell'utente durante una visita, per recuperare quelle informazioni nelle visite successive. La Treccani lo definisce con precisione: ‘file di testo di ridotte dimensioni che un sito web invia al browser dell'utente, dove vengono memorizzati per essere poi ritrasmessi allo stesso sito alla visita successiva.’

Non tutti i cookie sono uguali. Esistono tre categorie principali con finalità molto diverse tra loro, e capire la differenza è fondamentale per fare scelte consapevoli quando compare il banner del consenso.

Cookie tecnici: sono essenziali per il funzionamento del sito e non possono essere rifiutati senza compromettere l'esperienza. Sono quelli che ricordano cosa hai messo nel carrello di un e-commerce, che mantengono attiva la tua sessione di accesso dopo il login, che salvano le preferenze di lingua o di visualizzazione. Senza questi cookie, i siti moderni semplicemente non funzionerebbero. Non c'è nessun motivo valido per bloccarli.

Cookie analitici e statistici: misurano il comportamento degli utenti sul sito, come quante persone lo visitano, da dove arrivano, quali pagine guardano di più, per quanto tempo rimangono, con l'obiettivo di migliorare il servizio offerto. Possono essere completamente anonimi o pseudo-anonimi. Sono generalmente meno invasivi dei cookie di profilazione, ma contribuiscono comunque alla raccolta di dati comportamentali.

Cookie di profilazione e marketing: sono i più controversi e i più impattanti sulla privacy. Tracciano il comportamento dell'utente non solo su un singolo sito, ma attraverso decine o centinaia di siti diversi, grazie ai cosiddetti cookie di terze parti, installati da domini diversi da quello che si sta visitando, costruendo nel tempo un profilo dettagliatissimo degli interessi, delle abitudini di consumo e dei comportamenti di ciascuna persona. Questo profilo viene venduto a reti pubblicitarie che lo usano per inviare pubblicità altamente personalizzata. Sono questi che permettono al sito di scarpe di ‘seguirti’ con le sue pubblicità su altri siti dopo che hai chiuso la pagina.

Quando appare il banner del consenso ai cookie, hai sostanzialmente tre opzioni. Accettare tutto è come lasciare la porta di casa spalancata: comodo, ma massimizza la raccolta di dati su di te. Rifiutare tutto è come murare la porta: protegge la privacy ma può compromettere la funzionalità di alcuni siti. La scelta più equilibrata e consigliata è bloccare i cookie di terze parti: mantieni i cookie tecnici che servono al funzionamento dei siti e rinunci soltanto alla profilazione pubblicitaria inter-sito.

Come fare: Su Chrome: Impostazioni → Privacy e sicurezza → Cookie di terze parti → Blocca cookie di terze parti in modalità Incognito (o sempre per più protezione). Su Firefox: Preferenze → Privacy e sicurezza → Protezione antitracciamento avanzata. Su Safari è già attiva per default la protezione contro il tracciamento inter-sito.

Le tracce invisibili: il Fingerprinting. Come un'impronta

Mentre i cookie funzionano come un 'post-it' o una targhetta che un sito web attacca fisicamente sul vostro computer per riconoscervi quando tornate, il fingerprinting non ha bisogno di installare assolutamente nulla. Funziona in modo passivo: il sito web interroga il vostro browser e raccoglie un mix di dettagli tecnici. Qual è il vostro sistema operativo? Che risoluzione ha il vostro schermo? Quali font avete installato? Che fuso orario usate? Che scheda grafica avete? Prese singolarmente, queste informazioni sono innocue. Ma combinate insieme, creano un'impronta digitale praticamente unica. La differenza sostanziale con i cookie è tutta qui: i cookie li potete cancellare o bloccare perché sono file salvati sul vostro dispositivo. Il fingerprinting, invece, vi riconosce semplicemente 'guardando' come è fatto il vostro dispositivo.

La soluzione in questo caso è più complessa. Se si accede da PC, è utile scaricare estensioni del browser che lo aiutino a bloccare il tracciamento. A meno che non si utilizza un browser molto restrittivo come Brave, che è un'ottima soluzione anche per navigazione da Smartphone. Laddove, se si esce dall'app del browser, l'unica soluzione è usare app terze che bloccano il tracciamento e la pubblicità sulle singole app in uso.

Per passare ad un Livello Hard di protezione della privacy su PC e Smartphone, puoi scaricare la dispensa relativa inquadrando il QR code in calce al Modulo 1.

Le tracce visibili: cronologia e storico delle ricerche

Accanto ai cookie e al fingerprinting (tracce salvate prevalentemente sui server) il browser registra anche tracce locali nel dispositivo stesso, visibili a chiunque abbia accesso fisico al computer o allo smartphone.

La cronologia è l'elenco completo di tutti i siti visitati, organizzato per data

e ora. È uno strumento genuinamente utile, dato che permette di ritrovare rapidamente un sito visto giorni fa senza ricordarne l'indirizzo esatto, ma è anche una mappa dettagliata delle tue attività online: i tuoi interessi, le tue preoccupazioni di salute, i tuoi acquisti, le persone che hai cercato, le notizie che hai seguito. Chiunque abbia accesso fisico al tuo dispositivo e sappia come aprire la cronologia del browser può leggere questa mappa. Il classico esempio del regalo di Natale scoperto perché si condivide lo stesso PC in famiglia.

Lo storico delle ricerche mantiene traccia di tutte le parole chiave inserite nel motore di ricerca, mentre la barra degli indirizzi URL memorizza gli indirizzi digitati manualmente. Entrambi sono visibili a chiunque usi lo stesso dispositivo e, in molti casi, alle piattaforme dei motori di ricerca che li usano per personalizzare i risultati futuri. Cancellare periodicamente cronologia, storico e cache del browser, attraverso le Impostazioni → Cancella dati di navigazione in tutti i principali browser, è una buona abitudine di igiene digitale che vale la pena sviluppare.

La navigazione in incognito: un mantello parziale

La navigazione in incognito, chiamata anche navigazione privata o anonima a seconda del browser è probabilmente lo strumento di privacy più frainteso nell'uso quotidiano di internet. L'icona dell'omino con cappello e occhiali scuri ha contribuito a creare l'impressione che attivando questa modalità si diventi totalmente invisibili online. Non è così.

Ecco cosa fa concretamente la navigazione in incognito: al termine della sessione, non lascia tracce locali sul dispositivo. Non salva la cronologia delle pagine visitate. Non memorizza i cookie dopo la chiusura della finestra. Non salva le informazioni inserite nei moduli e nelle ricerche per la compilazione automatica futura. In sostanza: dopo aver chiuso la finestra in incognito, il dispositivo che stai usando non conserva nessuna traccia di quella sessione.

Ma ecco cosa la navigazione in incognito non fa, e qui sta il principale malinteso: **non nasconde la tua attività al tuo fornitore di connessione internet**, di fatti TIM, Vodafone, Fastweb, WindTre e tutti gli altri continuano a vedere i siti che visiti. Non nasconde la tua attività ai siti web che visiti, che continuano a registrare il tuo indirizzo IP e il tuo comportamento. Non ti protegge da chi monitora la rete, incluso il datore di lavoro se usi la rete aziendale, o un potenziale hacker su una rete Wi-Fi pubblica. Non è un sistema di anonimizzazione: è un sistema di pulizia locale.

Le due situazioni in cui la navigazione in incognito è genuinamente utile sono: quando si usa un computer che non è il proprio, ad esempio in hotel, in biblioteca; a casa di amici, per non lasciare account aperti o informazioni personali salvate; e quando si condivide un dispositivo con qualcuno e si vuole mantenere riservata una sessione specifica.

La navigazione in incognito NON ti rende anonimo su internet. Ti rende invisibile soltanto sul dispositivo che stai usando in quel momento. Il tuo fornitore di internet, i siti che visiti e chiunque monitori la rete continuano a vedere ogni tua mossa.

La VPN: il vero scudo della navigazione

La VPN – Virtual Private Network, Rete Privata Virtuale – è lo strumento che offre una protezione della privacy molto più sostanziale rispetto alla sola navigazione in incognito. La definizione tecnica è precisa: è una tecnologia che crea un tunnel di comunicazione cifrato tra il dispositivo dell'utente e un server remoto, attraverso cui passa tutto il traffico internet. Dall'esterno, chiunque monitori la rete vede soltanto che c'è una connessione cifrata verso il server VPN, ma non vede cosa contiene quella connessione né dove è diretta in definitiva.

Le quattro caratteristiche principali di una VPN nella vita quotidiana. La crittografia dei dati trasforma le informazioni trasmesse in un codice illeggibile per chiunque le intercetti: come inviare una lettera in una cassaforte blindata invece che su una cartolina aperta. Il mascheramento dell'indirizzo IP sostituisce il tuo indirizzo di rete reale con quello del server VPN: i siti che visiti vedono la posizione del server, non la tua. **L'aggiramento di restrizioni geografiche** consente di navigare come se si fosse in un paese diverso. **La protezione sulle reti pubbliche** è forse l'uso più importante nella vita quotidiana: usare una VPN su un Wi-Fi pubblico (al bar, in aeroporto, in hotel) rende i propri dati illeggibili per chiunque stia monitorando quella rete.

Esistono VPN gratuite e a pagamento. Le VPN a pagamento di fornitori affidabili (NordVPN, ExpressVPN, ProtonVPN) offrono garanzie di privacy più robuste e connessioni più stabili. Le VPN gratuite vanno usate con cautela: alcune finanziano il servizio gratuito raccogliendo e vendendo i dati degli utenti, che è esattamente il contrario di quello che si vuole ottenere usando una VPN.

E il Fingerprinting? La cosa più critica è che funziona anche se navighi in incognito o usi una VPN perché le caratteristiche della VPN non nascondono le caratteristiche del dispositivo. Puoi difenderti usando alcune strategie principali: usare un browser anti-tracciamento (La soluzione migliore) o bloccare gli script alla radice (usando estensioni Ad Blocker e antitracciamento). Puoi valutare i principali strumenti per Browser PC e Smartphone che difendono la nostra privacy inquadrando il QR code e scaricando la dispensa.



PERMESSI DELLE APP

Active Listening: gli smartphone ci ascoltano?

Nel 2024 CMG afferma di poter offrire ai clienti una tecnologia chiamata Active Listening (ascolto attivo) «una tecnologia pubblicitaria innovativa basata sull'analisi dei dati vocali e comportamentali degli utenti. Questa tecnologia sfrutta i microfoni dei dispositivi smart per raccogliere dati sulle conversazioni in tempo reale». Salvo poi ritrattare.

In molti, tuttavia, sono pronti a giurare di aver ricevuto un messaggio pubblicitario strettamente legato alla conversazione appena avuta. Sebbene la tecnologia esista (come ha tentato di vendere l'agenzia Cox Media), l'ascolto segreto a scopo di marketing è di fatto illegale. Le tutele del GDPR e la vigilanza del Garante (GPDP) sono così stringenti che le grandi multinazionali tecnologiche rifiutano categoricamente queste pratiche per non incorrere in sanzioni milionarie.

Se non ci ascoltano, come fanno a indovinare i nostri desideri? La risposta è nell'incrocio massiccio di dati. Gli algoritmi uniscono il nostro ID pubblicitario, la cronologia web, l'uso delle carte fedeltà e persino le posizioni GPS (per capire chi frequentiamo fisicamente), deducendo i nostri interessi con una precisione che sembra, a torto, telepatica.

L'unico vero rischio di essere “ascoltati” dal telefono non viene dal marketing, ma dal cybercrimine o dallo spionaggio tramite trojan. Scaricare app di dubbia provenienza o concedere autorizzazioni alla cieca espone al rischio di installare software malevoli capaci di attivare fraudolentemente il microfono a nostra insaputa.

I permessi delle app: come comportarsi

Le app che installiamo sullo smartphone chiedono spesso permessi di accesso a funzionalità del dispositivo: microfono, fotocamera, geolocalizzazione, galleria foto, contatti, messaggi SMS. Questi permessi sono a volte legittimamente necessari per le funzioni dell'app, ma spesso vengono richiesti senza una vera utilità funzionale, oppure con finalità non dichiarate di raccolta dati.

Il **principio del privilegio** minimo suggerisce di concedere a ogni app soltanto e unicamente i permessi che hanno un'effettiva e chiara funzionalità per le funzioni che si intende usare. Un'app torcia non ha alcuna ragione legittima per accedere ai contatti o alla posizione. Un'app di gioco non ha bisogno del microfono. Un'app meteo non ha bisogno della fotocamera. Quando un'app richiede permessi che non corrispondono alle sue funzioni dichiarate, è un segnale di allarme: quella richiesta serve probabilmente a raccogliere dati per scopi non dichiarati.

Le **autorizzazioni più sensibili** da monitorare con attenzione sono cinque: il microfono e la fotocamera, perché permettono la raccolta di contenuti audio e visivi dall'ambiente in cui ci si trova; la geolocalizzazione, perché costruisce nel tempo una mappa precisa dei luoghi frequentati; la galleria foto, che contiene spesso informazioni personali molto dettagliate, come luoghi, persone, documenti fotografati; i contatti, che rivelano l'intera rete sociale della persona; i messaggi SMS, permesso particolarmente critico perché intercettando gli SMS si possono rubare i codici OTP della banca.

Per ognuna di queste autorizzazioni, i sistemi operativi moderni offrono tre livelli di accesso: nessun accesso, accesso sempre (anche quando l'app è chiusa) e accesso solo mentre l'app è in uso. La scelta equilibrata e raccomandata è quasi sempre 'solo mentre l'app è in uso: permette all'app di funzionare quando si sta usando attivamente, ma impedisce la raccolta di dati in background.

Come controllare i permessi: su iPhone, vai in Impostazioni → Privacy e sicurezza, dove puoi vedere quali app hanno accesso a ogni tipo di risorsa. Su Android, vai in Impostazioni → App → Gestione permessi. Controlla regolarmente ogni tre o sei mesi e revoca i permessi che non ricordi di aver concesso o che non ti sembrano giustificati.

Le app che installiamo sullo smartphone chiedono spesso permessi di accesso a funzionalità del dispositivo: microfono, fotocamera, geolocalizzazione, galleria foto, contatti, messaggi SMS. Questi permessi sono a volte legittimamente necessari per le funzioni dell'app, ma spesso vengono richiesti senza una vera utilità funzionale, oppure con finalità non dichiarate di raccolta dati.

ID Pubblicitario: il Santo Graal del marketing

Il Browser web sta ai Cookie esattamente come il Sistema Operativo dello smartphone (iOS o Android) sta all'ID Pubblicitario. Se i Cookie di terze parti ti seguono mentre salti da un sito all'altro (es. da un e-commerce a Facebook via web), l'ID Pubblicitario ti segue mentre salti da un'app all'altra (es. dall'app del negozio all'app di Instagram). Mentre nel browser i siti installano tanti piccoli cookie diversi (tanti file di testo fisici), nello smartphone l'ID pubblicitario è uno solo. **È un unico "codice a barre" centralizzato** e di sistema fornito direttamente da Apple o Google. Questo lo rende, di fatto, ancora più potente e ordinato di un normale cookie, perché tutte le app leggono esattamente la stessa etichetta universale senza dover installare nulla di nuovo sul tuo telefono.

Come funziona: l'ID pubblicitario è una semplice stringa alfanumerica invisibile (ad esempio: 1A2B3C4D-5678-90EF...) assegnata dal sistema operativo al tuo dispositivo. Questo codice è condiviso tra tutte le app. Se apri l'app di un negozio di abbigliamento, l'app legge il tuo ID e lo invia a una rete pubblicitaria

dicendo: “L’utente 1A2B3C sta guardando giacche a vento”. Quando poi apri un giochino gratuito, il giochino invia lo stesso ID alla rete pubblicitaria per chiedere quale banner mostrare. La rete riconosce l’ID e ti compare la pubblicità della giacca a vento.

Le implicazioni sono le stesse dei cookie: quanta privacy siamo disposti a cedere in cambio della gratuità dei contenuti e dei servizi offerti?

Come disattivare l’ID pubblicitario: su iPhone, basta andare su Impostazioni > Privacy e sicurezza > Tracciamento. In cima alla schermata c’è un interruttore generale chiamato “Richiesta tracciamento attività”. Su Android, vai in Impostazioni > Google > Annunci dove troverai: “Elimina ID pubblicitario”.

SOCIAL ENGINEERING: LA PSICOLOGIA DELLA TRUFFA

Cos'è il social engineering

La maggior parte delle truffe digitali non richiede competenze informatiche sofisticate. Non sfrutta vulnerabilità tecniche nei sistemi (buchi nei software, debolezze nei protocolli di rete) ma vulnerabilità umane: la paura, la fretta, la curiosità, la fiducia, il desiderio di un guadagno facile. Questo approccio si chiama social engineering, ossia ingegneria sociale, ed è definito dalla Trecani come il complesso di strategie e metodi di manipolazione psicologica e di persuasione volto a indurre un utente a rivelare informazioni riservate. Il social engineering è così efficace e così diffuso perché aggira completamente i sistemi tecnologici di sicurezza. Non serve bucare un firewall sofisticato se puoi convincere l'utente a consegnare volontariamente le sue credenziali. Non serve installare un malware complesso se puoi convincere qualcuno a chiamare un numero falso e fornire i dati bancari di persona. La tecnologia è la scena del crimine, ma il crimine vero è psicologico. E la psicologia umana ha vulnerabilità che nessun aggiornamento software può correggere.

I tre grimaldelli emotivi

Ogni truffa digitale efficace sfrutta almeno uno di tre meccanismi emotivi fondamentali. Riconoscerli è la difesa più potente che esiste, più di qualsiasi software o protezione tecnica.

La paura: messaggi che creano un allarme immediato e paralizzante. “Il tuo conto è stato bloccato per attività sospette!”, “È stato rilevato un virus nel tuo computer!”, “La Polizia Postale ha aperto un'indagine a tuo nome!”. La paura attiva la risposta di emergenza del sistema nervoso autonomo: il ragionamento critico rallenta o si spegne del tutto, e il corpo spinge ad agire immediatamente per eliminare la minaccia. Chi si trova in questo stato emotivo non rallenta per verificare, non chiama il numero ufficiale, non legge i dettagli con attenzione: clicca subito, chiama subito, paga subito.

L'urgenza: messaggi che creano una pressione temporale artificiale. “Hai solo 24 ore per rispondere prima che il conto venga chiuso!”, “L'offerta scade tra 10 minuti!”, “Conferma ora o perdi definitivamente l'accesso!”. L'urgenza ha un effetto preciso e documentato sul processo decisionale: elimina il tempo necessario per riflettere e verificare. Chi è di fretta prende scorciatoie cognitive si affida alle apparenze, non controlla i dettagli, si fida della fonte apparente senza verificarla.

L'avidità e la curiosità: messaggi che promettono ricompense improbabili o stuzzicano una curiosità intensa. “Hai vinto un iPhone 15!”, “C'è un rimborso fiscale di 847€ in attesa di riscossione!”, “Guarda la foto scandalosa di [nome

famoso]!”. L'eccitazione generata da una promessa di guadagno inaspettato, o da una curiosità molto intensa, produce lo stesso effetto degli altri due grimaldelli: il pensiero critico viene bypassed dal desiderio di vedere, di sapere, di ottenere.

La regola d'oro contro il social engineering: se un messaggio ti fa sentire paura, urgenza o eccitazione intensa in modo improvviso, FERMATI. Non fare nulla per almeno cinque minuti. In quasi tutti i casi, la truffa si svela da sola quando si dà al cervello il tempo di tornare a funzionare normalmente.

I tre canali della truffa digitale

I cybercriminali usano tre canali principali per raggiungerti, tutti nominati con varianti del termine 'phishing' (che viene dall'inglese fishing, pescare) perché l'immagine dell'amo che pesca vittime ignare descrive perfettamente la tecnica.

Phishing: l'amo arriva via email. È la forma più antica e ancora la più diffusa e redditizia della truffa digitale. Il truffatore invia un'email che imita graficamente una comunicazione ufficiale della banca, delle Poste, di Amazon, di PayPal, dell'Agenzia delle Entrate, con loghi riprodotti fedelmente, toni formali, firme plausibili, e un link che porta a una pagina che copia quasi perfettamente il sito originale. Lo scopo è sempre lo stesso: far inserire all'utente le proprie credenziali, username e password, su un sito falso che le registra e le invia ai truffatori.

Smishing: l'amo arriva via SMS o WhatsApp. Segue la stessa logica del phishing ma sfrutta la maggiore fiducia che le persone tendono a riporre nei messaggi diretti rispetto alle email. Il messaggio sembra provenire da Poste Italiane, da un corriere, dalla propria banca o da un ufficio governativo. "Il tuo pacco è in giacenza: paga 1,99€ di spese amministrative tramite questo link" è uno degli scenari più frequenti. La sensazione che il messaggio sia personale (è arrivato direttamente sul mio telefono) abbassa la guardia.

Vishing: l'amo arriva a voce, attraverso una telefonata. Qualcuno si finge un operatore del servizio clienti bancario, un tecnico di supporto di Microsoft o Apple, un funzionario dell'Agenzia delle Entrate, un agente della Polizia Postale. La voce umana crea un senso di autenticità molto difficile da ignorare, e la conversazione in tempo reale non dà il tempo fisico di verificare l'identità del chiamante o di consultare qualcuno. È il canale più difficile da cui difendersi perché attiva tutti e tre i grimaldelli contemporaneamente: la paura dell'autorità, l'urgenza della situazione, la pressione della conversazione in corso.

GLI SCENARI DI TRUFFA: RICONOSCERE E DIFENDERSI

Il finto pacco – Smishing

Scenario 1: Il corriere fantasma

Lo scenario: Arriva un SMS: “Il tuo pacco (codice IT849302) è in giacenza presso il nostro deposito. Paga €1,99 di spese di gestione per autorizzare la consegna entro oggi: [link].” Il messaggio sembra autentico, usa un numero di tracking plausibile e crea urgenza con la scadenza giornaliera.

La verità: Non stai aspettando nessun pacco, o se lo aspetti, nessun corriere legittimo chiede pagamenti via SMS su link esterni. Quel link porta a una pagina che imita il sito del corriere e raccoglie i dati della tua carta di credito. I pochi euro chiesti sono un pretesto: i tuoi dati bancari valgono molto di più.

Difesa: Non cliccare il link, mai. Non pagare. Blocca il numero mittente e segnala il messaggio come spam nelle opzioni del messaggio. Se aspetti davvero un pacco, vai direttamente sul sito ufficiale del corriere digitando tu l'indirizzo nel browser, e inserisci manualmente il numero di tracking.

Lo spear phishing – Il phishing personalizzato

Scenario 2: Il messaggio dall'amico o dal capo

Lo scenario: Arriva un'e-mail che sembra provenire da un tuo collega, dal tuo responsabile o da un'istituzione con cui hai effettivamente rapporti. Il messaggio contiene dettagli specifici su di te (il tuo nome completo, la tua azienda, un progetto a cui stai lavorando) che la rendono molto più credibile di un phishing generico.

La verità: Il truffatore ha studiato la vittima in anticipo: ha raccolto informazioni dai profili LinkedIn e Facebook, da violazioni precedenti di database, da ricerche sul nome online. Lo spear phishing è un attacco su misura, molto più difficile da riconoscere rispetto al phishing di massa.

Difesa: Verifica sempre, anche con i tuoi contatti più fidati, se una richiesta insolita è legittima. Usa un canale diverso da quello in cui hai ricevuto la richiesta: se l'e-mail sembra del tuo capo ma contiene una richiesta strana, chiamalo al telefono. Non cliccare mai link in e-mail inaspettate, anche se sembrano provenire da mittenti conosciuti.

La truffa e-commerce – L'affare del secolo

Scenario 3: Il prezzo impossibile

Lo scenario: Una pubblicità su Facebook o Instagram propone: “Bici elettrica ultima generazione a €49 invece di €599! Offerta esclusiva solo per oggi, disponibilità limitata!” Le foto sembrano professionali e i commenti alla pubblicità sono tutti entusiasti.

La verità: Paghi con carta di credito su un sito che sembra professionale e non ricevi nulla, oppure ricevi un pacco con un articolo completamente diverso e di bassissima qualità. In più, hai consegnato i dati della tua carta a un sito criminale che potrebbe usarli per altri acquisti non autorizzati.

Difesa: Prima di acquistare su un sito sconosciuto: cerca le recensioni su Trustpilot e Google Reviews. Cerca su Google il nome del sito seguito dalla parola ‘truffa’. Verifica che esista un indirizzo fisico reale, una partita IVA e un numero di telefono funzionante. I commenti entusiasti sotto una pubblicità di Facebook possono essere falsi o filtrati dall’inserzionista. Se il prezzo sembra troppo bello per essere vero, è quasi certamente una truffa.

Il romance scam – Il principe azzurro digitale

Scenario 4: L'amicizia che diventa emergenza

Lo scenario: Qualcuno di molto affascinante ti chiede l'amicizia sui social o su un'app di incontri. Si presenta come un professionista all'estero: un militare in missione, un medico con una ONG, un ingegnere su una piattaforma petrolifera. Le conversazioni diventano quotidiane, affettuose, quasi romantiche, spesso per settimane o mesi.

La verità: Dopo aver investito molto tempo e molte emozioni nel costruire la relazione, arriva l'imprevisto drammatico: un incidente, un'operazione medica urgente, un blocco burocratico che impedisce il rientro. Ha bisogno di soldi subito. Non chiede tutto in una volta, inizia con cifre piccole e aumenta progressivamente.

Difesa: Non inviare mai denaro a qualcuno che non hai mai incontrato di persona, indipendentemente da quanto la relazione sembri reale. Fai una ricerca inversa per immagini sulla foto del profilo: spesso si scopre che appartiene a un'altra persona, trovata su internet. Se hai dubbi, parla con qualcuno di cui ti fidi prima di agire.

Il tech support scam – Il finto tecnico

Scenario 5: L'allarme a schermo

Lo scenario: Mentre navighi appare improvvisamente un pop-up che occupa l'intero schermo, lampeggia di rosso e riproduce un suono d'allarme: "VIRUS CRITICO RILEVATO! IL TUO COMPUTER È STATO COMPROMESSO. CHIAMA IMMEDIATAMENTE IL SUPPORTO MICROSOFT AL NUMERO 0800-xxx-xxx PER EVITARE LA PERDITA DI TUTTI I TUOI DATI!"

La verità: Non c'è nessun virus. È una normale pagina web progettata per sembrare un allarme di sistema – sfrutta l'HTML per bloccare la schermata e JavaScript per i suoni. Il "tecnico" che risponde chiederà di installare un programma di accesso remoto per 'pulire il computer': in realtà sta prendendo il controllo del dispositivo per rubare dati, installare malware o estorcere denaro.

Difesa: Non chiamare il numero. Non installare nessun programma. Chiudi il browser con la tastiera – Ctrl+W o Cmd+W – o spegni il PC forzatamente se lo schermo è completamente bloccato. Quando riapri, tutto sarà sparito. Microsoft, Apple e Google non contattano mai proattivamente gli utenti con avvisi di questo tipo.

Il phishing bancario – La banca in panico

Scenario 6: L'email urgente della banca

Lo scenario: Arriva un'e-mail con il logo ufficiale della tua banca, la grafica perfetta, il tono formale: "Abbiamo rilevato un accesso sospetto al tuo conto corrente dall'indirizzo IP 185.xxx.xxx. Per sicurezza, il tuo account è stato temporaneamente limitato. Clicchi qui entro 24 ore per verificare la tua identità e ripristinare l'accesso, altrimenti il conto verrà bloccato permanentemente."

La verità: LA BANCA NON TI CHIEDE MAI DATI SENSIBILI VIA EMAIL O SMS. Questa è la regola assoluta del settore bancario, senza eccezioni. Il link porta a un sito che imita perfettamente il portale della tua banca, ma i dati inseriti (username, password, codice dispositivo) vengono catturati dai truffatori che li useranno immediatamente.

Difesa: Non cliccare mai il link. Non inserire credenziali su pagine raggiunte tramite link ricevuti. Se hai un dubbio reale sulla sicurezza del tuo conto, chiama il numero verde della banca che trovi sul retro della tua carta di credito, oppure accedi all'app bancaria ufficiale. Segnala l'e-mail come phishing al tuo provider e-mail.

Il man in the middle – L'intercettazione sul Wi-Fi

Scenario 7: Il bonifico intercettato

Lo scenario: Sei seduto in un bar. Usi il Wi-Fi gratuito per accedere all'app della tua banca e fare un bonifico. L'operazione sembra andare a buon fine, vedi la schermata di conferma. Qualche ora dopo scopri che i soldi sono arrivati su un conto completamente diverso da quello che avevi indicato.

La verità: Su una rete Wi-Fi pubblica non protetta, un attaccante tecnicamente preparato può posizionarsi tra te e il server della banca. Intercettando la comunicazione, può modificare in tempo reale le coordinate bancarie del destinatario prima che raggiungano il server, oppure continuare a usare la tua sessione bancaria dopo che hai completato l'operazione senza fare logout.

Difesa: Per qualsiasi operazione bancaria o finanziaria usa sempre la tua connessione dati mobile non il Wi-Fi pubblico. Se sei costretto a usare un Wi-Fi non fidato, attiva una VPN prima di aprire l'app bancaria. Fai sempre logout esplicito dall'app bancaria dopo ogni uso, specialmente su reti pubbliche.

I trojan bancari – Le spie in tasca

Scenario 8: L'app innocua che non lo è

Lo scenario: Scarichi un'app che sembra del tutto innocua: una torcia potente, un gioco gratuito di successo, un'utilità per "pulire la memoria del telefono e velocizzarlo". L'app funziona, sembra legittima. Qualche settimana dopo la tua banca ti contatta: qualcuno ha effettuato operazioni non autorizzate dal tuo conto.

La verità: Quella app conteneva un trojan bancario. Questo tipo di malware usa due tecniche sofisticate. L'overlay: quando apri l'app ufficiale della tua banca, il trojan sovrappone una finestra trasparente identica allo schermo della banca. Tu vedi la tua banca, digiti le credenziali, ma stai digitando su una replica gestita dal malware. Il furto dell'OTP: alcuni trojan chiedono il permesso di "leggere gli SMS" e lo usano per intercettare i codici di conferma che la banca ti manda, permettendo di completare operazioni non autorizzate.

Difesa: Scarica le app solo dagli store ufficiali, App Store di Apple o Google Play Store. Prima di installare, controlla i permessi che l'app richiede: un'app torcia che chiede di leggere gli SMS o accedere ai contatti è quasi certamente malevola. Non concedere il permesso di 'Leggere gli SMS' a nessuna app tranne quella della tua banca ufficiale.

1. Cosa osservare in un sito E-commerce

Prima di inserire i dati della tua carta, analizza questi elementi fondamentali:

Protocollo HTTPS: Verifica sempre che l'indirizzo inizi con <https://> e che sia presente l'icona del lucchetto nella barra del browser, a indicare una connessione crittografata.

Dati Societari: Un sito serio deve esporre chiaramente nel “footer” (la parte bassa della pagina) la Partita IVA, la sede legale e i contatti (e-mail o telefono).

Politiche Legali: Controlla la presenza delle pagine relative alla Privacy Policy e, soprattutto, alle Condizioni di Reso e Rimborso. Se mancano, è un segnale di allarme.

Prezzi Irreali: Diffida di sconti eccessivi (es. un iPhone nuovo a 200€). Se l'offerta è troppo bella per essere vera, probabilmente è una truffa.

Segnali di Phishing: Presta attenzione a elementi grafici insoliti, come punti esclamativi gialli o avvisi che creano urgenza ingiustificata.

Gestione Cookie: Anche se comuni, popup di “GESTIONE DEI COOKIE” eccessivamente invasivi o con grafiche cartoonesche (come biscotti con braccia e gambe) in siti non familiari possono essere usati per mascherare script malevoli.

2. Strumenti esterni per valutare l'affidabilità

Non fidarti solo di ciò che vedi sul sito; usa queste “terze parti”:

Trustpilot / Sitejabber: Cerca il nome del negozio su queste piattaforme per leggere le recensioni degli altri utenti. Attenzione alle recensioni troppo simili tra loro o scritte in un italiano stentato.

ScamAdviser: Inserisci l'URL del sito per ottenere un punteggio di affidabilità basato su algoritmi che analizzano l'età del dominio e la sua collocazione geografica.

Verifica Partita IVA: Puoi usare il sito dell'Agenzia delle Entrate per verificare se la Partita IVA indicata sul sito esiste ed è attiva.

3. Come smascherare truffe dei rivenditori sui Marketplace

Sulle piattaforme di compravendita tra privati, il rischio è maggiore. Ecco come difenderti:

Analisi delle Foto: Diffida di foto generiche prese dal web o da cataloghi. Chiedi sempre al venditore delle foto reali del prodotto, magari con un foglietto accanto con scritta la data odierna.

Comunicazione Esterna: Se un venditore ti chiede di spostare la conversazione fuori dalla piattaforma (es. su WhatsApp o Telegram), rifiuta sempre. Le chat ufficiali ti proteggono legalmente.

Metodi di Pagamento: Mai accettare pagamenti tramite ricarica Postepay, bonifici istantanei o “Invio di denaro ad amici” su PayPal. Questi metodi non sono rimborsabili.

Urgenza e Pressione: I truffatori spesso usano un linguaggio allarmante (“Azione richiesta”, “L'offerta scade tra un'ora”) per non farti riflettere.

Errori e Link: Fai attenzione a messaggi con errori grammaticali o ortografici e non cliccare mai su link sospetti che sembrano portare a pagine di login della piattaforma.

Buone pratiche per scongiurare una Truffa

Proteggere i propri dispositivi:

1. Attiva l'Autenticazione a Due Fattori (2FA): Fallo su tutti gli account (e-mail, social, banca). Questo impedisce agli hacker di accedere anche se conoscono la tua password.

2. Usa Password Forti e Diverse: Non utilizzare la stessa password per più servizi. Utilizza un Password Manager per generare e conservare password complesse.

3. Aggiorna il Software: Mantieni sempre aggiornati il sistema operativo, il browser e l'antivirus. Gli aggiornamenti contengono patch di sicurezza contro le vulnerabilità note.

4. Permessi alle App: Perché una App “Torcia” vuole leggere i tuoi SMS? Perché un “Solitario” vuole accedere ai contatti? Se un'app chiede permessi strani, NON installarla.

Setup pratico per l'autenticazione a 2 fattori sulle principali piattaforme.

Google/Gmail Account Google -> Sicurezza -> Verifica in due passaggi.

Facebook / Meta: Impostazioni e Privacy -> Password e Sicurezza -> Autenticazione a due fattori.

Amazon: Il mio account -> Accesso e sicurezza -> Verifica in due fasi.

WhatsApp: Impostazioni -> Account -> Verifica in due passaggi (Qui è un PIN che protegge il numero).

App Bancarie: Entrare nelle impostazioni dell'app e cercare la voce Sicurezza, Privacy e Account

Comandamenti della Banca online

1. L'App Ufficiale è il Porto Sicuro: Non entrate nel conto dal browser (Chrome/Safari) del telefono cercando "Banca X" su Google (potreste finire su un sito clone). Usate solo l'App ufficiale scaricata dallo Store.

2. Monitora gli Estratti Conto Controlla regolarmente le transazioni bancarie. Segnala immediatamente alla banca qualsiasi operazione non autorizzata.

3. Effettua sempre il Logout: quando finisci di usare l'app, entra nelle opzioni ed effettua il logout.

4. Notifiche Push attive: Sarai sempre avvisato in tempo delle operazioni effettuate dal tuo conto; se non hai autorizzato l'operazione, la Notifica ti permette di saperlo in anteprima e bloccare il conto.

5. Fuori casa, usa i TUOI dati: Se devi controllare il conto fuori casa, spegni il Wi-Fi e usa la tua connessione 4G/5G. È molto più difficile da intercettare. Non c'è campo? Usal la VPN.

6. Link SMS non si clicca: Se la banca ti scrive "Conto bloccato", non cliccare. Apri l'App ufficiale e controlla lì. Se è vero, troverai un avviso dentro l'App

7. Aggiornamenti Tieni aggiornata l'app e il sistema operativo del telefono

Riepilogo dei concetti fondamentali

Questo percorso ha costruito una comprensione operativa completa delle trappole digitali e delle truffe online, muovendo dai meccanismi invisibili della navigazione quotidiana fino alle tecniche di manipolazione psicologica più sofisticate usate dalla cybercriminalità.

La navigazione online lascia tracce continue e spesso invisibili: cookie tecnici, analitici e di profilazione; cronologia e storico delle ricerche nel browser; indirizzo IP registrato da ogni sito visitato. Gestire consapevolmente queste tracce bloccando i cookie di terze parti, cancellando periodicamente la cronologia, usando la navigazione in incognito sui dispositivi non propri, è la base di una vita digitale più rispettosa della propria privacy.

La navigazione in incognito protegge soltanto dalle tracce locali sul dispositivo, non rende anonimi verso il fornitore di internet o i siti visitati. La VPN offre una protezione molto più profonda: cifra tutto il traffico, nasconde l'indirizzo IP e protegge le comunicazioni anche su reti Wi-Fi pubbliche. Verificare l'URL prima di inserire dati sensibili (controllando HTTPS, il lucchetto, il dominio reale) e applicare il principio del privilegio minimo ai permessi delle app sono due delle competenze di sicurezza più importanti e immediatamente applicabili.

Il social engineering è il cuore di quasi tutte le truffe digitali: manipola le emozioni invece di attaccare i sistemi. I tre grimaldelli (paura, urgenza, avidità) si riconoscono dallo stesso schema: un messaggio che provoca una reazione emotiva intensa e chiede un'azione immediata. Fermarsi cinque minuti prima di agire è la difesa più semplice e più efficace. Phishing, smishing e vishing sono i tre canali principali attraverso cui questi grimaldelli vengono consegnati.

Gli otto scenari descritti, dal finto pacco al romance scam, dal phishing bancario al man in the middle e ai trojan bancari, condividono la stessa struttura: una situazione plausibile, una verità nascosta e una strategia di difesa specifica. I quattro comandamenti della banca online (app ufficiale, rete mobile, no ai link via SMS, controllo dei permessi) sono la sintesi pratica applicabile ogni giorno.

La difesa migliore contro le truffe digitali non è tecnica: è culturale. Chi conosce le trappole raramente ci cade. Chi sa come funziona il social engineering si ferma prima di agire. La conoscenza è il migliore antivirus che esiste e non ha bisogno di aggiornamenti.

Test di autovalutazione

Indica la risposta corretta. Le risposte si trovano in fondo alla sezione.

1. Quale tipo di cookie traccia il comportamento dell'utente attraverso molti siti diversi per creare profili pubblicitari? a) Cookie tecnici. b) Cookie analitici. c) Cookie di terze parti e profilazione.
2. La navigazione in incognito nasconde la tua attività: a) Al tuo fornitore di internet. b) Al sito che stai visitando. c) Soltanto alle altre persone che usano lo stesso dispositivo.
3. Qual è la principale differenza tra phishing e spear phishing? a) Il phishing usa l'email, lo spear phishing usa gli SMS. b) Lo spear phishing è personalizzato sulla vittima, il phishing è generico. c) Il phishing è più pericoloso.
4. Quale di questi URL è sicuro per accedere a Facebook? a) <https://facebook-login.com> – b) <http://www.facebook.com> – c) <https://m.facebook.com> – d) <https://faceboook.com>
5. Quale grimaldello emotivo usa il messaggio: 'Il tuo conto sarà bloccato in 24 ore!'? a) Avidità. b) Paura e urgenza. c) Curiosità.
6. Cosa fare quando appare un pop-up che dice "VIRUS RILEVATO! Chiama il supporto al numero..."? a) Chiamare subito il numero. b) Non chiamare, chiudere il browser o spegnere il PC. c) Scaricare il programma di pulizia suggerito.
7. Perché è rischioso fare operazioni bancarie su Wi-Fi pubblico? a) Le reti pubbliche sono lente e le transazioni potrebbero fallire. b) Un attaccante sulla stessa rete potrebbe intercettare o modificare le comunicazioni. c) Le app bancarie bloccano l'accesso da Wi-Fi pubblico.
8. Quale permesso non dovrebbe avere quasi nessuna app, tranne quella bancaria ufficiale? a) L'accesso alla posizione solo mentre l'app è in uso. b) La lettura degli SMS. c) L'accesso alla fotocamera per fare foto.

Risposte: 1-c / 2-c / 3-b / 4-c / 5-b / 6-b / 7-b / 8-b

Autovalutazione delle competenze DigComp 2.2

Compila questa scheda prima e dopo il percorso formativo. Per ciascuna voce, indica il tuo livello su una scala da 1 a 5, dove 1 significa “non mi sento ancora in grado” e 5 significa “mi sento completamente autonomo”.

Area di Competenza	Prima del corso	Dopo il corso
So cosa sono i cookie e come gestirli consapevolmente		
Conosco i limiti reali della navigazione in incognito		
So verificare la sicurezza di un URL prima di inserire dati		
Riconosco i tre grimaldelli emotivi del social engineering		
So distinguere phishing, smishing e vishing		
Conosco i 4 comandamenti della sicurezza bancaria online		
So come comportarmi su reti Wi-Fi pubbliche		
So gestire i permessi delle app secondo il principio del privilegio minimo		
So cosa fare se ricevo un messaggio sospetto dalla mia banca		
So come segnalare una truffa alle autorità competenti		

Glossario essenziale

Clickbaiting: tecnica di manipolazione che usa titoli emotivamente intensi, incompleti o iperbolici per indurre clic su contenuti di scarsa qualità o fuorvianti. Sfrutta curiosità, paura e indignazione come leve.

Cookie: piccolo file di testo salvato nel browser durante una visita a un sito web, usato per ricordare informazioni tra una sessione e l'altra. Esistono in tre categorie principali: tecnici, analitici, di profilazione.

Cookie di terze parti: cookie installati da domini diversi dal sito che si sta visitando, usati da reti pubblicitarie per tracciare il comportamento dell'utente attraverso molti siti diversi e costruire profili commerciali.

HTTPS: protocollo di comunicazione cifrato (la "S" sta per Secure) che garantisce la trasmissione sicura dei dati tra browser e sito. Necessario – ma non sufficiente – per fidarsi di un sito con dati sensibili.

Man in the Middle: attacco informatico in cui un terzo si inserisce tra due comunicanti su una rete non sicura, intercettando o modificando i dati trasmessi. Particolarmente pericoloso sulle reti Wi-Fi pubbliche.

Navigazione in incognito: modalità del browser che non salva cronologia, cookie e dati localmente sul dispositivo. Non garantisce l'anonimato verso ISP, siti visitati o chi monitora la rete.

Phishing: frode digitale via e-mail che imita comunicazioni ufficiali per indurre l'utente a inserire credenziali su siti falsi. Le varianti per canale: smishing (SMS/WhatsApp), vishing (telefono).

Principio del privilegio minimo: regola di sicurezza che suggerisce di concedere a programmi e app solo i permessi strettamente necessari alle loro funzioni dichiarate, revocando tutto il resto.

Romance scam: truffa basata sulla costruzione artificiale di una relazione affettiva online, seguita da richieste di denaro urgenti motivate da emergenze inventate.

Session hijacking: furto di una sessione di navigazione attiva – tipicamente bancaria – da parte di un attaccante che si trova sulla stessa rete e non effettua il logout.

Social engineering: manipolazione psicologica sistematica per indurre le persone a rivelare informazioni riservate o compiere azioni dannose. Bypassa i sistemi tecnici di sicurezza agendo sulle vulnerabilità umane.

Spear phishing: variante personalizzata del phishing in cui l'attaccante ha studiato preventivamente la vittima per rendere il messaggio più credibile e difficile da riconoscere.

Tech support scam: truffa del finto supporto tecnico, realizzata attraverso falsi pop-up d'allarme che inducono la vittima a chiamare un numero e a concedere l'accesso remoto al dispositivo.

Trojan bancario: malware camuffato da app innocua che sovrappone interfacce false alle app bancarie reali per sottrarre credenziali, oppure intercetta gli SMS con i codici OTP.

Typosquatting: tecnica di truffa che registra domini con piccoli errori tipografici rispetto a quelli originali (es. faceboook.com) per ingannare gli utenti distratti.

VPN (Virtual Private Network): tecnologia che crea un tunnel cifrato per tutto il traffico internet, nascondendo l'indirizzo IP reale dell'utente e proteggendo le comunicazioni anche su reti pubbliche.

Contatti utili in caso di truffa

Polizia Postale: commissariatodips.it — sportello online per segnalare reati informatici, truffe online e phishing, attivo 24 ore su 24.

Garante per la Protezione dei Dati Personali: gdpd.it — per segnalare violazioni della privacy e richiedere informazioni sui propri diritti digitali.

AGCM — Antitrust: agcm.it — per segnalare pratiche commerciali scorrette e truffe nell'e-commerce.

CERT-AgID: cert-agid.gov.it — pubblica aggiornamenti in tempo reale sulle campagne di phishing e malware in circolazione in Italia.

Arbitro Bancario Finanziario: arbitrobancariofinanziario.it — per ricorsi in caso di controversie con banche o intermediari finanziari relativi a operazioni non autorizzate.

TEMA B
SICUREZZA E USO CONSAPEVOLE
DEI SERVIZI DIGITALI

 **BRAKE THE FAKE RICONOSCERE FAKE NEWS,**
TRUFFE E INGANNI ONLINE



Digita Facile
Campania

A chi è rivolto questo capitolo

Questo capitolo accompagna il percorso formativo BREAK THE FAKE: Riconoscere Fake News, Truffe e Inganni Online, sviluppato nell'ambito del progetto Digita Facile Campania, Tema B – Sicurezza e Uso Consapevole dei Servizi Digitali. Si rivolge a chiunque legga notizie, navighi sui social network, riceva messaggi in gruppi WhatsApp o si informi attraverso qualsiasi canale digitale – cioè, praticamente, a chiunque abbia uno smartphone o un computer collegato a Internet.

Il percorso si articola in quattro sezioni. L'introduzione 'Welcome to the Fake Jungle' apre il percorso esplorando la complessità dell'ecosistema informativo digitale: la giungla in cui viviamo ogni giorno, fatta di contenuti che si somigliano (notizie, opinioni, pubblicità, manipolazioni) e che scorrono con una velocità che non lascia tempo alla riflessione. Il Modulo 1 'Fake News Anatomy' entra nella struttura di una fake news pezzo per pezzo, smontandone i meccanismi e i meccanismi psicologici che la rendono efficace. Il Modulo 2 'Fake or Real Tools' fornisce strumenti pratici e quotidiani per verificare fonti, date e riscontri. Il Modulo 3 'Clickbait e Manipolazione' affronta le tecniche di persuasione e i dark pattern che ci spingono a cliccare, reagire e condividere senza pensare.

Al centro del percorso c'è Iris Feed: una metafora narrativa dell'algoritmo che seleziona e ordina i contenuti nei feed dei social network. Non mente, non inventa. Seleziona. Accelera. E capire come funziona è il primo passo per riprendere in mano la propria autonomia di giudizio.

Grazie a questa dispensa sarete più autonomi. La capacità di fermarsi un secondo prima di condividere, di fare una domanda in più prima di credere, di applicare tre controlli minimi su una fonte: queste sono le competenze che cambiano la qualità della propria vita informativa.

Welcome to the Fake Jungle: la giungla dell'informazione

Iris Feed e l'ecosistema informativo digitale

Iris Feed non è una persona reale. È una metafora. Rappresenta l'algoritmo che ogni giorno, su ogni piattaforma digitale che usiamo, decide cosa vediamo, in quale ordine lo vediamo e per quanto a lungo. Non urla, non impone, non obbliga. Semplicemente seleziona. E questa apparente normalità, il flusso di contenuti che scorre senza sforzo sullo schermo, è esattamente ciò che la rende così potente.

Iris Feed non cerca la verità. Cerca l'attenzione. E l'emozione trattiene l'attenzione molto più a lungo della verifica. Un contenuto che fa arrabbiare, che spaventa, che sorprende, che indigna: viene visto, cliccato, commentato, condiviso molte più volte di un contenuto accurato ma sobrio. Gli algoritmi imparano da questi comportamenti e amplificano i contenuti che li producono. Non è una cospirazione: è un modello di business. Viviamo in quella che possiamo chiamare una giungla dell'informazione: non tutto è pericoloso, ma non tutto è affidabile. In questa giungla i contenuti si somigliano moltissimo: una notizia può sembrare un'opinione, un'opinione può sembrare una notizia, una pubblicità può sembrare informazione giornalistica. Come in una giungla vera, non si sopravvive correndo a caso: si impara a osservare, a fermarsi, a leggere i segnali.

Dato, informazione, misinformazione, disinformazione

Prima di affrontare le fake news, è utile chiarire alcune distinzioni fondamentali che spesso vengono confuse, rendendo difficile ragionare con precisione su questi temi.

Il dato: è un frammento isolato, un numero, un'immagine, una frase, che non ha ancora un contesto. Un dato grezzo non dice nulla da solo. 'La temperatura è 38°' è un dato e senza contesto (ad es. è la febbre di una persona, la temperatura esterna di una città africana, il calore di un forno) non significa nulla.

L'informazione: è un dato inserito in un contesto verificabile, con una fonte identificabile e una data. L'informazione può essere controllata, confutata, aggiornata. È il risultato di un processo che richiede tempo, fonti multiple e responsabilità editoriale.

La misinformazione: è un'informazione falsa o inesatta condivisa senza intenzione di ingannare. Chi la diffonde crede di dire la verità: ha ricevuto un'informazione errata, non l'ha verificata, e l'ha passata ad altri in buona fede. La misinformazione può essere innocua o molto pericolosa a seconda del contesto — le informazioni false sulla salute, per esempio, possono avere conseguenze gravi anche quando vengono condivise senza cattive intenzioni.

La disinformazione: è un'informazione falsa o manipolata condivisa con l'intenzione deliberata di ingannare. Non è un errore: è una scelta. La disinformazione può avere obiettivi politici, economici, ideologici. È progettata per produrre un effetto specifico, per creare paura, orientare il voto, distruggere una reputazione, vendere un prodotto e usa la forma della notizia per sembrare credibile.

La distinzione tra misinformazione e disinformazione è importante non per

colpevolizzare chi condivide, ma per capire con che tipo di fenomeno ci si sta confrontando. La disinformazione si combatte con la verifica e l'educazione. La disinformazione richiede anche strumenti di individuazione delle origini e delle motivazioni.

Perché le fake news si diffondono: algoritmi, viralità, camere dell'eco

Capire perché le fake news si diffondono così rapidamente richiede di guardare sia alla tecnologia che alla psicologia. I due fattori si combinano e si amplificano reciprocamente.

Dal punto di vista tecnologico, gli algoritmi delle piattaforme social sono ottimizzati per massimizzare il tempo che gli utenti trascorrono sulla piattaforma. Per fare questo, imparano continuamente dalle interazioni (clic, like, commenti, condivisioni, tempo di visione) e propongono contenuti che producono più interazione. I contenuti emotivamente intensi producono più interazione. Quindi i contenuti emotivamente intensi vengono amplificati. Questo non è un effetto collaterale indesiderato: è la logica del sistema.

Dal punto di vista psicologico, i bias cognitivi giocano un ruolo fondamentale. Il bias di conferma porta a credere più facilmente alle informazioni che confermano ciò che già pensiamo, e a ignorare quelle che lo contraddicono. Il bisogno di appartenenza ci porta a condividere contenuti che ci fanno sentire parte di un gruppo, 'anche noi sappiamo la verità'. La paura di restare esclusi (FOMO, Fear of Missing Out) ci spinge a condividere prima di verificare per non perdere il momento in cui 'tutti ne parlano'.

Le camere dell'eco sono ambienti informativi in cui gli utenti sono esposti prevalentemente a contenuti e opinioni simili alle proprie, mentre le voci alternative vengono progressivamente filtrate dall'algoritmo. In una camera dell'eco, una fake news che conferma i valori del gruppo viene amplificata enormemente e incontra pochissima resistenza critica. Uscire dalla propria camera dell'eco, cercando deliberatamente fonti diverse, confrontandosi con punti di vista differenti, è uno degli atti di igiene informativa più importanti.

Le emozioni come punto di partenza

Un elemento ricorre in quasi tutte le fake news efficaci: l'emozione. Il contenuto arriva prima al cuore che alla testa. Paura, rabbia, indignazione, urgenza di condividere: queste emozioni sono il meccanismo di innesco che sospende temporaneamente il pensiero critico.

Questa non è ingenuità. È fisiologia. Quando siamo emotivamente attivati, specialmente da paura o indignazione, il cervello riduce la capacità di analisi critica e aumenta la tendenza all'azione rapida. Evolutivamente, questa rispo-

sta aveva senso: di fronte a un pericolo reale, non c'è tempo per riflettere. Nella giungla dell'informazione digitale, però, questo meccanismo viene sfruttato sistematicamente.

La consapevolezza di questo meccanismo è già di per sé una difesa. Quando un contenuto ci fa reagire con un'emozione intensa e improvvisa, quella stessa emozione è un segnale: fermati. Non condividere ancora. Fai almeno una domanda. L'emozione forte non è la conferma che una notizia sia vera: è spesso il contrario.

FAKE NEWS ANATOMY: DENTRO LA MACCHINA DELLA DISINFORMAZIONE

Obiettivi del modulo

Al termine di questo modulo saprai riconoscere gli elementi strutturali ricorrenti in una fake news e comprenderai perché certi contenuti ‘funzionano’ psicologicamente. Saprai distinguere una fake news dal clickbait e riconoscerla la zona grigia informativa, ossia quei contenuti che non sono apertamente falsi ma sono manipolatori per omissione o decontestualizzazione.

Cos'è davvero una fake news

Una fake news non è semplicemente una notizia falsa. Questa distinzione è fondamentale e spesso trascurata. Una notizia falsa è un errore e può essere prodotta in buona fede, può essere corretta e non ha necessariamente un'intenzionalità manipolativa. Una fake news è qualcosa di più specifico: è un contenuto progettato per produrre un effetto: catturare attenzione, generare reazione, ottenere condivisioni, orientare l'opinione. La falsità di una fake news, poi, non è sempre totale. È spesso parziale, selettiva, strategica. Un fatto reale può diventare una fake news se viene decontestualizzato, se vengono omessi elementi cruciali, se viene presentato in un modo che produce una conclusione che i fatti da soli non supporterebbero. La disinformazione più efficace lavora spesso in questa zona grigia: non mente apertamente, ma seleziona, enfatizza, tralascia.

La struttura di una fake news: gli elementi ricorrenti

Le fake news non sono improvvisate. Usano strutture che si ripetono, perché quelle strutture funzionano. Conoscerle è il modo più efficace per riconoscerle.

Il titolo: l'amo. Il titolo è la parte più importante di una fake news, e spesso è l'unica parte che viene letta. Non è progettato per informare: è progettato per fermare lo scorrimento, per creare una reazione immediata. Crea urgenza 'Allarme! Scoperto che...' e semplifica in modo estremo, trasformando una questione complessa in una certezza assoluta. Inoltre, promette rivelazioni ('La verità che nessuno ti dice'). Se il titolo ti fa reagire prima ancora di capire cosa sta dicendo, sta facendo esattamente il suo lavoro.

La leva emotiva. Dopo il titolo, entra in gioco l'emozione. Paura, rabbia, indignazione, compassione, scandalismo: sono le emozioni che le fake news prediligono perché producono la risposta più rapida e la condivisione più immediata. L'emozione arriva prima del pensiero. Quando un contenuto ci colpisce emotivamente, il cervello riduce il controllo critico, non per stupidità, ma per fisiologia.

Le immagini fuori contesto. Molte fake news non inventano immagini. Le riciclano. Un'immagine vera, fotografata in un contesto completamente diverso, viene usata come 'prova visiva' di qualcosa che non ha mai avuto luogo. Il cervello umano tende a fidarsi delle immagini: le considera più difficili da falsificare rispetto al testo. Questa fiducia viene sfruttata sistematicamente. Un'immagine vera può diventare una prova falsa semplicemente spostata nel tempo o nel contesto.

La falsa autorevolezza. Le fake news imitano il linguaggio dell'autorevolezza senza dimostrarne i requisiti. Frasi come 'secondo esperti', 'studi dimostrano', 'lo dicono tutti', 'fonti attendibili confermano' evocano la fonte senza identificarla, creano l'impressione di un consenso che non esiste, e producono in chi legge una sensazione di credibilità che non è supportata da nessun elemento verificabile.

L'invito implicito alla condivisione. Molte fake news sono costruite per generare la risposta 'devo assolutamente girare questo a tutti'. L'urgenza, la sensazione di possedere una verità nascosta, l'indignazione che spinge a 'far sapere agli altri': questi meccanismi trasformano il lettore in amplificatore. Condividere diventa un atto morale ('è mio dovere informare') il che abbassa ulteriormente la soglia della verifica.

Fake news vs clickbait: una distinzione importante

Non tutto ciò che attira l'attenzione con titoli esagerati è una fake news. Il clickbait (letteralmente 'esca per click') usa titoli sensazionalistici per portare il lettore a cliccare su un contenuto che spesso risulta deludente rispetto alle aspettative create. Il contenuto può essere vero, ma è povero, incompleto o fuorviante. L'obiettivo è il clic, che genera guadagni pubblicitari. Non necessariamente l'orientamento dell'opinione.

La fake news, invece, non vuole solo il clic. Vuole orientare il pensiero. Vuole che il lettore esca con una convinzione che non aveva prima, o con una convinzione preesistente rafforzata. La differenza: clickbait attira, fake news manipola. La distinzione è importante perché richiedono risposte diverse: al clickbait si risponde con il pensiero critico sulla qualità dell'informazione; alla fake news occorre anche chiedersi chi ha un interesse a far credere quella cosa.

La zona grigia informativa

La zona grigia è lo spazio più insidioso dell'ecosistema informativo digitale. Qui non c'è una bugia evidente: c'è una verità incompleta. Un fatto reale privato del contesto necessario per comprenderlo. Un dato vero usato in modo selettivo per supportare una conclusione che i dati completi non supporterebbero.

Esempi di zona grigia: una statistica reale presentata senza il confronto necessario per interpretarla; una citazione autentica di una persona autorevole decontestualizzata dal discorso in cui era inserita; una fotografia reale attribuita a un evento diverso da quello in cui è stata scattata; una notizia vera di mesi fa riproposta come ‘appena accaduto’. In tutti questi casi, non c’è una falsità esplicita da poter smentire facilmente. C’è una manipolazione del contesto che produce una percezione distorta della realtà.

I meccanismi psicologici: perché funziona su tutti

Comprendere perché le fake news funzionano richiede di guardare alla psicologia cognitiva, non alla stupidità. Le fake news sfruttano meccanismi che riguardano tutti gli esseri umani, indipendentemente dall’istruzione, dall’intelligenza, dall’esperienza digitale.

Il bias di conferma è forse il meccanismo più potente. Tendiamo a cercare, notare e ricordare le informazioni che confermano ciò che già pensiamo, e a ignorare o sminuire quelle che lo contraddicono. Una fake news che rafforza una convinzione preesistente incontrerà pochissima resistenza critica: la mente è già predisposta a credere.

Il bisogno di appartenenza ci porta a condividere contenuti che ci identificano come parte di un gruppo: persone che ‘hanno capito’, che conoscono ‘la verità nascosta’, che si oppongono a ‘ciò che tutti gli altri fanno finta di non vedere’. La condivisione non è soltanto informativa: è un atto identitario.

La paura di restare esclusi — FOMO — ci spinge a reagire e condividere immediatamente quando ‘tutti ne parlano’, per non essere gli unici a non sapere. In questo stato di ansia sociale, la verifica rallenta rispetto alla velocità richiesta dal flusso.

Le fake news non cercano di convincerti di qualcosa di lontano da te. Rafforzano ciò che già credi. Ti fanno sentire parte di un gruppo, custode di una verità condivisa. È questo che le rende così difficili da smentire: smentire la fake news significa smentire qualcosa di cui la persona si sente parte.

Obiettivi del modulo

Al termine di questo modulo saprai distinguere l'opinione dall'informazione verificata. Conoscerai i tre controlli minimi da applicare sempre (fonte, data, riscontro) e saprai come eseguirli in modo pratico. Conoscerai i principali strumenti di fact-checking disponibili e saprai come eseguire una ricerca consapevole che vada oltre il titolo sensazionalistico.

Opinione o informazione verificata?

Prima di applicare qualsiasi strumento di verifica, è utile fare una distinzione che sembra ovvia ma non lo è affatto nella pratica: la differenza tra un'opinione e un'informazione verificata. Non tutto ciò che leggiamo online è informazione. Molto di ciò che consumiamo come se fosse informazione è in realtà opinione, commento, interpretazione.

Un'opinione non è sbagliata: può essere preziosa, stimolante, illuminante. Ma non è verificabile nel senso in cui è verificabile un fatto. Se qualcuno dice 'questa politica economica è sbagliata', sta esprimendo un'opinione, quindi non una bugia, ma nemmeno un fatto controllabile. Se dice 'questa politica ha causato un aumento della disoccupazione del 3,7%', sta facendo un'affermazione fattuale verificabile.

Il problema sorge quando l'opinione si traveste da notizia: usa un tono assertivo e categorico che non ammette dubbi, non cita fonti verificabili, usa frasi come 'è evidente che', 'tutti sanno che', 'è chiaro come' per presentare come oggettiva una valutazione soggettiva. Riconoscere questo travestimento è uno dei passi più importanti verso una lettura critica dell'informazione.

I tre controlli minimi: Fonte, Data, Riscontro

Non serve verificare tutto. Serve sapere quando fermarsi e da dove partire. I tre controlli che seguono sono il minimo indispensabile per non essere completamente indifesi di fronte all'ecosistema informativo digitale. Sono semplici, rapidi e applicabili da chiunque.

1. Verificare la fonte

La fonte è il primo filtro. Non ci dice con certezza se una notizia è vera, ma ci dice se è attribuibile a qualcuno che si prende una responsabilità per ciò che scrive. Quando si legge un contenuto, ci si chiede: chi lo dice? Dove è pubblicato? Il nome di un autore o di una redazione è identificabile? Il sito ha una pagina 'Chi siamo' con contatti e riferimenti? L'URL è coerente con l'identità dichiarata e non una sequenza strana di caratteri o un dominio chiaramente improvvisato?

Se mancano questi elementi, non significa automaticamente che il contenuto sia falso. Significa che non si sa a chi attribuire la responsabilità di ciò che si legge. E quando non c'è nessuno che si prende la responsabilità di un'affermazione, quella affermazione vale molto meno di quanto sembra.

Un caso frequente: i siti che imitano testate giornalistiche note, con nomi molto simili ma non identici (ad es. Corriere Della Sera News, Il Sole 24 Ore Online Today, La Repubblica Breaking) progettati per sembrare fonti autorevoli a un'occhiata veloce. Prima di fidarsi di una fonte, val la pena verificare che il nome del sito corrisponda esattamente a quello della testata che si conosce.

2. Verificare la data

Le notizie vecchie riproposte come attuali sono uno dei meccanismi di disinformazione più diffusi e più efficaci. Un fatto reale accaduto anni fa viene ripreso, spesso senza modifiche, e ricondiviso come se fosse una notizia di oggi. Chi lo riceve, non avendo memoria dell'evento originale, lo percepisce come attuale. Il contesto temporale cambia completamente il significato.

Come si verifica la data? Si cerca sotto il titolo dell'articolo, spesso c'è la data di pubblicazione o di aggiornamento, o in fondo all'articolo, nonché negli screenshot, ma la data è spesso tagliata intenzionalmente: se manca, è già un segnale di allarme. Se la data non è chiara, la notizia può essere vera, ma fuori contesto. E fuori contesto diventa manipolazione.

Un caso tipico: durante eventi di attualità come crisi politiche, disastri naturali, situazioni di emergenza, vengono riproposte immagini e notizie di eventi simili accaduti in precedenza, presentati come se stessero accadendo in quel momento. La reazione emotiva del pubblico amplifica la diffusione prima che qualcuno verifichi la data originale.

3. Verificare il riscontro

Una notizia importante non esiste su un solo sito. Se un evento di rilievo è davvero accaduto, verrà riportato da più fonti indipendenti con dati sostanzialmente coerenti. Il riscontro, ossia cercare se la stessa notizia è riportata da fonti diverse, è uno dei controlli più efficaci e più trascurati.

Come si fa il riscontro in modo pratico e veloce? Si estrarrebbero due o tre parole chiave neutre dal contenuto, non il titolo sensazionalistico, che spesso è costruito appositamente per non essere rintracciabile, ma il fatto in sé: luogo, ente, persona, evento. Si cercano sul motore di ricerca. Si aprono almeno due risultati diversi. Si confrontano i dati 'duri': raccontano lo stesso evento? I numeri coincidono? Il contesto è lo stesso?

Se un'unica fonte riporta una notizia che è specialmente sensazionale o emotivamente coinvolgente e nessun'altra fonte indipendente la riporta, non significa automaticamente che sia falsa. Può essere uno scoop genuino. Ma può anche essere una fake news. La mancanza di riscontro è un segnale di allarme che richiede ulteriore cautela prima di condividere.

Regola pratica: Non copiare il titolo emotivo nella barra di ricerca. Cerca il fatto in sé con parole neutre. 'Titolo originale: SHOCK! Il sindaco di Milano dichiara emergenza per il gas!' diventa nella ricerca: 'Milano sindaco emergenza gas' e i risultati saranno molto più utili.

Strumenti di verifica: il toolkit pratico

Esistono strumenti specifici progettati per aiutare nella verifica delle informazioni. Non richiedono competenze tecniche avanzate: richiedono soltanto la volontà di rallentare e applicare un metodo.

I siti istituzionali: sono la prima fonte da consultare quando si tratta di informazioni relative a leggi, dati statistici, comunicati ufficiali, norme sanitarie. Siti come governo.it, salute.gov.it, istat.it, eur-lex.europa.eu offrono informazioni verificate e attribuite. Quando una notizia afferma che 'il governo ha deciso', 'le statistiche dimostrano', 'la legge prevede', il modo più rapido per verificarla è andare direttamente alla fonte istituzionale.

I portali di fact-checking: sono siti specializzati nella verifica delle informazioni più diffuse. In Italia, i più conosciuti sono Pagella Politica – pagellaPolitica.it – che si concentra sulle dichiarazioni dei politici italiani; Bufale.net, che documenta le bufale più virali; FactaNews.it, progetto dell'Agence France-Presse; e Open.online, con una sezione dedicata al fact-checking. A livello internazionale, Snopes.com è uno dei più autorevoli. Questi siti non sono infallibili, ma il loro metodo è trasparente: spiegano le fonti usate, le procedure seguite, le conclusioni raggiunte.

La ricerca inversa per immagini: è uno degli strumenti più potenti per smascherare immagini decontestualizzate. Su Google Immagini, cliccando sull'icona della fotocamera nella barra di ricerca, si può caricare un'immagine o incollare il suo URL per trovare tutte le occorrenze di quell'immagine sul web, inclusa la data e il contesto originale di pubblicazione. TinEye.com è un'altra piattaforma dedicata esclusivamente a questo tipo di ricerca. In pochi secondi si può scoprire se un'immagine 'di oggi' era già in circolazione anni fa in un contesto completamente diverso.

I motori di ricerca usati consapevolmente: la differenza tra una ricerca efficace e una inefficace sta spesso nella scelta delle parole chiave. Il metodo

base è: evitare di cercare il titolo sensazionalistico, identificare i dati ‘neutri’ dell’evento (chi, cosa, dove, quando) cercarli in combinazione, confrontare i risultati di almeno due o tre fonti diverse. Usare le virgolette per cercare una frase esatta quando si vuole trovare la fonte originale di una citazione.

Le immagini e i video fuori contesto

Un caso speciale di verifica riguarda immagini e video. Il cervello umano tende a fidarsi di ciò che vede: un’immagine sembra una prova più difficile da falsificare rispetto al testo. Questa fiducia viene sfruttata sistematicamente nella produzione di fake news. Esistono due categorie principali di manipolazione visiva. La prima, e più diffusa, è la decontestualizzazione: l’immagine è vera, ma viene attribuita a un evento diverso da quello in cui è stata scattata. Una fotografia di una protesta avvenuta in un paese straniero viene usata come ‘prova’ di una protesta in Italia. Un’immagine di danni da alluvione del 2010 viene usata per illustrare un’alluvione del 2024. La seconda categoria è la manipolazione diretta: l’immagine è stata modificata, ritoccata, tagliata, o generata artificialmente dall’intelligenza artificiale.

Per entrambe le categorie, la ricerca inversa per immagini è lo strumento più efficace. Per i video, una tecnica utile è identificare un frame significativo del video, fermarlo in un momento riconoscibile e fare la ricerca inversa su quel frame come immagine. Spesso si trova la fonte originale del video in pochi secondi.

CLICKBAIT E MANIPOLAZIONE: COME NON CASCARE NEL TRANELLO

Obiettivi del modulo

Al termine di questo modulo saprai riconoscere le tecniche di persuasione e i meccanismi del clickbait, comprenderai come il passaggio dal clickbait alla manipolazione avviene progressivamente, conoscerai i dark pattern informativi e saprai valutare l'impatto delle proprie azioni di condivisione online.

Cos'è il clickbait e perché funziona

Il clickbait (letteralmente 'esca per click') è una tecnica di costruzione dei contenuti che usa titoli esagerati, immagini shock e promesse emotive per attirare clic e generare traffico. L'obiettivo primario non è informare: è far cliccare, perché ogni clic genera guadagni pubblicitari o dati sugli utenti.

Il clickbait funziona perché sfrutta meccanismi cognitivi universali che non hanno nulla a che fare con la stupidità o la mancanza di istruzione.

La curiosità: nasce dall'informazione incompleta. Quando manca un pezzo di un'informazione, il cervello tende a volerlo colmare. Il titolo 'Ecco cosa ha fatto il sindaco dopo la riunione' attiva la curiosità sfruttando l'informazione mancante: cosa ha fatto? Il cervello vuole completare il quadro e l'unico modo per farlo è cliccare.

L'urgenza: riduce il tempo del pensiero critico. 'Ultimi minuti: la verità che cambia tutto'. Se la sensazione è 'devo sapere subito', la verifica passa in secondo piano. L'urgenza crea uno stato mentale simile al panico lieve: il ragionamento rallenta, l'azione si accelera.

La FOMO: Fear of Missing Out, la paura di restare esclusi. 'Tutti stanno già condividendo questo'. 'Non puoi non sapere questa cosa'. Quando l'ansia sociale si attiva, con la conseguente paura di non fare parte del gruppo o di essere l'unico a non essere aggiornato, si condivide ancor prima di aver verificato la notizia, per non perdere il momento.

L'indignazione: attiva una risposta immediata e quasi automatica. Quando qualcosa ci scandalizza o ci fa arrabbiare, reagiamo prima di analizzare. Il clickbait costruito attorno all'indignazione è particolarmente efficace perché trasforma la condivisione in un atto quasi morale: 'devo far sapere agli altri questa vergogna'.

Le tecniche linguistiche del clickbait

Alcune espressioni linguistiche ricorrono con tale frequenza nei contenuti clickbait e nelle fake news da essere quasi una firma. Riconoscerle è uno strumento di difesa immediato.

‘Non vogliono che tu lo sappia’: introduce un frame complottistico. Chi legge si sente parte di una minoranza ‘che ha capito’, contro un potere oscuro che nasconde la verità. Questo meccanismo è particolarmente seducente perché soddisfa il bisogno di appartenenza e di identità: io sono uno di quelli che sa.

‘Incredibile ma vero’: sospende il giudizio critico. L’incredulità viene dichiarata nel titolo prima che il lettore abbia la possibilità di formarla autonomamente: il contenuto è già stato etichettato come straordinario, e il cervello tende ad accettare questa categorizzazione.

‘Ecco cosa succede se...’: costruisce una promessa condizionale che invita ad agire per evitare una perdita o ottenere un vantaggio. È la struttura narrativa della trappola: prima crea il bisogno, poi offre la risposta. Ma la risposta è il clic.

‘Solo per oggi / Ultimo posto / Scade tra...’: sono le formule dell’urgenza artificiale. Eliminano il tempo per riflettere, verificare, confrontare. Funzionano nella pubblicità e funzionano ugualmente nelle fake news.

Dal clickbait alla manipolazione

Il passaggio dal clickbait, che mira al clic, alla manipolazione, che invece mira a orientare il pensiero, avviene progressivamente e spesso impercettibilmente. Non c’è un confine netto: è un continuum.

La manipolazione informativa avviene quando il contenuto è selettivo: si sceglie quali fatti presentare e quali omettere, producendo una percezione distorta dell’evento complessivo. Quando il contesto è ridotto o eliminato: un dato reale presentato senza il contesto necessario per interpretarlo correttamente diventa fuorviante. Quando la ripetizione rafforza una sola lettura: vedere la stessa interpretazione di un fatto proposta da molte fonti diverse – che in realtà attingono tutte alla stessa fonte originale – crea l’illusione del consenso.

Non viene imposta una verità. Viene ristretto lo spazio delle alternative. Iris Feed non dice cosa pensare: decide cosa vedere e con quale frequenza. E ciò che vediamo spesso e da prospettive simili ci sembra naturale, ovvio, inevitabile. Questa è la forma più sottile e più efficace di manipolazione.

I dark pattern informativi

I dark pattern (letteralmente ‘schemi oscuri’) sono strutture di design progettate per guidare il comportamento dell’utente in direzioni che non avrebbe necessariamente scelto se gli fosse stato chiesto esplicitamente. Originariamente usati nel design delle interfacce utente per spingere a fare acquisti non voluti, ad accettare condizioni sfavorevoli, a iscriversi a servizi senza rendersene conto, i dark pattern si trovano sempre più spesso anche nella progettazione dei contenuti informativi. Esempi di dark pattern informativi: titoli che promettono qualcosa di diverso da ciò che il contenuto effettivamente offre e che cambiano dopo il clic, quando è già troppo tardi. Anteprime incomplete che rivelano solo la parte più emotiva o scandalosa di un contenuto. Pulsanti di condivisione molto evidenziati e strategicamente posizionati per facilitare la condivisione impulsiva prima della lettura. Notifiche insistenti che creano urgenza artificiale. Suggerimenti automatici di contenuti simili che creano catene di consumo emotivo sempre più intense.

Il messaggio implicito di tutti i dark pattern è lo stesso: agisci ora, rifletti dopo. E nella giungla dell’informazione digitale, ‘riflettere dopo’ significa spesso non riflettere mai: il flusso è già andato avanti, il contenuto è già stato condiviso, la reazione è già avvenuta.

Condividere non è neutro

Uno dei messaggi più importanti di questo percorso è che condividere, anche se fatto con le migliori intenzioni, non è un atto neutro. Quando condividiamo un contenuto, partecipiamo alla costruzione dell’ecosistema informativo: aumentiamo la visibilità di quel contenuto, rinforziamo la fonte che lo ha prodotto, influenziamo le persone nella nostra rete.

La piattaforma non distingue l’intenzione. Per l’algoritmo, una condivisione fatta per indignazione ha lo stesso peso di una condivisione fatta per approvazione: entrambe aumentano la visibilità del contenuto, entrambe segnalano all’algoritmo che quel tipo di contenuto produce engagement, entrambe contribuiscono ad amplificarlo ulteriormente. Quando condividiamo una notizia per dire ‘guardate che assurdo!’, stiamo comunque aiutando quella notizia a diffondersi.

Questo non significa non condividere mai. Significa condividere con consapevolezza: avere fatto almeno i tre controlli minimi (fonte, data, riscontro) prima di trasformarsi in amplificatore di un contenuto.

La regola più semplice e più efficace: prima di condividere qualcosa che ti ha fatto sentire un’emozione intensa, aspetta. Non per sempre: aspetta abbastanza da fare una domanda. Chi lo dice? È attuale? Ne parlano altre fonti? Tre domande, trenta secondi, e si evita di diventare inconsapevolmente parte della macchina della disinformazione.

Le 5 regole d'oro per la verifica orizzontale

Al termine del percorso, le competenze acquisite si condensano in cinque regole operative, ossia le regole d'oro della verifica orizzontale dell'informazione. Non sono procedure tecniche complesse: sono abitudini di pensiero che, praticate con costanza, cambiano profondamente la qualità della propria vita informativa.

1. Conoscere la fonte. Chi dice quella cosa? Dove è pubblicato? Il nome è riconoscibile e verificabile? C'è una pagina 'Chi siamo' con contatti reali? Senza una fonte identificabile, un'informazione è solo un'affermazione anonima. E alle affermazioni anonime si dà il credito che meritano: pochissimo.

2. Incrociare i dati. La notizia è riportata da altre fonti indipendenti? Con dati coerenti? Una notizia importante è quasi sempre coperta da più testate. Se un'informazione esiste su un solo sito — specialmente se emotivamente molto coinvolgente — è necessaria prudenza extra prima di diffonderla.

3. Verificare su banche dati e fonti attendibili. Per le informazioni che riguardano salute, leggi, statistiche, dati scientifici: andare alle fonti primarie. I siti istituzionali, i portali governativi, le pubblicazioni scientifiche con peer review, i comunicati ufficiali degli enti competenti. Non tutto è verificabile in questo modo, ma quando lo è, la fonte primaria vale infinitamente di più di qualsiasi fonte secondaria.

4. Avere cura della propria reputazione online. Ogni condivisione contribuisce all'immagine che gli altri si formano di noi. Chi condivide sistematicamente contenuti sensazionalistici, non verificati o palesemente di parte costruisce nel tempo una reputazione informativa che riduce la propria credibilità. La cura della propria reputazione digitale passa anche dalla qualità di ciò che si sceglie di amplificare.

5. Applicare la lettura critica: gli interessi di chi diffonde. Chiedersi sempre: chi ha un interesse a diffondere questa informazione? Quale effetto vuole produrre? Nella giungla dell'informazione, quasi nessun contenuto è completamente neutro. Comprendere la motivazione di chi produce e diffonde un contenuto aiuta a valutarlo con maggiore accuratezza. Non per diventare sospettosi di tutto, ma per essere consapevoli che l'informazione non è mai prodotta nel vuoto.

Queste cinque regole non servono a verificare tutto, anche perché sarebbe impossibile. Servono a riconoscere quando è il momento di rallentare e fare qualche controllo in più. Un solo 'no' a una delle cinque domande dovrebbe essere sufficiente per fermarsi prima di condividere.

Il Kit Anti-Fake: strumenti pratici da portare a casa

Checklist rapida di verifica

Questa checklist è pensata per essere usata concretamente, ogni volta che si incontra un contenuto su cui si hanno dubbi. Non è necessario applicarla a tutto: si applica quando qualcosa crea un'emozione forte, quando sembra troppo sorprendente per essere vero, quando si è tentati di condividere subito.

Fonte: So chi ha scritto questo contenuto? Il sito è riconoscibile e ha una pagina 'Chi siamo'? L'URL ha senso? Sì / No

Data: Quando è stato pubblicato? È attuale o è una notizia vecchia riproposta? Sì / No

Riscontro: Altre fonti indipendenti riportano la stessa cosa con dati coerenti? Sì / No

Emozione: Questo contenuto mi fa sentire paura, rabbia, indignazione o urgenza intensa? Se sì, è un segnale di allarme – non di verità.

Interesse: Chi ha un interesse a diffondere questa informazione? Quale effetto vuole produrre?

Regola generale: se anche solo uno dei primi tre controlli dà un 'No', aspetta prima di condividere. Fai un controllo in più. Il contenuto sarà ancora lì tra cinque minuti.

Strumenti gratuiti a portata di click

Pagella Politica (pagellapolitica.it): fact-checking sulle dichiarazioni dei politici italiani. Usa una scala di valutazione chiara e cita sempre le fonti usate per la verifica.

Bufale.net: database italiano delle bufale più virali. Ottimo per verificare rapidamente se un contenuto è già stato smentito.

FACTA News (facta.news): progetto dell'Agence France-Presse in italiano. Fact-checking professionale su notizie virali.

Open.online: giornale online con una sezione dedicata al fact-checking italiano.

Snopes.com: il più antico e uno dei più autorevoli siti di fact-checking, prevalentemente in inglese.

Google Immagini (ricerca inversa): per verificare l'origine e il contesto di un'immagine. Vai su images.google.com, clicca l'icona della fotocamera, carica l'immagine o incolla il suo URL.

TinEye.com: piattaforma dedicata esclusivamente alla ricerca inversa per immagini. Trova tutte le occorrenze di un'immagine sul web con la data di prima pubblicazione.

Segnali di allarme immediati

Questi segnali non provano che un contenuto sia falso, ma indicano che vale la pena fare qualche controllo in più prima di crederci o condividerlo.

Elementi grafici: titoli scritti TUTTO IN MAIUSCOLO, uso eccessivo di punti esclamativi!!!, errori grammaticali o ortografici frequenti, qualità grafica scadente o logo di testate note riprodotto in modo leggermente diverso.

Elementi linguistici: espressioni come 'Non vogliono che tu lo sappia', 'La verità nascosta', 'Incredibile ma vero', 'Solo per oggi', 'Condividi prima che venga rimosso'. Tono apocalittico o salvatore. Uso di aggettivi iperbolici che non corrispondono ai fatti descritti.

Elementi strutturali: assenza di autore e/o testata identificabili, data di pubblicazione assente o difficile da trovare, URL strano o molto lungo, contenuto che non corrisponde alle promesse del titolo, assenza di link a fonti esterne.

Elementi emotivi: il contenuto produce in te una reazione molto intensa e immediata – paura, rabbia, indignazione, urgenza di condividere – senza che tu abbia ancora avuto il tempo di capire cosa stai effettivamente leggendo.

Riepilogo dei concetti fondamentali

Questo percorso ha costruito una comprensione operativa dell'ecosistema informativo digitale, degli strumenti che lo attraversano e delle competenze necessarie per navigarlo con maggiore consapevolezza.

Viviamo in una giungla dell'informazione in cui notizie, opinioni, pubblicità e manipolazioni si somigliano e scorrono alla stessa velocità. Iris Feed (la metafora dell'algoritmo che seleziona i nostri feed) non cerca la verità: cerca l'at-

tenzione. E l'emozione trattiene l'attenzione molto più della verifica. Capire questo meccanismo è il primo passo per non subirlo passivamente.

La distinzione tra dato, informazione, misinformazione e disinformazione non è accademica: è operativa. La misinformazione si combatte con la verifica e l'educazione; la disinformazione richiede anche di chiedersi chi ha un interesse a costruire e diffondere quel contenuto e con quale obiettivo.

Le fake news non sono improvvisate: usano strutture ricorrenti come titolo-amo, leva emotiva, immagini fuori contesto, falsa autorevolezza, invito alla condivisione, che si ripetono perché funzionano. Riconoscere la struttura è riconoscere il meccanismo. E il meccanismo, una volta visto, perde almeno una parte del suo potere.

I tre controlli minimi (fonte, data, riscontro) sono applicabili da chiunque in pochi minuti. Non servono a verificare tutto: servono a sapere quando è necessario fermarsi. Il clickbait usa le stesse leve emotive della disinformazione (curiosità, urgenza, FOMO, indignazione) con l'obiettivo del clic piuttosto che della manipolazione dell'opinione. Il confine tra i due è spesso sottile. I dark pattern informativi rendono la condivisione impulsiva ancora più facile, riducendo lo spazio per la riflessione.

Condividere non è mai neutro. Ogni condivisione amplifica un contenuto e una fonte, influenza la propria rete, contribuisce a costruire l'ecosistema informativo comune. Le cinque regole d'oro per la verifica orizzontale sono la sintesi pratica di tutto il percorso.

L'obiettivo finale non è la diffidenza: è la consapevolezza. Non 'non fidarsi di niente', ma 'fidarsi meglio'. Non 'verificare tutto', ma 'sapere quando fermarsi'. Da spettatori passivi del feed a lettori attivi della realtà.

Test di autovalutazione finale

Indica la risposta corretta. Le risposte si trovano in fondo alla sezione.

1. Qual è la differenza tra misinformazione e disinformazione? a) Sono la stessa cosa. b) La misinformazione è falsa senza intenzionalità; la disinformazione è costruita deliberatamente per ingannare. c) La disinformazione è solo un errore editoriale.
2. Una fake news è: a) Sempre una notizia completamente inventata. b) Un contenuto progettato per produrre un effetto – attenzione, reazione, condivisione – spesso con falsità parziale o decontestualizzazione. c) Solo una pubblicità travestita da notizia.
3. Quale di questi è uno strumento per la ricerca inversa per immagini? a) Wikipedia. b) Google Immagini o TinEye. c) Trustpilot.
4. Quale segnale di allarme indica una possibile fake news? a) Un solo segnale tra: fonte sconosciuta, tono allarmistico, assenza di link a fonti, data non verificabile. b) Due segnali contemporanei, altrimenti non conta. c) Solo la mancanza completa di fonti.
5. Cos'è la camera dell'eco? a) Un ambiente sonoro professionale. b) Un ambiente informativo in cui gli utenti sono esposti prevalentemente a contenuti simili alle proprie opinioni, con esclusione progressiva di voci diverse. c) Un gruppo WhatsApp di persone con le stesse idee.
6. Il bias di conferma ci porta a: a) Verificare con più attenzione le informazioni che confermano ciò che già pensiamo. b) Credere più facilmente alle informazioni che confermano le nostre convinzioni preesistenti. c) Condividere solo notizie verificate.
7. Perché condividere non è neutro? a) Perché la piattaforma potrebbe bloccare l'account. b) Perché ogni condivisione amplifica un contenuto, rinforza una fonte e influenza la propria rete, indipendentemente dall'intenzione. c) Perché le condivisioni sono visibili a tutti.
8. Qual è il primo dei tre controlli minimi da applicare sempre? a) Verificare il riscontro. b) Verificare la fonte. c) Verificare la data.

Risposte: 1-b / 2-b / 3-b / 4-a / 5-b / 6-b / 7-b / 8-b

Autovalutazione delle competenze DigComp 2.2

Compila questa scheda prima e dopo il percorso formativo. Per ciascuna voce, indica il tuo livello su una scala da 1 a 5: 1 = non mi sento ancora in grado, 5 = mi sento completamente autonomo.

Area di Competenza	DigComp	Prima (1-5)	Dopo (1-5)
So riconoscere quando una notizia è attendibile o manipolata	1.2		
So distinguere dato, informazione, disinformazione, misinformazione	1.2		
Riconosco gli elementi strutturali di una fake news	1.2		
So fare i tre controlli minimi: fonte, data, riscontro	1.2		
So usare strumenti di fact-checking e ricerca inversa per immagini	5.1		
Riconosco il clickbait e le sue leve emotive	1.2		
Riconosco i dark pattern informativi	4.3		
So valutare gli interessi di chi produce e diffonde un contenuto	1.2		
Condivido in modo più consapevole e responsabile	2.3		
Mi sento più autonomo/a nella lettura critica dell'informazione	Generale		

Glossario essenziale

Algoritmo: insieme di regole automatiche che determinano quali contenuti vengono mostrati a ciascun utente nei feed dei social network, ottimizzate per massimizzare il tempo trascorso sulla piattaforma piuttosto che per la qualità o la veridicità dell'informazione.

Bias di conferma: tendenza cognitiva a cercare, notare e ricordare le informazioni che confermano le proprie convinzioni preesistenti, ignorando o mi-

nimizzando quelle che le contraddicono.

Camera dell'eco: ambiente informativo in cui gli utenti sono esposti prevalentemente a contenuti e opinioni simili alle proprie, con progressiva esclusione di voci diverse, amplificata dagli algoritmi delle piattaforme.

Clickbait: tecnica di costruzione dei contenuti che usa titoli esagerati e promesse emotive per attrarre clic e traffico, spesso con contenuto deludente o fuorviante rispetto a quanto promesso.

Dark pattern informativo: struttura di progettazione dei contenuti e delle interfacce pensata per guidare l'utente verso comportamenti — come la condivisione impulsiva — che non avrebbe necessariamente scelto in modo consapevole.

Dato: frammento isolato di informazione grezzo, privo di contesto. Un dato senza contesto non produce informazione affidabile.

Disinformazione: informazione falsa o manipolata diffusa con l'intento deliberato di ingannare, orientare l'opinione o produrre un effetto specifico.

Fact-checking: processo di verifica sistematica della veridicità di affermazioni, dichiarazioni o contenuti, basato su fonti primarie e metodologia trasparente.

Fake news: contenuto progettato per sembrare informazione giornalistica ma costruito per produrre un effetto — attenzione, reazione, condivisione — spesso attraverso falsità parziale, decontestualizzazione o manipolazione emotiva.

FOMO (Fear of Missing Out): paura di restare esclusi da esperienze, informazioni o conversazioni che coinvolgono il proprio gruppo sociale. Viene sfruttata dal clickbait e dalle fake news per indurre la condivisione immediata.

Informazione: dato inserito in un contesto verificabile, con fonte identificabile e data. A differenza del dato grezzo, l'informazione può essere controllata, confutata e aggiornata.

Iris Feed: personaggio narrativo del percorso BREAK THE FAKE. Metafora dell'algoritmo che seleziona i contenuti nei feed digitali, non in base alla verità ma in base alla capacità di catturare e trattenere l'attenzione.

Misinformazione: informazione falsa o inesatta diffusa senza intenzione di ingannare. Chi la condivide crede di dire la verità: ha ricevuto un'informazione

errata e l'ha trasmessa senza verificarla.

Ricerca inversa per immagini: tecnica che permette di trovare la fonte originale e il contesto di un'immagine cercandola per contenuto visivo invece che per testo. Disponibile su Google Immagini e TinEye.

Verifica orizzontale: metodo di verifica che confronta una notizia su più fonti diverse e indipendenti, invece di verificare la credibilità di una singola fonte. Più efficace della verifica verticale (che controlla solo la reputazione della fonte) perché incrocia i dati.

Zona grigia informativa: spazio dei contenuti che non sono apertamente falsi ma sono manipolatori per omissione, decontestualizzazione o enfasi selettiva. La forma più insidiosa di disinformazione perché non può essere smentita semplicemente.

TEMA C

ACCESSO AI SERVIZI ESSENZIALI



ACCESSO AI SERVIZI ESSENZIALI



Digita Facile
Campania

A chi è rivolto questo capitolo

Questo capitolo nasce con un obiettivo preciso: accompagnarti, passo dopo passo, verso una maggiore autonomia nell'utilizzo dei servizi digitali pubblici. Non è importante da dove parti, né il livello di dimestichezza che hai con smartphone, computer o piattaforme online.

Ciò che conta è il punto di arrivo: sentirti in grado di gestire in prima persona pratiche, richieste e servizi che fino a oggi ti sono sembrati complessi, lontani o riservati ad altri. Il mondo in cui viviamo è profondamente cambiato.

Sempre più servizi della Pubblica Amministrazione sono accessibili da casa, in qualsiasi momento, senza vincoli di orario e senza la necessità di recarsi fisicamente presso uno sportello. Tuttavia, questa trasformazione non è stata accompagnata, per molto tempo, da un adeguato supporto alle persone. Ne è derivata una distanza reale tra ciò che è possibile fare e ciò che le persone si sentono effettivamente in grado di fare.

Non è la tecnologia a creare difficoltà. È la mancanza di accompagnamento

Le difficoltà che incontri non dipendono da te. Per anni, i servizi digitali sono stati progettati senza un reale supporto alle persone. Questo percorso serve proprio a colmare quella distanza. Questo capitolo si colloca proprio in questo spazio: non è un manuale tecnico, ma uno strumento di accompagnamento. Il suo compito non è solo spiegare “come si fa”, ma restituire sicurezza, fiducia e consapevolezza.

Le pagine che seguono riprendono la struttura del corso “Addio Code! Accesso Semplice ai Servizi Essenziali” e ne traducono i contenuti in forma discorsiva, per consentire una lettura continua, coerente e progressiva. Puoi scegliere di seguire l'ordine proposto oppure partire dai temi che senti più vicini alle tue esigenze.

Questo non è semplicemente un percorso formativo. È un passaggio di competenza. È un cambiamento di prospettiva. È l'inizio di una nuova modalità di relazione con i tuoi diritti.

Il digitale non è un mondo nuovo. È lo stesso mondo, senza attese.

Il digitale non cambia i tuoi diritti: cambia solo il modo in cui li eserciti. Un certificato, una domanda, un pagamento restano gli stessi. Ciò che cambia è il tempo, lo spazio e la possibilità di farlo in autonomia.

C'è un'esperienza che accomuna tutti: l'attesa. Attendere il proprio turno in un ufficio pubblico, prendere un numero, aspettare che venga chiamato, spesso per ottenere un documento che oggi potrebbe essere disponibile in pochi secondi direttamente sul proprio dispositivo.

Non si tratta solo di tempo perso. Si tratta di energia, di organizzazione, di dipendenza da orari e da procedure che non sempre si adattano alla vita quotidiana delle persone. A questo si aggiunge un ulteriore elemento: la necessità di chiedere aiuto. Un familiare, un conoscente, qualcuno “più pratico” a cui affidare operazioni che dovrebbero essere personali. Queste difficoltà non sono responsabilità individuali. Sono il risultato di un processo di digitalizzazione che, per molti anni, non ha tenuto conto dei bisogni reali delle persone. Interfacce poco intuitive, linguaggi tecnici, assenza di accompagnamento: tutto questo ha generato distanza, diffidenza e, spesso, rinuncia.

Il percorso formativo in cui si inserisce questa dispensa nasce esattamente per superare questa distanza. Non si tratta di imparare a usare un computer in senso generale, ma di acquisire una competenza concreta: utilizzare il digitale per esercitare i propri diritti in modo autonomo, semplice e consapevole.

Il progetto “Dritti al Punto”, all'interno del programma Digita Facile Campania della Fondazione IFEL Campania, si colloca in questa direzione. L'obiettivo non è formare esperti, ma cittadini digitali attivi, capaci di orientarsi e di agire. Il passaggio chiave è questo: trasformare la dipendenza in autonomia.

Autonomia digitale significa libertà concreta.

Essere autonomi nel digitale significa non dipendere dagli orari degli uffici, non dover chiedere aiuto per ogni operazione e poter controllare direttamente le proprie informazioni. È un cambiamento pratico, prima ancora che tecnologico.

La paura del digitale: un ostacolo reale, ma superabile

Quando si parla di difficoltà nell'utilizzo dei servizi digitali, si tende a pensare immediatamente alla tecnologia. In realtà, l'ostacolo principale è spesso di natura diversa. Non è lo strumento a essere complesso. È la percezione dello strumento. La paura di sbagliare, di bloccare un sistema, di inserire dati in modo errato o di compromettere una procedura è un elemento diffuso e profondamente radicato. A questa si aggiunge il timore del giudizio: l'idea di non essere “capaci”, di essere in ritardo rispetto agli altri, di non riuscire a recuperare.

La paura di sbagliare è normale. Restare fermi no.

L'errore non è un fallimento. È un passaggio del processo. Ogni competenza digitale nasce da tentativi, non da perfezione. Queste sensazioni sono legittime. Ma non sono definitive. Il digitale, se accompagnato nel modo corretto, diventa progressivamente familiare. E soprattutto, non è un percorso da affrontare in solitudine. I Punti di Facilitazione Digitale rappresentano una rete concreta di supporto, in cui ogni persona può trovare guida, ascolto e orientamento.

Non sei solo: esiste una rete di supporto.

Dietro ogni servizio digitale esiste una rete fisica di supporto: i facilitatori digitali e i punti di facilitazione. Chiedere aiuto è parte del percorso, non un segno di difficoltà. Il cambiamento avviene quando si passa da una logica di evitamento a una logica di sperimentazione.

Tre vantaggi concreti dei servizi digitali che cambieranno la tua quotidianità

Comprendere il valore del digitale significa andare oltre la dimensione teorica e riconoscerne l'impatto nella vita quotidiana.

Il primo vantaggio è di tempo e di economicità. Ogni operazione che può essere svolta online elimina spostamenti, attese e vincoli. Ogni certificato che scarichi tu stesso dall'ANPR non ti costa nulla, né in termini di marche da bollo né in termini di ore passate allo sportello. Ogni pagamento che effettui tramite PagoPA dal divano di casa è un viaggio in meno da fare, una coda in meno da sopportare.

Il secondo vantaggio è l'autonomia e la trasparenza. Quando gestisci tu stesso le tue pratiche digitali, hai il controllo diretto su ciò che ti riguarda. Puoi verificare in qualunque momento lo stato di una domanda all'INPS, scaricare un referto medico a mezzanotte, consultare le tue ricevute di pagamento. Non sei più dipendente dagli orari di uno sportello o dalla disponibilità di qualcun altro.

Il terzo vantaggio è l'inclusione. I servizi digitali pubblici italiani sono progettati per essere accessibili a tutti, compresi gli anziani e chi ha difficoltà visive o motorie. Le interfacce touch degli smartphone hanno reso molto più semplice interagire con i dispositivi rispetto ai vecchi computer con tastiera e mouse. Il digitale, se usato bene, livella le differenze invece di ampliarle.

Il digitale è uno strumento di inclusione, non di esclusione

Se usato correttamente, il digitale riduce le distanze, semplifica l'accesso e amplia le opportunità.

La nostra bussola: il quadro DigComp 2.2

Per dare struttura e coerenza al percorso formativo, si è fatto riferimento al quadro europeo DigComp 2.2, che definisce le competenze digitali fondamentali per ogni cittadino in relazione alla vita reale. Non è necessario conoscerne la struttura nel dettaglio. Ciò che è importante comprendere è che ogni contenuto affrontato risponde a un modello riconosciuto e condiviso a livello europeo.

DigComp non è teoria: è vita quotidiana.

Le competenze digitali non sono astratte: servono per informarsi, accedere ai servizi, comunicare e proteggersi nella vita di tutti i giorni. Il primo passo di questa bussola riguarda la capacità di orientarsi tra le informazioni, riconoscendo i canali ufficiali e utilizzando in modo corretto gli strumenti di ricerca.

Il primo passo è saper scegliere dove cercare. Nel digitale non conta sapere tutto. Conta sapere dove andare: siti ufficiali, portali istituzionali, fonti affidabili.

Verso l'autonomia digitale

Il percorso che si apre con questa dispensa non è fatto di nozioni isolate, ma di passaggi progressivi. Ogni modulo rappresenta un livello di competenza che si costruisce sul precedente: dall'identità digitale all'accesso ai servizi, dalla gestione dei pagamenti alla risoluzione dei problemi.

L'obiettivo finale non è semplicemente "saper fare". È saper fare in autonomia, con sicurezza e consapevolezza.

È il passaggio da utente passivo a cittadino digitale attivo.

Ed è proprio da qui che il percorso può iniziare.

Per comprendere davvero il funzionamento dei servizi digitali pubblici, è utile partire da un'immagine semplice. Si immagini un grande edificio che raccoglie tutti i servizi essenziali: il Comune, l'INPS, il sistema sanitario, la scuola. Per entrare, è necessario essere riconosciuti. Nel mondo fisico questo avviene mostrando un documento. Nel mondo digitale, il principio è lo stesso: cambia soltanto lo strumento.

Questo strumento si chiama identità digitale.

Non si tratta di un elemento aggiuntivo o complesso, ma della condizione necessaria per accedere ai servizi. È ciò che permette di essere riconosciuti in modo certo, di operare online con valore legale e di gestire in autonomia pratiche e richieste. Nel sistema italiano, l'identità digitale si utilizza attraverso due strumenti principali: SPID e CIE.

SPID e CIE: due strumenti, una sola identità

Quando si parla di identità digitale, è importante chiarire un aspetto fondamentale: non esistono due identità diverse. La persona è sempre la stessa. Ciò che cambia è il modo in cui viene riconosciuta.

Lo SPID rappresenta oggi lo strumento più diffuso. Si basa su credenziali personali, nome utente e password, integrate da un sistema di verifica tramite dispositivo. Consente di accedere a un numero molto elevato di servizi pubblici e privati, ed è utilizzabile da computer, smartphone e tablet.

La CIE, ovvero la Carta di Identità Elettronica, è invece un documento già in possesso della maggior parte dei cittadini. La sua funzione non si limita all'identificazione fisica: grazie al microchip integrato e all'utilizzo di un'App dedicata, può essere impiegata anche per l'accesso ai servizi digitali.

La differenza tra i due strumenti è soprattutto operativa: lo SPID è più immediato e adatto a un utilizzo frequente; la CIE richiede un passaggio aggiuntivo, ma garantisce un livello di sicurezza più elevato, perché combina un elemento fisico, la carta, e un elemento personale, il PIN.

SPID facilita l'accesso quotidiano. CIE garantisce il massimo livello di identità.

L'attivazione dello SPID

L'ottenimento dello SPID segue un percorso strutturato e guidato.

Il primo passaggio consiste nella scelta di un gestore di identità tra quelli accreditati da AgID, l'Agenzia per l'Italia Digitale. I più noti sono Poste Italiane

(PosteID), InfoCert, Aruba, Sielte e TIM. Ognuno offre procedure di registrazione leggermente diverse, ma il processo è sempre lo stesso nelle sue fasi essenziali.

Successivamente, è richiesta la registrazione; devi creare un account sul sito del gestore che hai scelto, inserendo i tuoi dati personali, un indirizzo e-mail valido e un numero di cellulare.

Poi devi scegliere una password sicura e completare il processo di riconoscimento, che serve a verificare che tu sia davvero la persona che dice di essere.

Il momento centrale del processo è rappresentato dal riconoscimento. È in questa fase che viene verificata l'identità della persona. Il riconoscimento può avvenire online, tramite strumenti digitali, oppure in presenza presso uno sportello. Una volta completata questa fase, le credenziali vengono attivate e diventano operative. Conservale con cura: sono la chiave di accesso a tutti i servizi pubblici digitali italiani. Da questo momento, l'accesso ai servizi digitali può avvenire in autonomia, senza necessità di intermediazione.

Come si attiva la CIE per il suo utilizzo digitale

La Carta di Identità Elettronica non è soltanto un documento di riconoscimento. È, a tutti gli effetti, uno strumento già predisposto per l'accesso ai servizi digitali.

Spesso questo aspetto non viene percepito immediatamente, perché la carta continua a essere utilizzata nella sua funzione più tradizionale. In realtà, tutte le condizioni per l'uso digitale sono già presenti. È necessario soltanto attivarla correttamente. Il primo passaggio consiste nell'installazione dell'app dedicata sul proprio smartphone. L'applicazione è disponibile sia per dispositivi Android che per iPhone e rappresenta il punto di collegamento tra la carta fisica e i servizi online.

Una volta installata, è necessario procedere con l'associazione della carta. Questa fase richiede che lo smartphone sia compatibile con la tecnologia NFC, la stessa utilizzata per i pagamenti contactless, perché è attraverso questa tecnologia che il dispositivo riesce a "leggere" il chip presente nella carta. Il secondo elemento indispensabile è il PIN della CIE. Il PIN non viene consegnato in un'unica soluzione, ma in due parti distinte: una parte viene rilasciata al momento della richiesta della carta presso il Comune, mentre la seconda viene inviata successivamente. Solo ricomponendo entrambe le parti è possibile ottenere il PIN completo necessario per l'attivazione.

Durante la procedura guidata dell'app, la carta viene avvicinata allo smar-

ophone e riconosciuta. A questo punto viene richiesto l'inserimento del PIN. È questo passaggio che consente di collegare in modo sicuro la carta al dispositivo e di renderla operativa per l'accesso ai servizi digitali. Può accadere che il PIN non sia stato conservato o non sia più disponibile. In questi casi non si tratta di un ostacolo definitivo. È possibile richiedere il recupero del codice - attraverso il cosiddetto PUK - rivolgendosi allo sportello anagrafico del proprio Comune. Si tratta di una procedura ordinaria, generalmente semplice e accessibile. Una volta completata l'attivazione, la funzione della CIE cambia in modo sostanziale. Non è più soltanto un documento da mostrare quando richiesto, ma diventa una chiave di accesso personale, utilizzabile ogni volta che è necessario entrare nei servizi digitali della Pubblica Amministrazione.

La CIE è già uno strumento digitale completo: l'attivazione ne rende possibile l'utilizzo reale.

La sicurezza: autenticazione a due fattori

Uno degli argomenti più importanti di questo modulo riguarda la sicurezza. L'accesso ai servizi digitali comporta la gestione di dati personali e sensibili. Per questo motivo, il sistema prevede un livello di sicurezza articolato.

Quando si accede con SPID o CIE, non è sufficiente inserire una password. Viene richiesto un secondo elemento di verifica: un codice temporaneo inviato al dispositivo personale. Questo sistema prende il nome di autenticazione a due fattori. Il primo elemento è "qualcosa che sai", la password.

Il secondo è "qualcosa che hai", il tuo Smartphone. Il codice temporaneo, chiamato OTP, One Time Password, ha una validità limitata nel tempo, pochi secondi, e può essere utilizzato una sola volta.

Questo sistema si chiama autenticazione a due fattori o 2FA, e rappresenta un meccanismo di sicurezza molto efficace. Anche se qualcuno riuscisse a scoprire la tua password, non potrebbe accedere ai tuoi servizi senza avere anche il tuo telefono. È come avere una porta blindata con due serrature diverse: aprirne una sola non basta.

Per lo SPID esistono tre livelli di sicurezza. Il Livello 1 richiede solo nome utente e password, ed è il meno sicuro. Il Livello 2 aggiunge il codice OTP temporaneo: è quello che si usa per la grande maggioranza dei servizi pubblici ed è ampiamente sicuro per l'uso quotidiano. Il Livello 3, il più elevato, richiede anche un dispositivo fisico aggiuntivo come la CIE o una smart card, e viene usato solo per operazioni particolarmente delicate.

Il codice OTP è strettamente personale e non deve essere condiviso

Le Tre regole d'oro per proteggere le tue credenziali

Oltre all'OTP, ci sono alcune regole fondamentali per custodire le proprie credenziali digitali.

La prima è che le credenziali SPID sono strettamente personali: non devono mai essere condivise con nessuno, nemmeno con i familiari più stretti. Se hai bisogno di aiuto per compilare una pratica, chiedi a qualcuno di guidarti mentre sei tu a inserire la password, non di farlo al tuo posto.

La seconda regola riguarda la password: sceglila lunga, complicata e diversa per ogni servizio. Una password sicura contiene lettere maiuscole e minuscole, numeri e simboli speciali, ed evita nomi di persone care, date di nascita o sequenze ovvie come "1234". Cambiala periodicamente, come faresti con la combinazione del lucchetto di una cassaforte.

La terza regola riguarda il PIN della CIE: non scriverlo sulla carta stessa o in un foglietto tenuto nel portafoglio insieme alla carta. Questo sarebbe come tenere la chiave della casa nella serratura. Un'ottima soluzione è usare un'app per note protetta da password sul tuo smartphone, oppure annotarlo in un posto sicuro a casa, lontano dalla carta.

REGOLA D'ORO: proteggere le credenziali significa mantenere il controllo della propria identità digitale

Dalla difficoltà alla familiarità

L'utilizzo iniziale degli strumenti digitali può generare incertezza. È una fase normale, legata alla novità del contesto. Con il tempo e con l'utilizzo, i passaggi diventano progressivamente più chiari. Le operazioni si semplificano e il livello di sicurezza percepita aumenta. L'autonomia digitale non si acquisisce in modo immediato, ma attraverso l'esperienza.

L'autonomia digitale si costruisce attraverso l'uso

Questo modulo rappresenta il punto di partenza. L'identità digitale consente l'accesso. Nel modulo successivo, questa chiave verrà utilizzata per entrare concretamente nei servizi della Pubblica Amministrazione.

LA PUBBLICA AMMINISTRAZIONE DIGITALE: ANPR, INPS E SINFONIA

Ora che hai la tua chiave digitale - SPID o CIE - è ora di usarla per entrare nei portali della Pubblica Amministrazione. In questo modulo affronteremo tre strumenti fondamentali: l'ANPR, il portale online del Comune; l'INPS, per la gestione dei contributi e delle prestazioni sociali; e l'app Sinfonia, il portale della sanità campana. L'obiettivo di questo modulo è renderti capace di svolgere le pratiche più comuni in autonomia, senza dover prendere un giorno di permesso dal lavoro o aspettare ore allo sportello.

ANPR: il Comune che non chiude mai

L'ANPR è l'Anagrafe Nazionale della Popolazione Residente. In parole semplici, è il portale online che contiene i dati anagrafici di tutti i cittadini italiani e che permette di scaricare certificati senza mettere piede in Comune.

Fino a pochi anni fa, per ottenere un certificato di residenza, di nascita o di stato di famiglia, dovevi recarti allo sportello anagrafico, ritirare un numero, aspettare il tuo turno, pagare la marca da bollo e aspettare che l'impiegato compilasse il documento. Oggi, attraverso il sito anpr.interno.it, puoi fare tutto questo in meno di due minuti, dalla comodità di casa tua, a qualsiasi ora del giorno e della notte, compresi i festivi. Il portale ANPR offre gratuitamente certificati di residenza, stato di famiglia, nascita, matrimonio, cittadinanza, godimento dei diritti politici e molti altri. I documenti scaricati in formato PDF hanno pieno valore legale: puoi presentarli ovunque ti venga richiesto un certificato anagrafico, senza bisogno di marche da bollo per i documenti destinati alle Pubbliche Amministrazioni.

Per accedere, vai sul sito anpr.interno.it, clicca su "Accedi ai servizi" e scegli se autenticarti con SPID o con CIE. Una volta dentro, troverai un menu chiaro con tutti i certificati disponibili. Seleziona quello che ti serve, scegli se vuoi scaricare il PDF o riceverlo per email, e il gioco è fatto. Non esiste procedura più semplice.

L'autocertificazione: il tuo diritto che in pochi conoscono

Accanto ai certificati, la legge italiana prevede uno strumento ancora più potente: l'autocertificazione. Si tratta di una dichiarazione scritta in cui il cittadino afferma sotto la propria responsabilità fatti che lo riguardano - come la residenza, il titolo di studio, lo stato civile - senza dover allegare il relativo certificato. Questo diritto è sancito dagli articoli 46 e 47 del Decreto del Presidente della Repubblica n. 445 del 2000. In base a questa legge, la Pubblica Amministrazione e i gestori di pubblici servizi non possono richiedere certificati per fatti che il cittadino può autocertificare: sono obbligati per legge ad

accettare la dichiarazione sostitutiva al posto del documento originale. Questo significa che, nella maggior parte dei casi, non devi nemmeno scaricare il certificato dall'ANPR: ti basta compilare un modulo di autocertificazione, firmarlo e presentarlo. Puoi generare direttamente dal portale ANPR una dichiarazione sostitutiva precompilata con i tuoi dati. Stampala, firmala, e hai un documento con valore legale senza spendere un centesimo e senza fare nemmeno un passo fuori casa.

INPS: non solo pensioni

Molte persone associano l'INPS esclusivamente alle pensioni. In realtà, l'Istituto Nazionale della Previdenza Sociale gestisce una vastissima gamma di prestazioni e servizi che toccano la vita di tutti: dalla maternità alla disoccupazione, dall'assegno unico per i figli all'ISEE, dalle pratiche di invalidità ai bonus di vario genere. L'accesso all'area riservata del portale INPS, raggiungibile all'indirizzo inps.it, avviene sempre tramite SPID o CIE. Una volta dentro, puoi consultare la tua posizione contributiva - cioè tutti i contributi versati nel corso della tua vita lavorativa, fondamentali per il calcolo della pensione - e simulare la data e l'importo della tua futura pensione con lo strumento chiamato "La mia pensione".

Puoi richiedere e visualizzare il tuo ISEE - l'Indicatore della Situazione Economica Equivalente, necessario per accedere a quasi tutti i bonus e le agevolazioni pubbliche - presentando direttamente online la Dichiarazione Sostitutiva Unica (DSU) precompilata, che viene generata automaticamente con i dati già in possesso dell'INPS e dell'Agenzia delle Entrate. Questo ti evita di dover raccogliere decine di documenti e andare da un CAF.

Puoi anche visualizzare e gestire le pratiche attive che ti riguardano, come ad esempio una domanda di disoccupazione (NASpi) o un sussidio in corso, controllarne lo stato e ricevere comunicazioni ufficiali. Il fascicolo previdenziale del cittadino, accessibile dall'area riservata, raccoglie in un unico posto tutta la storia contributiva e tutte le pratiche in corso o concluse.

LO SAPEVI? Puoi simulare la tua futura pensione direttamente dall'area riservata INPS, senza dover fare nessuna telefonata o andare in nessun ufficio. Lo strumento si chiama "La mia pensione futura" ed è gratuito, riservato e aggiornato in tempo reale con i tuoi contributi.

L'app Sinfonia: la sanità campana in tasca

Per i cittadini della Campania, uno strumento particolarmente prezioso è l'app Sinfonia, acronimo di Sistema Informativo Sanità Campania. Si tratta del portale regionale che raccoglie in un'unica interfaccia tutti i principali servizi sanitari digitali.

Tramite Sinfonia puoi prenotare visite specialistiche ed esami attraverso il CUP - il Centro Unico di Prenotazione regionale - selezionando la struttura più comoda, l'orario preferito e confermando l'appuntamento. Non devi più chiamare un numero verde e aspettare in attesa: tutto avviene dall'app, in pochi tocchi. Puoi consultare il tuo Fascicolo Sanitario Elettronico, che contiene referti, esami diagnostici, lettere di dimissione e tutta la tua storia clinica, accessibile solo da te e dal personale sanitario che ti ha in cura. Puoi vedere le ricette elettroniche che il tuo medico ti ha prescritto, con il relativo numero di ricetta elettronica (NRE) da usare in farmacia. Puoi gestire la scelta o il cambio del medico di base o del pediatra. Puoi anche gestire la situazione sanitaria dei tuoi familiari - figli minorenni, genitori anziani - se hai la loro delega.

Sinfonia si scarica gratuitamente dall'App Store (iPhone) o dal Google Play Store (Android) e l'accesso avviene - come ormai capisci - tramite SPID o CIE. Una volta configurata, l'app ti manda notifiche per ricordarti gli appuntamenti e avvisarti quando un referto è disponibile.

E-mail e PEC: la comunicazione ufficiale con gli enti

Un'ultima parola merita la comunicazione digitale con gli enti pubblici. Tutti conoscono l'e-mail ordinaria. La PEC - Posta Elettronica Certificata - è invece l'equivalente digitale di una raccomandata con ricevuta di ritorno: quando mandi un documento a un ente pubblico tramite PEC, hai la prova certificata dell'invio e della ricezione, con valore legale.

Avere una PEC non è obbligatorio per i privati cittadini, ma può essere molto utile per inviare istanze, ricorsi o documentazione agli enti senza dover andare fisicamente allo sportello. I servizi di PEC gratuiti o a basso costo sono disponibili da vari provider italiani. Se non l'hai ancora, valuta di attivarne una: è uno strumento che, una volta provato, difficilmente si abbandona.

PAGOPA: PAGARE LA PA IN MODO SICURO E SEMPLICE

Dopo aver compreso come ottenere la propria identità digitale e come accedere ai principali servizi pubblici, resta da affrontare un passaggio altrettanto importante della vita amministrativa quotidiana: il pagamento.

Multe, tasse, rette scolastiche, ticket sanitari e altri versamenti dovuti alla Pubblica Amministrazione, per lungo tempo, hanno seguito percorsi diversi, con sportelli differenti, procedure poco uniformi e modalità di pagamento non sempre immediate da comprendere. Per il cittadino questo ha significato, molto spesso, disorientamento, perdite di tempo e la necessità di adattarsi ogni volta a regole nuove.

PagoPA nasce proprio per superare questa frammentazione. Si tratta del sistema che ha reso uniforme il pagamento verso la Pubblica Amministrazione, introducendo uno standard unico. Questo significa che, pur cambiando l'ente a cui il pagamento è destinato, il cittadino si muove all'interno di una struttura riconoscibile, leggibile e affidabile. Non si è più davanti a una pluralità di modalità scollegate fra loro, ma a un sistema ordinato, costruito per rendere il pagamento più trasparente, più sicuro e più facile da gestire.

PagoPA, dunque, non è una banca, non è una carta di credito e non è nemmeno un portafoglio digitale. È un sistema di pagamento, uno standard che collega gli strumenti abituali del cittadino, quali conto corrente, home banking, app bancaria, carta, con l'ente pubblico che deve ricevere il versamento. Il pagamento continua a essere effettuato con i mezzi che già si conoscono, ma all'interno di un canale certificato, tracciato e uniforme.

Questo è il punto centrale: non cambia necessariamente lo strumento personale con cui si paga, cambia il sistema che rende il pagamento certo, leggibile e riconosciuto.

Attraverso PagoPA, il cittadino sa con precisione a chi sta pagando e per quale ragione; può scegliere liberamente il canale che preferisce; e ha la garanzia che ogni operazione sia registrata e certificata. È questo che rende PagoPA una vera piattaforma abilitante: non aggiunge complessità, ma mette ordine.

PagoPA non è un luogo in cui pagare, ma il sistema che rende il pagamento verso la Pubblica Amministrazione uniforme, trasparente e sicuro.

Che cos'è PagoPA e perché è diverso da una banca

Per comprendere davvero il valore di PagoPA, occorre soffermarsi sul concet-

to di standardizzazione. In passato, ogni ente pubblico poteva seguire logiche diverse nella gestione dei pagamenti. Questo obbligava il cittadino a imparare ogni volta procedure differenti, spesso poco chiare. Con PagoPA, invece, il principio cambia radicalmente: gli enti pubblici adottano un linguaggio comune, una struttura condivisa, un modello che rende il pagamento riconoscibile in ogni situazione. Questo non significa che il cittadino debba usare un solo canale. Al contrario, uno dei punti di forza del sistema è proprio la libertà di scelta. Il versamento può essere effettuato attraverso l'home banking, tramite una app, mediante l'App IO, oppure utilizzando canali fisici abilitati, come la posta, la tabaccheria o la ricevitoria. Il sistema resta uno solo; è il cittadino a scegliere dove e come utilizzarlo.

In questo senso, si può affermare che lo sportello non è più un luogo fisso e lontano, ma uno strumento che accompagna la persona, adattandosi alle sue abitudini e alle sue possibilità.

Come leggere un avviso di pagamento PagoPA

Uno degli aspetti più importanti per utilizzare PagoPA con sicurezza è imparare a leggere correttamente l'avviso di pagamento. Ogni avviso, sia esso cartaceo o digitale, segue una struttura standard. Questo rappresenta un grande vantaggio, perché consente di orientarsi anche quando si è alla prima esperienza. Pur cambiando l'ente creditore, l'impianto dell'avviso resta leggibile e coerente.

Nell'intestazione compaiono il nome dell'ente, i suoi dati identificativi e le informazioni utili a capire da chi proviene la richiesta di pagamento. Nella parte centrale si trovano invece i dati del debitore, la tipologia del versamento, l'importo dovuto e la relativa scadenza. Ma soprattutto, vi sono due elementi fondamentali, senza i quali il pagamento non potrebbe essere gestito in modo corretto: il QR Code e il Codice Avviso, detto anche IUV.

Il QR Code è il codice quadrato che può essere inquadrato con lo smartphone. La sua funzione è quella di accelerare il pagamento. Una volta letto dall'app della banca o dall'App IO, il sistema riconosce automaticamente i dati dell'operazione: importo, destinatario, causale. In questo modo, non è necessario digitare nulla manualmente. Si tratta della modalità più immediata e veloce. Il Codice Avviso o IUV, cioè l'Identificativo Unico di Versamento, è invece il codice numerico che identifica in maniera precisa quella specifica posizione debitoria. Se il QR Code non può essere utilizzato, oppure se il pagamento viene effettuato da computer o tramite un canale fisico, è questo il dato da inserire o da comunicare. È il riferimento che consente al sistema di individuare la pratica esatta.

Per chi utilizza i servizi a un livello più essenziale, questo significa soprattutto una cosa: anche senza ricorrere direttamente allo smartphone, il pagamento resta possibile, purché si sappia riconoscere e utilizzare correttamente il codice avviso. Per chi invece ha maggiore dimestichezza con gli strumenti digitali, il Codice IUV assume anche un valore successivo al pagamento, perché rappresenta il riferimento utile in caso di verifica o contestazione.

Il QR Code semplifica il pagamento; il Codice IUV identifica con certezza il versamento.

I canali di pagamento: libertà di scelta e continuità del sistema

Uno dei principali vantaggi di PagoPA consiste nel fatto che il cittadino non è obbligato a pagare in un solo modo. Il sistema lascia piena libertà nella scelta del canale, pur mantenendo la stessa struttura di riferimento.

Tra i canali disponibili, un ruolo centrale è occupato dall'App IO. Questa applicazione rappresenta oggi uno dei punti di contatto più importanti tra cittadino e Pubblica Amministrazione. Attraverso IO è possibile ricevere direttamente avvisi di pagamento, comunicazioni istituzionali e notifiche relative a pratiche in corso. Ciò significa che le informazioni non restano disperse tra lettere, e-mail e messaggi diversi, ma vengono raccolte in un unico ambiente digitale, ordinato e facilmente consultabile. All'interno dell'App IO è anche possibile pagare direttamente gli avvisi PagoPA. Una volta effettuato l'accesso con SPID o CIE e collegato il proprio metodo di pagamento, l'operazione può essere completata senza uscire dall'applicazione. Questo rende il processo particolarmente lineare e trasparente.

Accanto all'App IO, resta molto importante anche l'home banking. Quasi tutte le banche mettono a disposizione una sezione dedicata a PagoPA, e questo consente di operare in un ambiente già noto, utilizzando strumenti abituali. Per molti cittadini, questa rappresenta la modalità più familiare. Naturalmente restano disponibili anche i canali fisici, come gli sportelli postali, le tabaccherie e le ricevitorie abilitate. Anche in questi casi, però, si opera sempre all'interno dello stesso sistema standardizzato. Non si tratta dunque di modalità alternative in concorrenza tra loro, ma di porte diverse che conducono al medesimo sistema.

L'App IO: un punto di accesso ordinato ai pagamenti pubblici

L'App IO merita un'attenzione specifica, perché non è soltanto un'applicazione per pagare. È uno strumento che raccoglie e organizza il rapporto digitale con la Pubblica Amministrazione. Attraverso IO, il cittadino riceve messaggi ufficiali, promemoria, avvisi di pagamento e comunicazioni provenienti dagli enti pubblici. Questo rende più semplice seguire le scadenze e riduce il rischio di

smarrire documenti o informazioni importanti.

Quando un avviso PagoPA arriva nell'app, il cittadino non ha più bisogno di cercare altrove i dati necessari. Può visualizzare direttamente il pagamento, scegliere il metodo con cui effettuarlo e completare l'operazione in pochi passaggi. L'applicazione, in questo senso, non solo semplifica il pagamento, ma contribuisce a rendere più ordinata l'intera gestione delle relazioni economiche con la Pubblica Amministrazione.

L'App IO non è solo un canale di pagamento: è uno spazio unico in cui ricevere, leggere e gestire comunicazioni pubbliche e avvisi PagoPA

La sicurezza del sistema e la regola anti-phishing

Quando si parla di pagamenti digitali, la questione della sicurezza è inevitabilmente centrale. Ed è importante chiarire subito un aspetto fondamentale: il sistema PagoPA è sicuro. Il rischio non nasce dalla piattaforma in sé, ma da tentativi esterni di imitare comunicazioni ufficiali e indirizzare il cittadino verso canali falsi.

Queste truffe prendono spesso la forma del phishing. Si riceve un'e-mail o un SMS apparentemente credibile, con un link che invita a pagare o a inserire dati personali. Il messaggio può sembrare urgente, formale, plausibile. In realtà, conduce a un sito falso, costruito con l'obiettivo di sottrarre informazioni o denaro.

Per questa ragione, la regola di protezione più importante è molto semplice: non cliccare mai su link di pagamento ricevuti via e-mail o SMS. Se arriva un avviso di pagamento, il comportamento corretto consiste sempre nell'aprire direttamente l'App IO, entrare nel proprio home banking oppure collegarsi al sito ufficiale dell'ente che ha emesso l'avviso, inserendo lì i dati necessari. In questo modo, il cittadino ha la certezza di utilizzare il canale ufficiale. Il vero PagoPA non impone mai di cliccare su un link esterno per completare un pagamento. Fornisce un avviso, con un QR Code o un Codice IUV, e lascia al cittadino la scelta del canale da utilizzare. Se un messaggio genera dubbio, se il tono appare insolitamente urgente, se il mittente non è chiaramente riconoscibile, è sempre preferibile fermarsi e verificare.

Il pagamento online tramite PagoPA è sicuro. Il rischio nasce solo quando si esce dai canali ufficiali

La ricevuta elettronica: prova del pagamento e strumento di tutela

Ogni volta che un pagamento viene effettuato tramite PagoPA, il sistema genera una ricevuta elettronica. Questo documento non ha un valore inferiore rispetto alla ricevuta cartacea tradizionale. Al contrario, ha pieno valore legale

e costituisce la prova del versamento effettuato. La differenza è che, essendo digitale, può essere conservata con maggiore ordine e facilità. Non si smarrisce come un foglio cartaceo, può essere archiviata in una cartella dedicata e recuperata rapidamente in caso di necessità.

Per questa ragione, è buona norma conservare sempre tutte le ricevute relative ai pagamenti verso la Pubblica Amministrazione. Un modo semplice ed efficace consiste nel creare uno spazio dedicato, ad esempio una cartella denominata “Ricevute PA”, nella quale raccogliere ogni documento ricevuto. Se si utilizza l’App IO, questa operazione risulta ancora più semplice, perché le ricevute restano già associate ai pagamenti effettuati. Conservare la ricevuta non è una formalità. È una forma di tutela. Significa poter dimostrare in qualunque momento che il versamento è stato effettuato, con tutti gli elementi utili a ricostruire l’operazione.

Dal pagamento alla gestione ordinata del proprio portafoglio digitale

Utilizzare PagoPA non significa soltanto eseguire un pagamento. Significa anche imparare a gestire in modo ordinato i propri rapporti economici con la Pubblica Amministrazione. Per alcune persone, il primo obiettivo sarà semplicemente imparare a leggere correttamente un avviso, riconoscendone i codici, l’importo e la scadenza. Per altre, il passaggio successivo sarà utilizzare il QR Code, pagare direttamente dall’App IO o dal proprio home banking e conservare la ricevuta digitale in modo sistematico.

In entrambi i casi, il risultato è lo stesso: trasformare un’operazione che un tempo richiedeva spostamenti, attese e incertezza in una procedura chiara, tracciabile e sotto controllo. Questo è il vero significato del “portafoglio digitale”: non soltanto pagare, ma sapere cosa si sta pagando, come lo si sta pagando e dove ritrovare ogni prova dell’operazione effettuata.

Con questo modulo, il pagamento verso la Pubblica Amministrazione smette di essere un momento separato, confuso o inevitabilmente legato allo sportello fisico. Diventa invece una parte integrata del percorso di autonomia digitale, da gestire con sicurezza, semplicità e consapevolezza.

QUANDO QUALCOSA VA STORTO: PROBLEM SOLVING E FACILITATORI

Questo quarto modulo tratta uno degli aspetti più importanti - e spesso più trascurati - dell'alfabetizzazione digitale: cosa fare quando qualcosa non funziona come dovrebbe. Perché la tecnologia, per quanto ben progettata, non è infallibile. E la differenza tra un cittadino digitale timido e uno autonomo non sta nel non sbagliare mai, ma nel sapere cosa fare quando si incontra un ostacolo.

Il messaggio centrale di questo modulo è chiaro: un errore non è una sconfitta. È un segnale, un indizio. La tecnologia è una strada con delle buche, ma con gli strumenti giusti puoi aggirarle o riempirle.

Il primo passo: l'autovalutazione

Quando qualcosa non va - una pagina web che non si apre, un accesso SPID che fallisce, un file che non si carica - la prima cosa da fare è fermarsi un momento e fare una diagnosi. Non andare nel panico, non chiudere tutto di scatto: osserva cosa sta succedendo.

Distingui innanzitutto tra due tipi di problemi. Il primo tipo è il problema tecnico legato ai dati: il sistema ti dice esattamente cosa c'è di sbagliato. Messaggi come "Password errata", "Formato file non supportato" o "Codice OTP non valido" sono errori descrittivi, e la soluzione è nell'errore stesso. Hai digitato la password sbagliata? Riprova con attenzione, controllando se il blocco maiuscole è attivo. Il file che stai tentando di caricare è in un formato non supportato? Salvalo in un altro formato.

Il secondo tipo è il problema di navigazione: non riesci a trovare un pulsante, non capisci quale opzione scegliere, una pagina sembra diversa da come te l'aspettavi. Questo non è un errore tecnico: è un problema di orientamento nell'interfaccia, e si risolve con un po' di pazienza e, se necessario, chiedendo aiuto.

I trucchi pratici per i problemi più comuni

Esistono alcune azioni che risolvono la maggior parte dei problemi tecnici comuni, indipendentemente dalla specifica operazione che stai cercando di fare.

Se una pagina web non si apre o si apre in modo incompleto, il primo tentativo è sempre aggiornare la pagina premendo il tasto F5 oppure il pulsante con la freccia circolare nella barra del browser. Se questo non basta, prova a usare un browser diverso: ad esempio, se stai usando Google Chrome, prova con Mozilla Firefox o Microsoft Edge. I portali pubblici a volte hanno problemi di

compatibilità con versioni vecchie o poco diffuse di alcuni browser.

Se il codice OTP che ricevi non funziona, verifica che l'orologio del tuo smartphone sia impostato automaticamente: i codici OTP sono sincronizzati con l'ora esatta, e se il tuo telefono è indietro o avanti di qualche minuto, il codice potrebbe già essere scaduto quando lo inserisci. Verifica anche di non star inserendo il codice troppo lentamente: i codici OTP durano in genere 30 secondi. Se hai dimenticato la password SPID, usa sempre la funzione "Password dimenticata" sul sito del tuo gestore di identità. Non tentare più volte con password che non ricordi: dopo un certo numero di tentativi falliti, l'account potrebbe bloccarsi temporaneamente per motivi di sicurezza, e sbloccare un account sospeso richiede più tempo e fatica di quanto sembri. Se una sessione sembra bloccata - stai aspettando da troppo tempo una pagina che non si carica, o un messaggio di "elaborazione in corso" che non finisce mai - controlla la tua connessione a internet. A volte è sufficiente avvicinarsi al router Wi-Fi, o aspettare qualche minuto se c'è un problema temporaneo di connettività. Se usi la rete dati del telefono, verifica di avere campo e che i dati mobili siano attivati.

I Punti di Facilitazione Digitale: la tua rete di supporto

Ma c'è un caso in cui il fai-da-te non basta, e in quel caso la soluzione più intelligente è chiedere aiuto. Chiedere aiuto non è debolezza: è l'azione più efficiente che puoi compiere quando ti trovi di fronte a un problema che supera le tue conoscenze attuali.

Il progetto Dritti al Punto ha creato apposta una rete di supporto umana, distribuita sul territorio campano: i Punti di Facilitazione Digitale. Si tratta di luoghi fisici - biblioteche, centri civici, uffici comunali, spazi dedicati - dove troverai gratuitamente dei Facilitatori Digitali, persone formate appositamente per aiutare i cittadini nell'uso dei servizi digitali pubblici. I Facilitatori non sono tecnici informatici nel senso tradizionale del termine: non devono riparare computer o installare software. Sono guide umane, il cui obiettivo primario non è fare le cose al posto tuo, ma insegnarti a farle da solo. Ogni interazione con un Facilitatore Digitale è pensata per accrescere la tua autonomia, non per aumentare la tua dipendenza da un aiuto esterno.

Per trovare il Punto di Facilitazione più vicino a casa tua, puoi cercare sul sito del progetto Dritti al Punto o chiedere al tuo Comune di riferimento. I servizi sono completamente gratuiti e accessibili senza appuntamento nelle fasce orarie di apertura dello sportello.

Come chiedere aiuto in modo efficace

Quando ti rivolgi a un Facilitatore o a qualunque altra persona per avere sup-

porto su un problema digitale, ci sono alcune informazioni che, se fornite subito, accelerano enormemente la risoluzione del problema.

Descrivi cosa stavi cercando di fare: ad esempio “stavo cercando di scaricare il certificato di residenza dall’ANPR”. Poi descrivi cosa è successo: ad esempio “dopo aver inserito le credenziali SPID, compare un messaggio di errore rosso”. Se il tuo schermo lo consente, scatta uno screenshot del messaggio di errore: è la forma più precisa e univoca di comunicare un problema tecnico. Infine, indica se è la prima volta che ti capita oppure se hai già provato in precedenza. Con queste quattro informazioni – cosa volevo fare, cosa è successo, come appare il problema, se è ricorrente – qualunque Facilitatore potrà aiutarti in modo rapido ed efficace.

Il tuo Kit Digitale: riepilogo del percorso

Sei arrivato alla fine di questa dispensa. Prima di chiuderla, vale la pena fare un passo indietro e vedere insieme quanta strada hai percorso.

Hai imparato cosa sono SPID e CIE, come si ottengono e come si usano in sicurezza. Hai scoperto che i certificati anagrafici si scaricano gratis dal portale ANPR in qualunque momento della giornata, e che l’autocertificazione ha lo stesso valore legale di un certificato ufficiale. Hai capito che l’INPS non è solo l’ente delle pensioni, ma il custode digitale di tutta la tua vita previdenziale e assistenziale. Hai conosciuto l’app Sinfonia, lo strumento che ti permette di prenotare visite, consultare referti e gestire la tua salute digitalmente senza aspettare in fila. Hai capito come funziona PagoPA, come si legge un avviso di pagamento e come difendersi dalle truffe online. E hai imparato che quando qualcosa va storto, il panico non serve: l’autovalutazione e i Facilitatori Digitali sono i tuoi alleati.

I TUOI 4 SUPERPOTERI DIGITALI: 1. SPID e CIE – la tua chiave di accesso a tutti i servizi pubblici digitali; 2. ANPR e INPS – il tuo Comune e la tua previdenza in tasca; 3. PagoPA e App IO – il tuo portafoglio sicuro per i pagamenti alla PA; 4. I Facilitatori Digitali – la tua rete di supporto umana sul territorio

Un consiglio finale: pratica, pratica, pratica

La conoscenza teorica è importante, ma la vera autonomia digitale si conquista con la pratica. Non aspettare di avere un certificato urgente da scaricare per imparare a usare l’ANPR: aprilo oggi, esplora le sezioni, prova a cercare il certificato di residenza. Non aspettare una scadenza di pagamento per imparare PagoPA: scarica l’App IO e configurala con calma, senza fretta.

Ogni piccola esplorazione che fai oggi ti renderà più sicuro la prossima volta. E se sbagli qualcosa? Non succederà nulla di irreparabile: nessun portale pubblico può danneggiare il tuo dispositivo o cancellare i tuoi dati se inserisci informazioni sbagliate in un form. Il peggior scenario possibile è un messaggio di errore, e come abbiamo visto, i messaggi di errore sono semplicemente indicatori che ci guidano verso la soluzione giusta.

Sei un cittadino digitale. Non perché lo dica questa dispensa, ma perché hai dedicato il tuo tempo a imparare come funziona il mondo che ti circonda. Questo è il primo passo, e i passi successivi saranno sempre più facili.

Piccolo glossario dei termini usati nel corso

ANPR - Anagrafe Nazionale della Popolazione Residente

Il portale online del Ministero dell'Interno che contiene i dati anagrafici di tutti i cittadini italiani e permette di scaricare certificati gratuitamente, disponibile all'indirizzo anpr.interno.it.

App IO

L'app ufficiale del Governo italiano per la comunicazione e i pagamenti verso la Pubblica Amministrazione. Gratuita, disponibile per tutti gli smartphone, accessibile tramite SPID o CIE.

Autenticazione a due fattori (2FA)

Sistema di sicurezza che richiede due prove di identità per accedere a un servizio: tipicamente una password (qualcosa che sai) e un codice OTP temporaneo ricevuto via SMS o generato da un'app (qualcosa che hai).

CIE - Carta di Identità Elettronica

La carta d'identità fisica rilasciata dai Comuni italiani, dotata di chip NFC che, abbinato all'app CIE ID, permette di autenticarsi sui portali digitali con il massimo livello di sicurezza.

DigComp 2.2

Il quadro europeo di riferimento per le competenze digitali dei cittadini, elaborato dalla Commissione Europea. Definisce cinque aree di competenza: alfabetizzazione su informazioni e dati, comunicazione e collaborazione, creazione di contenuti digitali, sicurezza, e problem solving.

Fascicolo Sanitario Elettronico

Il registro digitale personale che contiene tutta la storia clinica di un cittadino: referti, esami, ricoveri, vaccini, prescrizioni. Accessibile tramite app Sinfonia in Campania o tramite il portale del proprio Fascicolo Sanitario regionale.

INPS - Istituto Nazionale della Previdenza Sociale

L'ente pubblico che gestisce pensioni, contributi previdenziali, prestazioni di disoccupazione, maternità, invalidità e molte altre forme di sostegno sociale in Italia. Accessibile digitalmente tramite inps.it.

ISEE - Indicatore della Situazione Economica Equivalente

Un indicatore che misura la situazione economica di un nucleo familiare, usato per determinare l'accesso a prestazioni sociali, bonus e agevolazioni. Si calcola presentando la Dichiarazione Sostitutiva Unica (DSU) all'INPS o a un CAF.

OTP - One Time Password

Un codice numerico temporaneo, tipicamente di 6 cifre, valido per soli 30 secondi, usato come secondo fattore di autenticazione. Viene generato dall'app del proprio gestore SPID o inviato via SMS.

PagoPA

La piattaforma nazionale italiana per i pagamenti verso la Pubblica Amministrazione. Non è una banca: è uno standard tecnologico che collega il cittadino e l'ente pubblico attraverso qualsiasi strumento di pagamento bancario o postale.

PEC - Posta Elettronica Certificata

Un tipo speciale di email che ha valore legale equivalente a una raccomandata con ricevuta di ritorno. Usata per inviare documenti ufficiali a enti pubblici con la certezza certificata dell'invio e della ricezione.

Phishing

Una tecnica di truffa online in cui i malintenzionati inviano email o SMS che sembrano provenire da enti ufficiali (banche, INPS, Agenzie delle Entrate) per indurre il destinatario a cliccare su link fraudolenti e inserire i propri dati personali o bancari.

Sinfonia

L'app del Sistema Informativo Sanità Campania, che raccoglie i principali servizi sanitari digitali per i cittadini della regione: prenotazioni, referti, ricette, Fascicolo Sanitario.

SPID - Sistema Pubblico di Identità Digitale

Il sistema di identità digitale italiano che permette ai cittadini di accedere a oltre 3.000 servizi online della Pubblica Amministrazione e di privati accreditati, tramite un unico nome utente e password.

TEMA C

ACCESSO AI SERVIZI ESSENZIALI



LA SANITÀ IN RETE: SALUTE DIGITALE ACCESSIBILE



Digita Facile
Campania

A chi è rivolto questo capitolo

Questo capitolo accompagna il percorso formativo La Sanità in Rete: Salute Digitale Accessibile, sviluppato nell'ambito del progetto Digita Facile Campania, Tema C – Accesso ai Servizi Essenziali. Nasce con un obiettivo preciso: trasformare cittadini dipendenti dagli sportelli fisici in cittadini digitalmente autonomi, capaci di gestire in modo indipendente i propri diritti sanitari attraverso i canali digitali disponibili.

Il percorso copre i quattro ambiti fondamentali della sanità digitale campana. Il primo riguarda l'identità digitale – SPID, CIE, CNS – le chiavi di accesso a tutti i servizi pubblici online. Il secondo introduce il Fascicolo Sanitario Elettronico, l'archivio personale di tutti i propri dati clinici. Il terzo affronta i servizi operativi quotidiani: prenotare una visita tramite CUP, scegliere o cambiare il medico di base, pagare il ticket con PagoPA. Il quarto esplora le esenzioni ticket – per reddito e per patologia – e il meccanismo del rinnovo automatico. Un quinto modulo di approfondimento completa il percorso con uno sguardo al futuro della medicina digitale: telemedicina, intelligenza artificiale e interoperabilità del FSE.

Questo capitolo è pensato per chi non ha una formazione tecnica e non vuole acquistarla: vuole soltanto poter accedere ai servizi sanitari in modo autonomo, senza code, senza carta e senza stress. La difficoltà non è mai la tecnologia in sé: è la paura di sbagliare e la mancanza di una guida. Questo capitolo è la guida.

L'obiettivo di questo corso non è insegnare la tecnologia. È restituire autonomia. Non solo l'utilizzo di un'App, ma gli strumenti per diventare cittadini capaci di esercitare i propri diritti risparmiando tempo e denaro e facendolo senza stress.

Perché la sanità digitale riguarda tutti noi

I vantaggi concreti del digitale nella sanità

Quando si parla di servizi sanitari digitali, la prima reazione di molte persone è la diffidenza: 'Non sono capace', 'Preferisco fare di persona', 'Ho paura di sbagliare'. Queste reazioni sono comprensibili e legittime. Ma vale la pena confrontarle con la realtà concreta di ciò che il digitale offre, in termini pratici e misurabili.

Il risparmio di tempo è il vantaggio più immediato. Gli sportelli delle ASL, dei Cup, degli uffici sanitari hanno orari limitati, spesso incompatibili con i ritmi di lavoro e vita di molti cittadini. Un portale digitale è aperto ventiquattro ore

su ventiquattro, sette giorni su sette: si può prenotare una visita la domenica sera, scaricare un referto il sabato mattina, verificare le proprie esenzioni in qualsiasi momento. Zero trasporto, zero code, zero carta e la ricevuta digitale ha lo stesso valore legale di quella cartacea.

L'autonomia e la trasparenza sono il secondo grande vantaggio. Con i servizi digitali si ha accesso diretto allo stato delle proprie pratiche: non bisogna più sperare che qualcuno richiami, aspettare risposte, dipendere dalla disponibilità di uno sportellista.

Si accede con la propria identità digitale e si vede esattamente cosa c'è, cosa manca, cosa è stato fatto. Il Fascicolo Sanitario Elettronico significa non perdere mai più un referto, non dover trasportare carta in ospedale, avere la propria storia clinica sempre disponibile per qualsiasi medico la necessiti.

L'inclusione e l'accessibilità sono il terzo vantaggio, spesso il meno evidente ma il più profondo. La rivoluzione del touchscreen ha reso la tecnologia accessibile a fasce della popolazione che ne erano sistematicamente escluse: anziani, persone con scarsa familiarità con i computer, abitanti delle aree interne lontane dai centri urbani. Oggi uno smartphone è sufficiente per gestire in autonomia tutti i servizi sanitari che vedremo in questa dispensa.

La bussola DigComp 2.2

Questo percorso formativo usa come riferimento il quadro europeo DigComp 2.2 (Digital Competence Framework) che definisce le competenze digitali fondamentali per il cittadino europeo del ventunesimo secolo. Non è un insieme di nozioni tecniche astratte: è una bussola pratica che aiuta a identificare dove si è e dove si vuole arrivare in termini di autonomia digitale.

Le competenze DigComp rilevanti per questo percorso riguardano principalmente due aree. La prima è l'Alfabetizzazione su informazioni e dati: la capacità di accedere, navigare e interpretare le informazioni disponibili nei portali digitali sanitari. La seconda è la Comunicazione e collaborazione, nello specifico la competenza 2.3 Cittadinanza digitale: la capacità di interagire in modo consapevole, sicuro ed efficace con le istituzioni pubbliche attraverso i canali digitali, esercitando i propri diritti e adempiendo ai propri doveri. Il percorso prevede quattro moduli principali più un modulo di approfondimento finale. Il Modulo 1 introduce SPID, CIE e CNS, le identità digitali. Il Modulo 2 esplora il Fascicolo Sanitario Elettronico. Il Modulo 3 affronta i servizi operativi quotidiani sul portale Sinfonia: CUP, scelta del medico, PagoPA. Il Modulo 4 approfondisce le esenzioni ticket. Il Modulo 5 chiude con uno sguardo al futuro della medicina digitale.

Cosa significa essere cittadino digitale

Essere cittadino digitale non significa essere esperti di informatica. Significa essere capaci di interagire in modo consapevole, sicuro ed efficace con le istituzioni attraverso il web. È una definizione che enfatizza, da un lato, la consapevolezza, ossia sapere cosa si sta facendo, dall'altro la sicurezza, ossia farlo senza rischi. In termini pratici, un cittadino digitale sa accedere ai servizi pubblici online senza dover necessariamente recarsi di persona agli sportelli. Sa riconoscere i canali ufficiali da quelli non affidabili. Sa proteggere le proprie credenziali. Sa fare logout quando termina una sessione su un dispositivo condiviso. Sono competenze concrete, applicabili da subito, che non richiedono anni di studio.

I tre strumenti di autenticazione: SPID, CIE e CNS

Per accedere ai servizi digitali della Pubblica Amministrazione italiana, inclusi tutti i servizi sanitari che vedremo, è necessaria una forma di autenticazione digitale certificata. Esistono tre strumenti principali, con caratteristiche diverse.

SPID – Sistema Pubblico di Identità Digitale: è un'identità digitale virtuale, composta da uno username e una password, gestita da enti privati accreditati dall'Agenzia per l'Italia Digitale – i cosiddetti Identity Provider, tra cui Poste Italiane, Aruba, Sielte, TIM e altri. È disponibile in tre livelli di sicurezza: il Livello 1 usa soltanto username e password; il Livello 2, il più usato e consigliato per il cittadino comune che aggiunge, come secondo fattore, un codice temporaneo OTP inviato via SMS o generato da un'app; il Livello 3 richiede dispositivi fisici di sicurezza aggiuntivi. Per l'accesso ai portali sanitari come Sinfonia, è sufficiente e raccomandato il Livello 2.

CIE – Carta di Identità Elettronica: è il documento d'identità fisico che ha incorporato anche una funzione digitale. È lo strumento di autenticazione che nel medio termine è destinato a diventare il più importante, perché combina la solidità di un documento ufficiale con le funzionalità dell'identità digitale. Per usarla come strumento di accesso ai servizi online è necessario scaricare l'app CIE ID sullo smartphone e completare la registrazione. Offre un livello di sicurezza intrinsecamente elevato.

CNS – Carta Nazionale dei Servizi: è la tessera sanitaria con un chip abilitato. Richiede un codice PIN e, nella maggior parte dei casi, un lettore di smart card fisico collegato al computer. Questo la rende meno pratica rispetto a SPID e CIE per l'uso quotidiano su smartphone, ed è progressivamente meno utilizzata come strumento di autenticazione per i nuovi servizi.

Come ottenere SPID: la procedura passo per passo

Ottenere SPID richiede di seguire alcuni passaggi precisi, ma il processo è stato notevolmente semplificato negli ultimi anni ed è accessibile a chiunque abbia uno smartphone e un documento di identità valido.

Il primo passo è scegliere il proprio Identity Provider, ossia il gestore dell'identità. Tra i più usati: Poste Italiane con PosteID, facilmente accessibile anche agli anziani grazie alla capillare presenza degli uffici postali sul territorio; Aruba, scelta popolare per chi preferisce gestire tutto online; TIM, per i clienti del gestore telefonico.

Il secondo passo è il riconoscimento dell'identità. È il momento in cui si dimostra di essere chi si dichiara di essere. Esistono diverse modalità: di persona presso uno sportello del provider scelto, che è la modalità più semplice per chi non ha dimestichezza con il digitale; via webcam in videochiamata con un operatore; tramite firma digitale; tramite la CIE, usando l'app CIE ID (la modalità più moderna e rapida) per autenticarsi e completare tutto il processo da smartphone.

Una volta completato il riconoscimento, si ricevono le credenziali SPID (username e password) e si può subito configurare il Livello 2 scaricando l'app del provider scelto per ricevere i codici OTP. Da quel momento, SPID è attivo e può essere usato su tutti i siti e portali della PA italiana che lo accettano.

Come attivare CIE: pochi passaggi in massima sicurezza

L'attivazione della CIE come strumento digitale permette oggi di accedere ai servizi online con la stessa semplicità dello SPID, offrendo diverse modalità d'uso. Il primo passo fondamentale è recuperare i codici PIN e PUK (la prima metà di queste cifre viene consegnata allo sportello dell'Anagrafe al momento della richiesta, mentre la seconda viene consegnata insieme alla carta stessa): una volta ottenuti, è necessario scaricare l'app CieID e registrare il documento tramite il sensore NFC dello smartphone. Per rendere l'accesso ancora più fluido, il portale ufficiale consente di attivare le credenziali di livello 1 e 2: questa procedura permette di creare un nome utente e una password associati alla propria identità digitale. In questo modo, per molti servizi della Pubblica Amministrazione non sarà più indispensabile avere la tessera fisica a portata di mano; basterà inserire le proprie credenziali e autorizzare l'accesso tramite una notifica push sull'app o un codice OTP via SMS. Una volta completata questa configurazione, la CIE diventa a tutti gli effetti un sistema versatile e sicuro, pronto per essere utilizzato da computer, tablet o smartphone in pochi istanti.

Dove chiedere aiuto: In Campania, i Punti di Facilitazione Digitale del progetto Digita Facile sono punti di supporto gratuiti dove si può ricevere assistenza per ottenere SPID, attivare la CIE e imparare a usare i servizi digitali. Non è necessario affrontare questo percorso da soli.

L'autenticazione a due fattori: la doppia difesa

Il concetto di autenticazione a due fattori – 2FA, Two-Factor Authentication – è il principio di sicurezza su cui si basano lo SPID e la CIE Livello 2 ed è fondamentale per capire perché è così sicuro.

Il sistema si basa sulla combinazione di due elementi: qualcosa che si sa, ossia la password; qualcosa che si ha, quindi lo smartphone, su cui arriva il codice OTP o c'è l'app che lo genera. Per entrare in un servizio protetto da 2FA non è sufficiente conoscere la password: serve anche avere fisicamente accesso al dispositivo associato all'account. Questo significa che anche se qualcuno riesce a scoprire o rubare la tua password attraverso phishing, spiando lo schermo, o in qualsiasi altro modo, non può comunque accedere al tuo account senza il tuo telefono. La sicurezza è geometricamente superiore rispetto a una semplice password.

L'OTP – One Time Password – è un codice numerico di sei cifre che viene generato in modo casuale e ha una validità di pochi secondi o minuti. Una volta usato, non può essere riutilizzato: anche se qualcuno lo intercettasse nel momento della trasmissione, sarebbe già scaduto prima che possa utilizzarlo. Questa caratteristica lo rende estremamente sicuro contro i tentativi di intercettazione.

Password sicure: come crearle e gestirle

Le password deboli sono ancora oggi una delle principali porte d'ingresso dei criminali informatici nei sistemi digitali. Gli errori più comuni sono quelli che vengono in mente per primi: usare il proprio nome o quello di familiari, la data di nascita, il nome dell'animale domestico, sequenze semplici come '123456' o 'password'. Questi dati sono facilmente individuabili da persone che ci conoscono, ma anche da software automatici che testano milioni di combinazioni al secondo.

Una password sicura deve rispettare tre caratteristiche fondamentali. Deve essere lunga: almeno dieci-sedici caratteri. Deve essere complessa: includere lettere maiuscole e minuscole, numeri e caratteri speciali come @, #, !, %. Deve essere unica: non usare la stessa password per servizi diversi, perché se un servizio viene violato tutti gli account con la stessa password sono immediatamente a rischio. Il metodo della passphrase rende la creazione di pas-

sword sicure e memorizzabili molto più semplice. Si parte da una frase significativa (ad es. ‘Il mio gatto si chiama Poldo!’) e si trasforma in una password usando le iniziali di ogni parola: ImgscP! o, aggiungendo numeri e variazioni, ImgscP!2024. Questa password è lunga, complessa, unica se personalizzata, e facile da ricordare perché è legata a qualcosa di significativo.

Una regola aggiuntiva importante: non salvare le password nel browser, specialmente su dispositivi condivisi. Un browser che ha salvato le credenziali di accesso è accessibile a chiunque usi quel dispositivo dopo di te.

Il logout: chiudere la porta

Il logout, cioè la disconnessione attiva da un servizio digitale, è uno dei comportamenti di sicurezza più semplici e più trascurati. Chiudere la finestra del browser non equivale a fare logout: la sessione può rimanere attiva in background, accessibile al prossimo utente che apre lo stesso browser sullo stesso dispositivo.

Il rischio è reale in tutti i contesti in cui si usa un dispositivo condiviso: un computer di una biblioteca o di un Internet café, il PC di casa che si divide con familiari, lo smartphone prestato per un momento a qualcuno. Se si è effettuato l'accesso a un servizio sanitario, o a qualsiasi altro servizio con dati sensibili e non si fa il logout prima di lasciare il dispositivo, si lascia la propria identità digitale aperta e accessibile al prossimo utente.

La regola è semplice e assoluta: dopo ogni accesso a un servizio digitale, specialmente su dispositivi che non sono esclusivamente propri, cliccare esplicitamente su Logout o Disconnetti prima di chiudere la pagina. È un gesto che richiede tre secondi e che protegge mesi o anni di dati personali e sanitari.

Le trappole del web: phishing e ingegneria sociale

Avere SPID e usare password sicure non è sufficiente se non si conoscono le tecniche usate dai criminali per sottrarre le credenziali. Due tecniche sono particolarmente diffuse nel contesto dei servizi pubblici digitali.

Il phishing è il tentativo fraudolento di ottenere credenziali inviando e-mail o messaggi che imitano comunicazioni ufficiali di banche, enti pubblici, provider di servizi. Il messaggio sembra provenire da Poste Italiane, dall'INPS, dalla propria banca, dall'Agenzia delle Entrate, con loghi ufficiali, toni formali e una richiesta urgente di ‘verificare le credenziali’, ‘confermare i dati’, ‘risolvere un problema’. Il link nel messaggio porta a una pagina che sembra quella ufficiale ma non lo è. La regola è semplice: non cliccare mai su link ricevuti via e-mail o SMS per accedere a servizi sensibili. Aprire sempre il browser e digitare manualmente l'indirizzo del servizio.

L'ingegneria sociale è la manipolazione psicologica per indurre una persona a rivelare informazioni sensibili o a compiere azioni che non avrebbe altrimenti compiuto. Si può manifestare come una telefonata da qualcuno che si spaccia per un tecnico informatico, un operatore INPS, un funzionario dell'ASL. Diffidare sempre di richieste non sollecitate di credenziali, PIN, OTP o installazione di software. Nessuna istituzione legittima chiede mai queste informazioni via telefono o e-mail.

Regola fondamentale: nessuna istituzione pubblica (INPS, ASL, Agenzia delle Entrate, banca) chiede mai credenziali di accesso, password o codici OTP via e-mail, SMS o telefono. Se qualcuno lo chiede, è sempre una truffa.

IL FASCICOLO SANITARIO ELETTRONICO (FSE)

Cos'è il FSE e perché cambia tutto

Il Fascicolo Sanitario Elettronico – FSE – è l'archivio digitale personale e sicuro che raccoglie tutti i dati e i documenti clinici e socio-sanitari generati nel corso della propria storia di salute. Non è una semplice cartella clinica ospedaliera: è qualcosa di più ampio, più completo e più accessibile. È il luogo digitale in cui converge tutta la documentazione sanitaria che ti riguarda, prodotta da qualsiasi struttura sanitaria tu abbia frequentato, tra cui ospedali, ambulatori, laboratori, pronto soccorso, farmacie.

Prima del FSE, il problema della continuità assistenziale era concreto e quotidiano: quando si cambiava medico di base, quando ci si faceva vedere in una struttura diversa, quando si affrontava un'urgenza lontano da casa, la propria storia clinica era nella testa, in qualche cartella di carta a casa, o nella memoria di un singolo medico. Il FSE elimina questo problema: qualsiasi medico autorizzato, in qualsiasi struttura, può accedere alla storia clinica completa in pochi secondi.

Cosa contiene il FSE

I contenuti del Fascicolo Sanitario Elettronico si organizzano in categorie principali, ognuna delle quali corrisponde a un tipo di documento clinico che viene automaticamente aggiunto al fascicolo ogni volta che viene prodotto da una struttura sanitaria.

Referti di laboratorio e esami strumentali: analisi del sangue, esami delle urine, ecografie, radiografie, TAC, risonanze magnetiche e tutti gli altri esami diagnostici. Ogni referto, una volta prodotto, è disponibile nel FSE non appena la struttura lo carica, spesso entro poche ore dall'esame.

Verbali di pronto soccorso: ogni accesso al pronto soccorso genera un verbale che viene inserito nel FSE. In caso di emergenze future, i medici che intervengono possono immediatamente verificare eventuali allergie, farmaci in uso, patologie note.

Lettere di dimissione: il documento che si riceve alla fine di un ricovero ospedaliero, con la diagnosi, le terapie effettuate e le indicazioni per il follow-up, è parte del FSE.

Prescrizioni farmaceutiche e specialistiche: le ricette del medico di base, sia quelle per farmaci che quelle per visite specialistiche, sono visibili nel FSE come ricette elettroniche, con il Numero Ricetta Elettronica (NRE) che serve per prenotare la visita tramite CUP.

Profilo Sanitario Sintetico – Patient Summary: è il documento più importante del FSE: un riassunto essenziale e aggiornato della storia clinica della persona, che include diagnosi principali, allergie, farmaci in uso abituale, vaccinazioni. È quello che in un'emergenza può letteralmente salvare la vita.

Il consenso informato: tu sei il titolare dei tuoi dati

La base legale del FSE è cristallina: il cittadino è l'unico titolare dei dati contenuti nel proprio fascicolo. Non il medico, non l'ASL, non la Regione. Tu. Questo principio ha implicazioni pratiche molto concrete nella gestione dell'accesso. L'alimentazione del FSE, cioè il caricamento dei documenti nel fascicolo da parte delle strutture sanitarie, avviene automaticamente: ogni volta che un laboratorio produce un referto o un ospedale genera una lettera di dimissione, quel documento viene automaticamente inserito nel tuo FSE. Non devi fare nulla per questo. La consultazione del FSE, cioè la possibilità per un operatore sanitario di vedere i documenti contenuti nel tuo fascicolo, è una cosa completamente diversa. Non è automatica. È subordinata al tuo Consenso Informato Esplicito. Senza questo consenso, i medici e i professionisti sanitari non possono accedere ai tuoi documenti pregressi, anche se esistono nel sistema. Sei tu a decidere chi può vedere cosa.

Il consenso può essere fornito in qualsiasi momento, direttamente dall'app Sinfonia nella sezione dedicata alla Gestione Consensi. E, aspetto fondamentale, può essere revocato in qualsiasi momento: se revochi il consenso, gli operatori smettono immediatamente di poter consultare i documenti pregressi. La revoca non cancella i documenti dal fascicolo: li rende soltanto inaccessibili agli operatori.

Esiste anche la funzione di oscuramento: la possibilità di rendere non visibili specifici documenti all'interno del FSE, anche dopo aver fornito il consenso generale. Se ci sono referti particolarmente sensibili relativi a patologie che preferisci non condividere con tutti gli operatori sanitari, puoi oscurarli specificamente, mantenendo il consenso per tutto il resto.

Come accedere al FSE tramite Sinfonia

In Campania, il Fascicolo Sanitario Elettronico è accessibile tramite il portale Sinfonia, che rappresenta il punto di accesso digitale alla sanità campana ed è accessibile tramite sito web o app. L'accesso richiede autenticazione con SPID Livello 2 o CIE: non è accessibile con una semplice email e password, proprio per garantire il massimo livello di sicurezza ai dati sanitari.

I passaggi per il primo accesso al FSE tramite l'app Sinfonia sono i seguenti. Si apre lo store del proprio smartphone (App Store per iPhone, Google Play Store per Android) e si cerca 'Sinfonia Regione Campania'. Si installa l'app, la

si apre, si seleziona il tasto “accedi” e si sceglie la modalità di autenticazione preferita (SPID o CIE). Una volta entrati, si cerca la sezione Fascicolo Sanitario. Al primo accesso, verrà mostrato un banner o una richiesta di attivazione del consenso alla consultazione: è questo il momento in cui si autorizza il sistema a permettere agli operatori sanitari di consultare il fascicolo. Si clicca, si legge l’informativa e si conferma il consenso.

Cosa fare subito: Dopo aver attivato l’accesso al FSE, dedica qualche minuto a esplorare i documenti disponibili. Verifica che i tuoi referti più recenti siano presenti e scaricabili. Controlla che il Profilo Sanitario Sintetico contenga informazioni corrette. Se trovi inesattezze, segnalale al tuo medico di base.

I benefici del FSE per la cura e la sostenibilità

I vantaggi del Fascicolo Sanitario Elettronico non si limitano alla comodità di non portare carta agli appuntamenti medici. Hanno implicazioni più profonde sulla qualità delle cure e sull’efficienza del sistema sanitario.

Per la cura individuale, il FSE permette diagnosi più rapide e accurate: un medico che ha accesso all’intera storia clinica di un paziente può prendere decisioni migliori in meno tempo. Permette la prevenzione proattiva: il medico curante può monitorare l’aderenza alle terapie e intervenire tempestivamente. E in caso di emergenza, quando il paziente non è in grado di fornire informazioni, l’accesso immediato al Profilo Sanitario Sintetico può essere letteralmente salvavita.

Per la sostenibilità del sistema sanitario, il FSE riduce gli esami ripetuti: se un referto è già nel fascicolo, non c’è motivo di ripetere l’esame. Riduce sprechi di carta e logistica. Ottimizza il tempo degli operatori sanitari: il tempo risparmiato nella gestione burocratica può essere dedicato all’assistenza diretta al paziente.

Il futuro del FSE: verso l’interoperabilità

Il Fascicolo Sanitario Elettronico è in costante evoluzione verso quello che viene chiamato FSE 2.0. L’obiettivo nazionale è rendere il FSE consultabile in tutte le Regioni italiane, superando la frammentazione attuale in cui ogni Regione ha il proprio sistema. L’obiettivo europeo va oltre: la possibilità, in futuro, di accedere ai propri dati sanitari anche quando si è in un altro paese dell’Unione Europea, in vacanza, in viaggio di lavoro, o in caso di emergenza sanitaria all’estero; l’attivazione del Profilo Sanitario Sintetico, nonché la creazione di un Taccuino in cui il cittadino potrà annotare alcuni dati specifici (come, ad esempio, gli effetti collaterali di un farmaco) e contribuire ad implementare il FSE; l’attivazione delle deleghe digitali.

CUP, SCELTA DEL MEDICO E PAGOPA: SINFONIA AL LAVORO

Il portale Sinfonia: lo sportello sanitario in tasca

Sinfonia è il portale digitale della Regione Campania che connette il cittadino ai servizi amministrativi e informativi della sanità regionale. Disponibile come sito web e come app per smartphone, è accessibile tramite SPID Livello 2 o CIE e offre ventiquattro ore su ventiquattro, sette giorni su sette, tutte le funzioni che fino a pochi anni fa richiedevano code agli sportelli.

Le funzioni principali di Sinfonia includono: prenotare visite ed esami specialistici tramite il CUP regionale; consultare il Fascicolo Sanitario Elettronico con referti, esami e lettere di dimissione; vedere ricette e promemoria elettronici; gestire il proprio medico di base o pediatra; gestire anche i profili di familiari, figli minori, genitori anziani; ricevere notifiche su appuntamenti, esiti di esami e promemoria sanitari, pagare il ticket per le prestazioni sanitarie in totale sicurezza, verificare le proprie esenzioni per patologia e autocertificare esenzioni per reddito, consultare il corredo vaccinale e molto altro.

Scegliere e cambiare il medico di base

Il medico di medicina generale – MMG – o il pediatra di libera scelta – PLS per i bambini – sono le figure centrali del sistema sanitario di base: il punto di primo contatto con il servizio sanitario, il professionista che conosce la storia clinica del paziente e coordina il percorso di cura. Ogni cittadino ha il diritto di scegliere e di cambiare liberamente il proprio medico di base.

Fino a non molti anni fa, questa operazione richiedeva di recarsi fisicamente agli sportelli ASL con il modulo cartaceo, fare la fila, aspettare la verifica della disponibilità e confermare la scelta. Con Sinfonia, l'intera procedura si fa in pochi clic con effetto immediato.

I passaggi per la scelta o il cambio del medico tramite Sinfonia sono i seguenti. Si accede al portale con SPID o CIE. Si seleziona il proprio profilo. Si va alla sezione dedicata alla Scelta/Revoca MMG/PLS. Si usano i filtri disponibili (disponibilità libera, comune o area geografica, nome del medico) per identificare il professionista desiderato.

Si conferma la scelta: la modifica ha effetto immediato nel sistema. Se il nome del medico desiderato non appare tra i risultati selezionabili, il motivo più probabile è che abbia raggiunto il massimale di pazienti nel suo ambito territoriale, non che ci sia un problema tecnico.

Prenotare una visita specialistica con il CUP Web

Il Centro Unico di Prenotazione – CUP – è il sistema tramite cui si prenotano le visite specialistiche e gli esami diagnostici nel Servizio Sanitario Nazionale.

La versione web del CUP, accessibile tramite Sinfonia, permette di prenotare direttamente dal proprio smartphone o computer, senza telefonate, senza code, con piena visibilità delle disponibilità.

Per utilizzare il CUP Web su Sinfonia è necessario un solo elemento: il Numero Ricetta Elettronica (NRE) che si trova sulla ricetta elettronica che il medico di base rilascia quando prescrive una visita o un esame. Non serve il codice fiscale, non serve il numero di tessera sanitaria: basta l'NRE.

I passaggi per la prenotazione sono i seguenti. Si accede a Sinfonia e si va alla sezione CUP o Prenotazioni. Si inserisce il Numero Ricetta Elettronica (NRE) oppure, più semplicemente, sull'app Sinfonia si seleziona la ricetta con cui si intende prenotare la prestazione direttamente dal proprio FSE. Si usa il filtro di prossimità per scegliere l'ASL, l'ospedale o il poliambulatorio preferito. Il sistema mostra la prima data disponibile, garantendo il rispetto dei tempi massimi di attesa previsti dalla normativa. Si sceglie la data e l'orario preferiti e si conferma la prenotazione. Si riceve una notifica di conferma.

Una volta prenotato, l'appuntamento è gestibile interamente da Sinfonia: lo si può visualizzare nella lista degli appuntamenti futuri, modificare la data o l'orario se necessario, o disdire se non si può più andare. Questo ultimo punto è importante: disdire un appuntamento che non si può rispettare, con un anticipo adeguato di almeno 48 ore, è un atto di rispetto verso gli altri cittadini. La mancata disdetta toglie la possibilità a un altro paziente bisognoso di usufruire di quell'appuntamento.

Come gestire la ricetta elettronica: Quando il medico di base prescrive una visita o un esame, la ricetta elettronica sarà caricata in automatico nel FSE. In questo modo è possibile effettuare la prenotazione direttamente cliccando sulla ricetta (o inquadrando il codice a barre) - nell'app - o inserendo il NRE manualmente sul web e procedendo seguendo le indicazioni della piattaforma.

PagoPA: il pagamento del ticket in sicurezza

PagoPA è il sistema di pagamento elettronico standard della Pubblica Amministrazione italiana. Non è una banca, non è una carta di credito: è un'infrastruttura, uno standard unico, che permette di effettuare pagamenti verso qualsiasi ente pubblico in modo sicuro, tracciabile e certificato.

Per il cittadino, PagoPA significa che il pagamento del ticket sanitario, così come qualsiasi altro pagamento verso la PA, può essere effettuato da qualsiasi dispositivo, in qualsiasi momento, usando qualsiasi metodo di pagamento disponibile: carta di credito, carta di debito, bancomat, conto corrente, portafogli digitali. Non è necessario recarsi fisicamente alla cassa del poliambu-

latorio, fare la fila al Postamat o all'ATM, o avere in mano denaro contante. Lo strumento principale dell'avviso PagoPA sono due codici. Il QR Code (il quadrato a scacchiera che si trova sulla ricevuta o sull'avviso di pagamento) funziona come un teletrasporto: si inquadra con la fotocamera dello smartphone e in un secondo l'app riconosce automaticamente l'importo, il destinatario e la causale del pagamento. Il Codice IUV, ossia il codice Identificativo Univoco di Versamento, è il codice numerico alternativo al QR Code: se il QR non funziona o si è su un PC senza fotocamera, si digita questo codice nel proprio home banking per trovare la pratica e procedere al pagamento.

La ricevuta digitale generata al termine di un pagamento tramite PagoPA ha pieno valore legale: è equiparata a tutti gli effetti alla ricevuta cartacea e va conservata, in formato digitale, nella cartella delle e-mail o dei download dello smartphone. Non è necessario stamparla, a meno che la struttura sanitaria non la richieda esplicitamente per una procedura specifica.

Il pagamento tramite PagoPA garantisce la piena tracciabilità della transazione attraverso il Codice IUV: in caso di contestazioni o verifiche, è sempre possibile dimostrare l'avvenuto pagamento con certezza assoluta. Conserva sempre la ricevuta digitale del pagamento.

ESENZIONI TICKET: CONOSCERE I PROPRI DIRITTI

Il ticket sanitario e il principio di equità

Il ticket sanitario è la quota di partecipazione alla spesa che il cittadino è chiamato a pagare per determinate prestazioni del Servizio Sanitario Nazionale: visite specialistiche, esami di laboratorio, esami strumentali. Il suo obiettivo è duplice: contribuire al finanziamento del SSN e disincentivare l'uso inappropriato delle prestazioni; evitare che risorse limitate vengano consumate da richieste non necessarie.

Le esenzioni dal ticket sono le eccezioni a questa regola: misure di equità pensate per garantire che il fattore economico non sia mai un ostacolo all'accesso alle cure necessarie. Il principio è semplice e fondamentale: nessuno dovrebbe rinunciare a una cura medica perché non può permettersi il ticket. Le esenzioni esistono proprio per garantire questo.

Un dato importante da conoscere: molte persone che hanno diritto a un'esenzione non la utilizzano semplicemente perché non sanno di averne diritto. Il risultato è che pagano un ticket di cui sono legalmente esenti. Questa dispensa vuole anche correggere questa situazione: al termine di questo modulo, sarai in grado di verificare se hai diritto a un'esenzione e come farla valere.

Due tipi di esenzione: patologia e reddito

Esistono due categorie fundamentalmente diverse di esenzione, con logiche, durate e ambiti di applicazione completamente distinti.

Esenzioni per patologia: riguardano specifiche malattie croniche o rare riconosciute a livello nazionale. Chi è affetto da diabete, ipertensione, cardiopatie, tumori, malattie rare certificate e molte altre, ha diritto all'esenzione dal ticket per tutte le prestazioni direttamente collegate alla cura e al monitoraggio di quella specifica patologia. L'esenzione non copre tutto: una persona esente per diabete non è automaticamente esente per una visita ortopedica, a meno che non ci sia un collegamento clinico documentato.

La validità è generalmente indefinita o molto lunga, perché la patologia cronica non cambia nel tempo. Il codice di esenzione per patologia viene assegnato dall'ASL dopo attestata certificazione da parte del medico specialista di struttura pubblica dopo la diagnosi.

Esenzioni per reddito: riguardano la situazione economica e anagrafica del cittadino. I codici nazionali vanno da E01 a E04 e corrispondono a categorie specifiche. E01 è per soggetti con meno di 6 anni o più di 65 con reddito familiare fiscale sotto una soglia determinata. E02 è per i disoccupati con basso reddito. E03 è per i titolari di assegno (pensione) sociale. E04 è per i titolari di pensione minima con più di 60 anni. Queste esenzioni coprono quasi tutte le

prestazioni di specialistica ambulatoriale e diagnostica – un ambito molto più ampio delle esenzioni per patologia. La loro validità è però limitata nel tempo, tipicamente un anno, perché la situazione economica può cambiare.

Il ruolo del MEF e il rinnovo automatico

Il Ministero dell'Economia e delle Finanze – MEF – è il soggetto che, attraverso l'Agenzia delle Entrate, detiene i dati fiscali e reddituali di tutti i cittadini italiani. Ogni anno, il MEF trasmette alle Regioni – e quindi alle ASL – le liste aggiornate dei cittadini che risultano automaticamente esenti in base alle dichiarazioni dei redditi dell'anno precedente.

Il meccanismo del rinnovo automatico funziona così: se sei presente nelle liste del MEF come avente diritto all'esenzione E01, E03 o E04, la tua esenzione viene rinnovata automaticamente dall'ASL ogni anno. Non devi fare nulla, non devi recarti allo sportello, non devi presentare documenti: il sistema aggiorna automaticamente la tua esenzione e la si può verificare sull'app Sinfonia in Salute.

C'è però un'eccezione importante a questa comodità del rinnovo automatico, e merita attenzione speciale: l'esenzione E02 per disoccupazione. Lo stato di disoccupazione deve essere certificato attivamente dal cittadino, perché il MEF non dispone automaticamente di questa informazione nel modo in cui dispone dei dati reddituali. Se sei disoccupato e hai diritto alla E02, devi presentare ogni anno la documentazione che attesta il tuo stato di disoccupazione, tipicamente all'ASL, o effettuare una nuova autocertificazione sul portale Sinfonia.

Attenzione: se sei disoccupato e pensi di avere automaticamente l'esenzione E02, verifica la situazione sul portale Sinfonia. A differenza delle altre esenzioni per reddito, la E02 non si rinnova automaticamente e richiede la tua azione attiva ogni anno per rimanere valida.

Come verificare le proprie esenzioni

Le esenzioni attive sulla propria tessera sanitaria sono consultabili direttamente tramite il portale Sinfonia, nella sezione dedicata alle Esenzioni. Accedendo con SPID o CIE, è possibile vedere in tempo reale quali esenzioni sono attive, la loro scadenza e l'ambito di applicazione.

Se si ritiene di avere diritto a un'esenzione che non risulta attiva, i canali per ottenerla dipendono dal tipo. Per le esenzioni per patologia, il percorso parte dalla certificazione di struttura pubblica che attesta la patologia: le informazioni trasmesse all'ASL sono necessarie per l'attivazione del codice di esenzione. Per le esenzioni per reddito, il processo è in alcuni casi automatizzato per E01, E03 ed E04 – ma richiede che si siano presentate le dichiarazioni dei redditi in modo corretto, perché è da quelle che il MEF ricava le informazioni. Per la E02, la documentazione deve essere presentata attivamente.

Le nuove frontiere: telemedicina, AI e interoperabilità

La digitalizzazione della sanità non si ferma agli strumenti che abbiamo visto finora: è un processo in costante evoluzione che sta ridisegnando profondamente il modo in cui i cittadini accedono alle cure e in cui il sistema sanitario funziona.

Telemedicina e telesalute: la telemedicina non è semplicemente una videochiamata con il medico. È un ecosistema di servizi che include consulti a distanza, monitoraggio remoto di parametri vitali attraverso dispositivi wearable (frequenza cardiaca, glicemia, pressione arteriosa) e teleassistenza per pazienti cronici. Per le aree geografiche isolate, come molte delle aree interne della Campania dove opera questo progetto formativo, la telemedicina può risolvere il problema dell'accesso alle cure specialistiche: un paziente anziano di un comune montano non deve più fare ore di viaggio per una visita di controllo che può essere gestita a distanza.

Intelligenza Artificiale e diagnostica: l'AI non sostituisce il medico, ma lo affianca in alcune funzioni specifiche in modo straordinariamente efficace. Nell'analisi di immagini diagnostiche (radiografie, TAC, risonanze, screening oncologici) i sistemi di AI sono già in grado di identificare pattern e anomalie con una precisione e una velocità che superano le capacità umane in contesti specifici. Il beneficio per il cittadino è concreto: diagnosi più veloci e più accurate, meno errori diagnostici, percorsi di cura più personalizzati.

FSE interoperabile: oggi il Fascicolo Sanitario Elettronico funziona prevalentemente a livello regionale. L'obiettivo nazionale è renderlo consultabile in tutte le Regioni italiane: un paziente campano che si trova in emergenza a Milano potrà avere il suo FSE accessibile ai medici del Pronto Soccorso lombardo. L'obiettivo europeo è ancora più ambizioso: l'accesso ai propri dati sanitari anche in altri paesi dell'Unione Europea.

La sostenibilità della sanità digitalizzata

La digitalizzazione della sanità non è sostenibile solo perché elimina la carta: è sostenibile perché ottimizza le risorse umane ed economiche in modo sistemico. I benefici si misurano su più dimensioni.

Il riuso del dato è il vantaggio più strutturale: un dato clinico, una volta generato e inserito nel FSE, è riutilizzabile in tutti i contesti futuri senza dover essere ricreato. Questo elimina i costi di esami ripetuti, riduce il carico di lavoro degli operatori sanitari, riduce i rischi di errori che possono derivare da informazioni incomplete o contraddittorie.

La riduzione degli errori amministrativi è un altro beneficio concreto: meno burocrazia manuale significa meno probabilità di errori nella trascrizione, nella comunicazione tra strutture, nella gestione delle pratiche. L'automazione dei processi routinari, come il rinnovo delle esenzioni o la trasmissione automatica dei referti nel FSE, libera tempo prezioso del personale sanitario. L'ottimizzazione del personale è forse il beneficio più significativo per la qualità delle cure: il tempo risparmiato dall'operatore ASL che non deve più gestire code fisiche, compilare moduli cartacei e rispondere a telefonate per informazioni disponibili online è tempo che può essere dedicato all'assistenza diretta al paziente. La digitalizzazione non toglie lavoro alle persone: sposta il loro lavoro verso attività a più alto valore umano.

L'autonomia digitale è un muscolo che va allenato. La tecnologia cambia velocemente, e le competenze digitali si ottengono e si mantengono con la pratica. Questa dispensa e questo corso sono un punto di partenza: l'obiettivo è costruire le basi per un'autonomia digitale che cresce nel tempo, con l'uso quotidiano.

I tre impegni del cittadino digitale

Al termine di questo percorso, i concetti fondamentali si condensano in tre impegni concreti che sintetizzano quanto appreso.

Conosco la mia chiave. Comprendo la differenza tra SPID, CIE e CNS e so quale scegliere in base al mio dispositivo e alle mie esigenze. So come ottenere SPID, come usarlo con l'autenticazione a due fattori, e come mantenerlo sicuro. So che la CIE è il documento fisico con funzione digitale integrata e che nel futuro avrà sempre più importanza.

Uso l'armatura forte. Le mie password sono lunghe, complesse e uniche per ogni servizio. Non le salvo nel browser, non le condivido con nessuno, non le digito su richiesta di terzi via telefono o email. Riconosco i tentativi di phishing e di ingegneria sociale e so come reagire: non clicco su link sospetti, non installo software su richiesta, non fornisco credenziali a nessuno che me le chieda.

Chiudo la porta. Eseguo il logout al termine di ogni sessione su un servizio digitale, specialmente su computer o dispositivi che non sono esclusivamente miei. So che chiudere la finestra del browser non è equivalente al logout. Questo gesto semplice protegge l'intera mia identità digitale e tutti i dati sanitari che vi sono associati.

Essere un cittadino digitale autonomo non significa sapere tutto. Significa sapere dove cercare, come accedere, e quando chiedere aiuto. La rete di supporto del progetto Digita Facile Campania è disponibile per accompagnarti in ogni passo di questo percorso.

Test di autovalutazione finale

Indica la risposta corretta. Le risposte si trovano in fondo alla sezione.

1. Qual è la definizione più accurata di 'cittadino digitale'? a) Chi usa prevalentemente lo smartphone. b) Chi sa navigare sui social media in sicurezza. c) Chi è capace di interagire in modo consapevole, sicuro ed efficace con le istituzioni attraverso il web.
2. Qual è il livello SPID consigliato per l'accesso ai portali istituzionali come Sinfonia? a) Livello 1: solo credenziali. b) Livello 2: credenziali più codice temporaneo OTP o App. c) Livello 3: dispositivo fisico di sicurezza.
3. L'obiettivo principale del Fascicolo Sanitario Elettronico è: a) L'accesso gratuito a farmaci e visite. b) Garantire la continuità assistenziale in qualsiasi luogo di cura. c) Archiviare tutti i documenti sanitari in formato cartaceo.
4. Chi è l'unico titolare dei dati contenuti nel FSE? a) Il Medico di Base. b) L'ASL Regionale. c) Il Cittadino/Assistito.
5. L'esenzione E02 per disoccupazione non si rinnova automaticamente perché: a) La disoccupazione non è considerata una patologia cronica. b) Lo stato di disoccupazione deve essere certificato attivamente dal cittadino ogni anno. c) I disoccupati non pagano tasse e quindi non figurano nelle liste MEF.
6. Quale azione è essenziale dopo aver utilizzato un servizio sanitario su un computer condiviso? a) Cancellare la cronologia del browser. b) Eseguire sempre il LOGOUT attivo dal sistema. c) Disattivare la connessione Wi-Fi.
7. Quale identificativo è indispensabile per prenotare una visita specialistica tramite il CUP su Sinfonia? a) Il codice fiscale. b) Il numero di cellulare. c) Il Numero di Ricetta Elettronica (NRE).
8. Il sistema PagoPA è: a) Un'app bancaria privata. b) Uno standard unico di pagamento elettronico verso la PA, sicuro e tracciabile. c) Un servizio di pagamento alternativo a PayPal.

Risposte: 1-c / 2-b / 3-b / 4-c / 5-b / 6-b / 7-c / 8-b

Autovalutazione delle competenze DigComp 2.2

Compila questa scheda prima e dopo il percorso formativo. Per ciascuna voce, indica il tuo livello su una scala da 1 a 5: 1 = non mi sento ancora in grado, 5 = mi sento completamente autonomo.

Area di Competenza	Prima (1-5)	Dopo (1-5)
So cosa sono SPID, CIE e CNS e quando usarli		
So come ottenere SPID e attivare il Livello 2		
Comprendo il meccanismo dell'autenticazione a due fattori		
So creare una password sicura e gestirla correttamente		
So cosa è il FSE e come accedervi tramite Sinfonia		
Comprendo il Consenso Informato e so come gestirlo		
So prenotare una visita specialistica tramite CUP su Sinfonia		
So come cambiare il medico di base tramite Sinfonia		
So pagare un ticket sanitario tramite PagoPA		
Conosco le esenzioni ticket a cui potrei avere diritto		

Glossario essenziale

ASL (Azienda Sanitaria Locale): ente pubblico che gestisce i servizi sanitari di base nel territorio di competenza: medici di base, poliambulatori, sportelli amministrativi, esenzioni.

Autenticazione a due fattori (2FA): sistema di sicurezza che combina qualcosa che sai – la password – con qualcosa che hai – lo smartphone per il codice OTP. Anche conoscendo la password, senza il dispositivo non è possibile accedere.

CIE (Carta di Identità Elettronica): documento d'identità fisico con funzione digitale incorporata. Con l'app CIE ID è utilizzabile come strumento di autenti-

cazione per i servizi pubblici online.

CNS (Carta Nazionale dei Servizi): tessera sanitaria con chip abilitato. Richiede PIN e lettore di smart card. Progressivamente sostituita da SPID e CIE.

Codice IUV (Identificativo Univoco di Versamento): codice numerico presente sull'avviso PagoPA che permette di identificare univocamente un pagamento. Alternativo al QR Code per i pagamenti da PC o home banking.

Consenso Informato: autorizzazione esplicita fornita dal cittadino per permettere agli operatori sanitari di consultare i documenti del proprio FSE. Obbligatorio per accedere alla storia clinica completa, revocabile in qualsiasi momento.

CUP (Centro Unico di Prenotazione): sistema per la prenotazione di visite specialistiche ed esami diagnostici nel SSN. Accessibile via web tramite il portale Sinfonia con il solo Numero Ricetta Elettronica.

Esenzione ticket: esonero dal pagamento del ticket sanitario per determinate prestazioni, basato su criteri economici (reddito: codici E01-E04) o clinici (patologia). Misura di equità per garantire l'accesso alle cure.

FSE (Fascicolo Sanitario Elettronico): archivio digitale personale e sicuro di tutti i dati e documenti clinici e socio-sanitari del cittadino. Garantisce la continuità assistenziale. Il cittadino è l'unico titolare dei propri dati.

Identity Provider: ente privato accreditato da AgID che gestisce le identità SPID degli utenti. Tra i principali: Poste Italiane, Aruba, TIM, Sielte.

Logout: azione di disconnessione attiva da un servizio digitale. Essenziale dopo ogni accesso su dispositivi condivisi. Chiudere la finestra del browser non equivale al logout.

MEF (Ministero dell'Economia e delle Finanze): ministero che, tramite l'Agenzia delle Entrate, gestisce i dati reddituali e trasmette alle ASL le liste dei cittadini aventi diritto alle esenzioni per reddito. Responsabile del rinnovo automatico delle esenzioni E01, E03, E04.

NRE (Numero Ricetta Elettronica): identificativo univoco della ricetta elettronica emessa dal medico di base. Indispensabile per prenotare visite ed esami tramite il CUP Web su Sinfonia.

Oscuramento: funzione del FSE che permette al cittadino di rendere non visibili specifici documenti agli operatori sanitari, anche dopo aver fornito il consenso generale alla consultazione.

OTP (One Time Password): codice temporaneo a sei cifre valido per pochi secondi, usato nel secondo fattore di autenticazione dello SPID Livello 2. Inviato via SMS o generato dall'app del provider.

PagoPA: infrastruttura standard per i pagamenti elettronici verso la Pubblica Amministrazione italiana. Garantisce sicurezza, tracciabilità e la piena validità legale della ricevuta digitale.

Patient Summary (Profilo Sanitario Sintetico): documento riassuntivo della storia clinica contenuto nel FSE, con diagnosi principali, allergie, farmaci in uso e vaccinazioni. Fondamentale in caso di emergenze.

Phishing: tentativo fraudolento di sottrarre credenziali tramite comunicazioni che imitano enti ufficiali. Regola: mai cliccare link in email/SMS per accedere a servizi sensibili; digitare sempre l'indirizzo manualmente.

Sinfonia: portale digitale della Regione Campania per l'accesso ai servizi sanitari: FSE, CUP, scelta del medico, esenzioni, PagoPA. Accessibile via app o web con SPID Livello 2 o CIE.

SPID (Sistema Pubblico di Identità Digitale): identità digitale virtuale composta da username e password, gestita da Identity Provider accreditati. Disponibile in tre livelli di sicurezza; il Livello 2 è quello consigliato per l'accesso ai servizi sanitari.

Telemedicina: insieme di servizi sanitari a distanza: consulti via videochiamata, telemonitoraggio di parametri vitali, teleassistenza. Particolarmente utile per aree geograficamente isolate e pazienti cronici.

INTERVISTE DAP



Digita Facile
Campania

LA VOCE DI FRANCESCO

Come descriverebbe la sua esperienza durante il corso?

Frequento l'ultimo anno di scuola superiore e ho partecipato al corso sull'accesso ai servizi digitali presso il Palazzo della Cultura di Vallo della Lucania. Pensavo di assistere a una lezione come tante, invece mi sono trovato in un incontro molto coinvolgente, dove è stato facile seguire gli argomenti e sentirsi parte attiva delle attività proposte.

Qual è stato il momento che ricorda con più piacere?

Sicuramente il role-playing nato durante il corso. La formatrice mi ha coinvolto direttamente in una dimostrazione pratica e, quasi senza accorgersene, quello che doveva essere un semplice esempio è diventato un momento divertente e partecipato che ha coinvolto tutta la sala. Questo mi ha aiutato a comprendere meglio gli argomenti e a viverli in modo molto più concreto.

Come valuta i contenuti affrontati durante il corso?

Li ho trovati interessanti e utili. Molti dei servizi presentati fanno ormai parte della vita quotidiana e conoscere questi strumenti permette di essere più autonomi e consapevoli, soprattutto per noi giovani che ci prepariamo a entrare nel mondo del lavoro e dell'università.

Come descriverebbe la formatrice?

È riuscita fin da subito a creare un'atmosfera positiva e partecipata, coinvolgendo persone di età molto diverse tra loro. Nessuno si è sentito escluso o semplice spettatore. La sua capacità di dialogare con il pubblico ha reso tutto più naturale e interessante. Anche il Direttore Annapaola Voto ha partecipato con grande spontaneità al role-playing, entrando nel gioco con noi e contribuendo a rendere il momento ancora più coinvolgente. Vedere una figura istituzionale partecipare con semplicità e disponibilità ha reso l'esperienza ancora più piacevole e ha aiutato tutti a sentirsi a proprio agio.

Consiglierebbe questa esperienza ad altre persone?

Assolutamente sì. È stata un'esperienza utile, diversa dal solito e capace di far imparare cose nuove in modo leggero e coinvolgente.

Parteciperebbe ad altre iniziative simili?

Certamente. Mi piacerebbe partecipare ad altri incontri come questo perché permettono di imparare in modo pratico, confrontarsi con gli altri e scoprire strumenti che possono essere davvero utili nella vita di tutti i giorni.

LA VOCE DI ANGELINA

Come descriverebbe la sua esperienza durante il corso?

All'inizio sono arrivata con molta diffidenza. Pensavo che il digitale fosse qualcosa di troppo complicato per me e avevo paura di non riuscire a seguire. Invece ho trovato un ambiente accogliente, dove nessuno si sentiva giudicato e dove ogni domanda aveva la sua importanza.

Qual è stata la cosa che l'ha colpita di più?

Mi ha colpito il modo in cui gli argomenti sono stati spiegati. Non ho avuto la sensazione di assistere a una lezione, ma di partecipare a una conversazione. Anche temi che mi sembravano difficili sono diventati comprensibili e vicini alla vita di tutti i giorni.

Come valuta i contenuti del corso?

Molto utili e concreti. Ho scoperto servizi che non conoscevo e ho capito che molte operazioni che prima affidavo ad altri posso imparare a gestirle personalmente. È stato un percorso pratico, che mi ha fatto sentire più sicura.

Come descriverebbe la formatrice?

Con pazienza, disponibilità e grande capacità di ascolto. Mi sono sentita accompagnata passo dopo passo, senza fretta e senza imbarazzo per le mie difficoltà. Questo ha fatto davvero la differenza.

Consiglierebbe questa esperienza ad altre persone?

Absolutamente sì. Penso che molte persone abbiano le mie stesse paure e che potrebbero trarre grande beneficio da un percorso come questo.

Parteciperebbe ad altri corsi?

Senza dubbio. Anzi, mi piacerebbe approfondire altri argomenti legati al digitale, perché oggi mi sento molto più curiosa e fiduciosa di quando sono entrata in aula la prima volta.

LA VOCE DI ANTONIO

Come descriverebbe la sua esperienza durante il corso?

Mi chiamo Antonio, vivo a Montella e nella vita ho sempre fatto l'agricoltore. Ho trascorso gran parte delle mie giornate tra i campi e il lavoro all'aria aperta, per questo il mondo del digitale mi è sempre sembrato qualcosa di lontano dalla mia realtà. Quando ho deciso di partecipare al corso avevo molti dubbi, perché pensavo che queste cose fossero troppo complicate per me. Invece, incontro dopo incontro, ho capito che bastava qualcuno che le spiegasse con semplicità e pazienza.

Qual è stata la cosa che ricorda con più soddisfazione?

Il momento che ricordo con più piacere è quando sono riuscito a scaricare da solo un certificato. Può sembrare una cosa da poco, ma per me è stato importante. Fino a quel momento, quando avevo bisogno di un documento, andavo sempre negli uffici oppure chiedevo aiuto a qualcuno. Riuscire a farlo da solo mi ha dato una grande soddisfazione e mi ha fatto capire che potevo imparare molto più di quanto pensassi.

Come valuta gli argomenti trattati durante il corso?

Li ho trovati molto utili perché riguardavano situazioni che possono capitare a tutti. Non erano spiegazioni teoriche o difficili da capire, ma cose pratiche che possono aiutare nella vita di tutti i giorni. Ho scoperto servizi che non conoscevo e strumenti che possono farmi risparmiare tempo e spostamenti.

Come descriverebbe la formatrice?

Molto disponibile e paziente. Non mi sono mai sentito in difficoltà nel fare domande, nemmeno quando pensavo che fossero banali. Ha spiegato tutto in modo chiaro e con parole semplici, mettendo tutti a proprio agio.

Consiglierebbe questa esperienza ad altre persone?

Sì, soprattutto a chi pensa di essere troppo grande per imparare queste cose o a chi, come me, ha sempre svolto un lavoro lontano dal mondo della tecnologia. Con il giusto aiuto si può imparare e diventare più autonomi.

Parteciperebbe ad altri corsi?

Sicuramente sì. Questo corso mi ha fatto cambiare idea sul digitale. Oggi lo vedo come uno strumento utile e mi piacerebbe continuare a conoscere altri servizi che possono semplificare la vita quotidiana.

LA VOCE DI ROSETTA

Come descriverebbe la sua esperienza durante il corso?

Sono Rosetta, un'insegnante in pensione della provincia di Benevento. Ho partecipato al corso presso una Cooperativa Sociale di Comunità del territorio perché sentivo il bisogno di comprendere meglio alcuni strumenti digitali che ormai fanno parte della vita quotidiana. Tra gli impegni della famiglia e le attenzioni che dedico ogni giorno a mio figlio, per me era importante acquisire maggiore autonomia nella gestione di alcune pratiche e imparare a utilizzare servizi che fino a quel momento avevo sempre guardato con un po' di diffidenza.

Qual è stata la scoperta più importante che ha fatto durante il percorso?

La scoperta più significativa è stata sicuramente il Fascicolo Sanitario Elettronico. Ne avevo sentito parlare, ma non avevo mai compreso davvero quanto potesse essere utile. Durante il corso ho scoperto che molti referti e documenti sanitari erano già disponibili online e facilmente consultabili. Per chi, come me, si trova spesso a gestire aspetti legati alla salute propria e dei familiari, è stato rassicurante capire di poter avere tutto a disposizione in modo semplice e ordinato.

Come valuta i contenuti affrontati durante il corso?

Li ho trovati molto utili perché concreti e vicini alle esigenze delle persone. Ogni argomento era spiegato con chiarezza e collegato a situazioni reali, rendendo facile comprendere l'utilità dei servizi presentati e la loro applicazione nella vita quotidiana.

Come descriverebbe la formatrice?

Preparata, disponibile e soprattutto molto attenta alle persone. Ha saputo creare un clima sereno e accogliente, mettendo tutti a proprio agio. Non ho mai avuto timore di fare domande o di chiedere spiegazioni, perché ogni difficoltà veniva affrontata con pazienza e disponibilità.

Consiglierebbe questa esperienza ad altre persone?

Sì, senza alcun dubbio. Credo che molte persone della mia generazione possano trarre beneficio da percorsi come questo, che aiutano a sentirsi più sicuri e autonomi nell'utilizzo dei servizi digitali.

Parteciperebbe ad altri corsi?

Certamente. Questa esperienza mi ha fatto capire che non è mai troppo tardi per imparare e che il digitale, se spiegato nel modo giusto, può diventare un valido aiuto nella vita di tutti i giorni.

LA VOCE DI PASQUALE

Come descriverebbe la sua esperienza durante il corso?

Mi chiamo Pasquale, vivo a Monteforte e faccio l'artigiano. Non sono una persona molto abituata a usare il computer o i servizi digitali e, fino a poco tempo fa, preferivo sbrigare tutto di persona. Quando ho saputo di questo incontro ho deciso di partecipare per curiosità, senza sapere bene cosa aspettarmi.

Qual è stata la cosa che l'ha colpita di più?

La scoperta di PagoPA. Non ne avevo mai sentito parlare e pensavo che per molti pagamenti fosse ancora necessario andare agli sportelli o perdere tempo tra uffici e attese. Durante l'incontro ho capito che esiste un modo molto più semplice per fare queste operazioni e che, con pochi passaggi, si può pagare in sicurezza senza muoversi da casa.

Come valuta i contenuti affrontati durante il corso?

Li ho trovati molto utili perché riguardavano cose che possono servire davvero a tutti. Non erano argomenti lontani dalla vita quotidiana, ma strumenti concreti che permettono di risparmiare tempo e di semplificare molte attività.

Come descriverebbe la formatrice?

La cosa che mi è piaciuta di più è stata la capacità di coinvolgere tutte le persone presenti. Fin dall'inizio si è creato un clima sereno e spontaneo, in cui ognuno si sentiva libero di intervenire, raccontare la propria esperienza e fare domande. Anche chi all'inizio era più timido o diffidente è stato coinvolto nella discussione. Con il suo modo di spiegare, semplice e vicino alle persone, è riuscita a farci seguire gli argomenti con interesse e partecipazione, trasformando l'incontro in un momento piacevole oltre che utile.

Consiglierebbe questa esperienza ad altre persone?

Sì, sicuramente. Penso soprattutto a chi, come me, ha sempre pensato che il digitale fosse complicato o poco adatto alle proprie abitudini. Partecipare a un incontro del genere aiuta a vedere le cose in modo diverso e a capire che molti strumenti sono più semplici di quanto si immagini.

Parteciperebbe ad altri corsi?

Certamente. Questa esperienza mi ha fatto scoprire servizi che non conoscevo e mi ha dato più fiducia nell'utilizzo degli strumenti digitali. Per questo parteciperei volentieri ad altri incontri e ad altre attività.

CANNALONGA (SA)

Formatrici: Letizia e Paola

Cittadino : SIG VITTORIO CLASSE 1950

F: Signor Vittorio, ci troviamo qui, presso la biblioteca Comunale di Cannalonga, allora “il DIGITALE INSIEME è FACILE “?

V: Apre molte strade, anche io che ho una certa età ho ritenuto utilissima l'opportunità di utilizzo del digitale.

F: All'esito dei corsi di oggi, quindi, possiamo dire che si sente più addentrato nel mondo del digitale?

V: Più invogliato e più tranquillo nell'usarlo, in realtà io frequento anche il Punto di FACILITAZIONE DIGITALE spesso presente nel nostro comune grazie al quale avevo già scaricato l'APP CIE E l'APP IO, ma con il corso formativo di oggi ho potuto approfondire delle tematiche che mi interessavano.

F: Ci seguirà nei prossimi corsi?

V: Assolutamente sì, spero ce ne sarà presto un altro e coinvolgerò anche alcuni “giovani” della mia età che sono ancora scettici alla sola parola “digitale”. Complimenti alle formatrici!

F: Grazie ed a presto!

ALFANO (SA)

Formatrici: Letizia e Paola

Servizio Civile: Aylana e Giuseppe

F: Ragazzi, la tematica che avete seguito nei corsi di formazione di oggi è quella del lavoro. Pensate dopo i corsi di oggi che ci sia correlazione tra il mondo del lavoro ed il digitale?

A: Assolutamente sì, innanzitutto è una tematica fondamentale per noi che ci affacciamo al mondo del lavoro ed il corretto utilizzo del digitale, ci permette, a partire dalla creazione del curriculum fino alla scoperta delle piattaforme su cui candidarlo, passando per i portali dedicati alle politiche attive del lavoro, di prepararci e candidarci in maniera adeguata.

G: Le dritte ricevute nei corsi di formazione sono state molto utili e ne farò tesoro perché mi hanno redarguito su alcuni errori che avevo fatto compilando il mio primo curriculum e mi hanno aperto gli occhi sulle possibilità che posso sfruttare con il digitale per il mondo del lavoro.

F: voto alle formatrici?

A: 10 e lode!

G: 10 e lode!

F: Torniamo a casa con un bel 20!

ROCCADASPIDE (SA)

Formatrici: Letizia e Paola

Servizio Civile: David e Maria Francesca

F: Ragazzi qual è la vostra impressione sui corsi di oggi sulla sanità in rete?

D: Particolarmente interessante anche perché come servizio civile siamo stati coinvolti anche nel progetto di telemedicina e grazie ai corsi di stamattina in particolare anche all' utilizzo dell' APP Sinfonia Salute ci sentiamo maggiormente pronti ad aiutare i cittadini .

MF: Saper cambiare il medico, piuttosto che prenotare una visita anche ad una terza persona, o pagare il ticket risparmiando tempo e facendolo con una semplice APP è un valore aggiunto che abbiamo oggi grazie ai vostri corsi formativi per noi stessi e per aiutare gli altri.

D: abbiamo anche imparato l'importanza nel mettere verde al fascicolo sanitario!

F: Spiegateci meglio però per coloro che non sanno cosa sia.

D: Sull'APP Sinfonia Salute è possibile dare il consenso (mettere verde, perché è rosso quindi negato a tutti) alla consultazione del Fascicolo Sanitario da parte degli operatori Sanitari.

F: ed a cosa serve dare questo consenso? Aiuta a cosa?

MF: consultare il fascicolo sanitario permette agli operatori sanitari di conoscere immediatamente la storia clinica del paziente ed intervenire in maniera tempestiva!

F: bravissimi ragazzi, siete stati molto attenti! Vi aspettiamo al prossimo corso!

D e MF: Speriamo si terrà presto!

POLLA (SA)

Formatrici: Letizia e Paola

Progetto GOL: Loredana e Pina

F: Oggi a Polla grande partecipazione, in particolare del progetto GOL, Loredana, Pina, cosa vi è rimasto dei corsi formativi di oggi?

L: Molte cose non sapevamo nemmeno che esistessero, vi ringraziamo per questa occasione formativa gratuita che stiamo avendo, per noi è un valore aggiunto essere formati su queste tematiche relative al digitale.

P: Siete delle formatrici al top perché con un linguaggio semplice, simpatico e soprattutto con tanta pazienza siete riuscite a farci comprendere delle tematiche importanti relative al digitale che possono aiutarci nella vita di tutti i giorni.

F: Vi aspettiamo ai prossimi corsi?

L e P: Assolutamente sì!

OTTATI (SA)

Formatrici: Letizia e Paola

Cittadino: Antonio

F: Antonio, secondo te qual è stato il valore aggiunto per te per i cittadini di Ottati, di questi corsi sulla digitalizzazione?

A: Io che sono restio a questi strumenti tecnologici ne sto ricavando tantissimo ausilio. Credo che corsi del genere andrebbero fatti con maggiore frequenza e sarebbe utile estenderli anche ai dipendenti comunali. Oggi la tematica delle truffe, mi ha orientato tantissimo sui pericoli del web e mi sento più sicuro nella navigazione.

F: Voto alle formatrici?

A: Non è facile trovare persone che riescono a trasmettere tematiche così importanti e che un po' spaventano chi come me non è natio digitale, con empatia e professionalità: Voto dieci e lode!

SAN RUFO (SA)

Formatrici: Letizia e Paola

Cittadino: Carmelo

F: Signor Carmelo, cosa mi dice dei corsi di oggi? Le sono sembrati utili?

C: Intanto io sono stato a mio agio, voi siete state delle ottime guide nel farci muovere in questo mondo così complesso e pericoloso per noi anziani che è quello del digitale.

F: L'aspettiamo ai prossimi corsi?

C: Con vero piacere!

LAUREANA CILENTO (SA)

Formatrici: Letizia e Paola

Assessore: Anna

F: Assessore, abbiamo tenuto qui a Laureana molti corsi, ottima partecipazione soprattutto del servizio civile e progetto GOL, insomma qual è stato l'impatto sulla cittadinanza?

A: Abbiamo aderito a questo progetto con grande entusiasmo, i corsi sono stati apprezzati dalla comunità, soprattutto dalla comunità più giovane, quindi l'età media dei partecipanti ai corsi è stata molto bassa perché i giovani sono maggiormente attratti dal digitale, questo però non toglie che anche la popolazione meno giovane abbia aderito al progetto. Hanno apprezzato tutte le tematiche proposte ma in particolare l'accento va posto sulla tematica del lavoro. Questi corsi sono stati molto importanti perché i ragazzi hanno appreso le tecniche di redazione di un curriculum ed hanno utilizzato questi curriculum redatti per candidarsi e so che qualcuno è stato anche contattato per dei colloqui! Quindi grazie e complimenti a voi Formatrici e speriamo ci siano altre occasioni formative a supporto della cittadinanza.

F: Grazie a voi per averci ospitato!

MOIO DELLA CIVITELLA (SA)

Formatrici: Letizia e Paola

Sindaco di Moio

F: Sindaco, all'esito di questi corsi di formazione sul digitale che riscontro ha avuto dalla popolazione? Anzi, abbiamo avuto l'onore di avere lei oggi, che ha partecipato in prima persona, quindi esperienza diretta.

S: E' stata un'esperienza molto positiva e sta già tornando utile a molte persone che hanno partecipato i quali si sono fatti anche da portavoce. Non vi nascondo che stesso io ne sono stato sorpreso dai contenuti. In particolare non conoscevo l'APP Sinfonia Salute e basti pensare che a volte per un semplice cambio del medico si perdono anche 2 ore ed invece si può fare questa operazione tranquillamente con il telefonino dal divano di casa.

F: Quindi vero il nostro slogan " IL digitale insieme è facile?"

S: ..(risata) PIU' FACILE!

SALA CONSILINA (SA)

Formatrici: Letizia e Paola

Cittadino: Pasquale

F: Signor Pasquale, classe 1955, ci racconti la sua esperienza relativamente ai nostri corsi di formazione che ha seguito

P: Prima di tutto tanta gratitudine perché mettete a proprio agio con il vostro modo di fare nonché con la vostra preparazione, ad ogni domanda fatta da noi c'è stata una pronta risposta vostra. Anzi posso dire una cosa voi oggi avete innescato un fattore demoltiplicatore. Che significa voi avete insegnato a me ed io con gratitudine sento di insegnarlo agli altri. E poi devo farvi i complimenti perché siete sicure di ciò che dite e trasmettete questa sicurezza anche agli altri, oltre ad essere 2 formatrici che letteralmente strappate l'empatia.

F: Signor Pasquale siamo noi che ringraziamo lei e speriamo di vederci ai prossimi corsi.

LAUREANA CILENTO (SA)

Formatrici: Letizia e Paola

Servizio Civile: Francesca

Form: Francesca, ci hai seguite in tutti i corsi, donaci un tuo giudizio!

Francesca: Questi corsi, in particolare modo quelli sul lavoro, sono stati molto utili. Direi fondamentali per capire molte cose nell'ambito lavorativo a partire da come presentare un CV ed anche strumenti digitali per facilitare la digitalizzazione e l'applicazione al lavoro.

Form: Voto alle formatrici!

Francesca: Sinceramente il mio voto è un 5 stelle perché siete preparate, simpatiche e molto disponibili!

MONTANO ANTILIA (SA)

Formatrici: Letizia e Paola

Progetto GOL e Servizio Civile: Marika ed Annapia

F: ragazze cosa abbiamo imparato oggi?

M: Che per immetterci nel mondo del lavoro innanzitutto dobbiamo avere un curriculum convincente che supera le ATS ed arriva almeno ai selezionatori!

A: Ho appreso di piattaforme Dove è possibile candidare il mio curriculum ed anche siti dove poter perfezionare gratuitamente le mie Skills.

F: Ci sarete ai prossimi corsi ?

A e M: Assolutamente sì!

VALLO DELLA LUCANIA (SA)

Formatrici: Letizia e Paola

Studenti scuola Cenni: Carlo e Leonardo

F: Ragazzi, allora, cosa ci dite dei corsi di oggi?

C: In verità pensavamo che fossero dei corsi noiosi, ma ci siamo dovuti ricredere oltre al fatto che abbiamo imparato come creare e presentare un CV vincente e dove andarlo a candidare. Molto utile e simpatico è stato anche simulare colloqui per la ricerca del lavoro.

M: È stato molto interessante anche riflettere sulle opportunità di lavoro del nostro territorio.

F: insomma siamo state meno noiose di quanto immaginate?

C e M: speriamo che si farà presto un altro corso!

GIUNGANO (SA)

Formatrici: Letizia e Paola

Servizio Civile: Noemi

F: Noemi, lasciaci un feedback relativo ai corsi che hai seguito!

N: Ho risolto molti dubbi relativi al digitale ed ho iniziato a pensarlo non solo come utilizzo di Social ma come un vero e proprio strumento per facilitare la vita come ad esempio l'utilizzo dell'app sinfonia salute e per migliorarmi come ad esempio le piattaforme sul lavoro!

F: voto alle formatrici ?

N: preparate ed empatiche, farei almeno un corso al mese con voi!

CAMPAGNA (SA)

Formatrici: Letizia e Paola

Progetto Gol: Annamaria

F: Annamaria, ritieni sia stato utile seguire questo corso di formazione ?

A: Assolutamente sì, in generale piace formarmi su tutto ciò che non conosco ma nello specifico oggi ho avuto direttamente oltre al lato teorico formativo anche il lato pratico che da subito applicherò per facilitarmi la vita con il digitale come avete detto voi!

F: Speriamo di averti ai prossimi corsi, grazie !



IFEL - Istituto per la Finanza e l'Economia Locale della Regione Campania

Sede legale

Via Santa Lucia, 81 – 80132

Sede operativa

Via Generale Giordano Orsini, 40 – 80132 Napoli

Tel.: 0811-8901333

Centro Direzionale Isola E3 – 80143 Napoli

Tel.: 081-18893690

info@ifelcampania.it

[**www.ifelcampania.it**](http://www.ifelcampania.it)