FONDO per la REPUBBLICA DIGITALE

IFEL ISTITUTO PER LA FINANZA E L'ECONOMIA LOCALE DELLA CAMPANIA

DISPENSA DIDATTICA

TEMA B
SICUREZZA E USO CONSAPEVOLE DEI SERVIZI DIGITALI

SICUREZZA DIGITALE E ALFABETIZZAZIONE SU INFORMAZIONE E DATI

Digita Facile Campania

"DIGITA FACILE CAMPANIA" Bando "DRITTI AL PUNTO" è un progetto selezionato e sostenuto dal Fondo per la Repubblica Digitale Impresa sociale

Presentazione della dispensa

Questa dispensa 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 percorso 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.

> Questa dispensa è pensata per essere usata, non solo letta. Tienila vicina 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.

MODULO 1
Fondamentali della Navigazione Digitale

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 trumenti 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 traccianti 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: amaz0n.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.

MODULO 2
Fondamentali della Comunicazione Digitale

Obiettivi del modulo

Al termine di questo modulo padroneggerai le funzionalità essenziali dell'email, 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 destinatari. 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.

MODULO 3 **Creatività Digitale**

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 condivisione 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 email 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.

APPROFONDIMENTO 1

Difendere i propri account: password e autenticazione

La password: prima linea di difesa

Le password sono le chiavi di accesso ai nostri spazi digitali: email, 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 particolare 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.

APPROFONDIMENTO 2

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.

> 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.

APPROFONDIMENTO 3

Intelligenza Artificiale e informazione: le nuove sfide

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.

APPROFONDIMENTO 4

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 conoscevamo 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.

Note finali e 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: gpdp.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.

Questa dispensa è un materiale didattico prodotto nell'ambito del progetto Digita Facile Campania, promosso dalla Fondazione IFEL Campania e selezionato e sostenuto dal Fondo per la Repubblica Digitale – Impresa sociale, nell'ambito del bando "Dritti al Punto", in collaborazione con il Dipartimento per la Trasformazione Digitale.

Per ulteriori informazioni sul progetto e per conoscere il calendario dei prossimi corsi, visita la pagina dedicata su ifelcampania.it/eventi.