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

OPPORTUNITÀ DELLA RETE E CYBERSECURITY

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 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.

Perché la sicurezza digitale riguarda tutti

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.

MODULO 1

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'email, 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.

MODULO 2

Difendere il dispositivo: sistemi di protezione passiva

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. Entrambi 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 attivamente. 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 messaggi 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.

MODULO 3

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**, ossira 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.

MODULO 4

La Cassaforte Digitale: backup e protezione dei dati

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 batte 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 antivirus 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.

Competenza	Prima	Dopo
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.

Note finali

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.

Il progetto si rivolge a cittadine e cittadini delle aree interne della Campania con l'obiettivo di rafforzare le competenze digitali nelle fasce di popolazione più esposte al rischio di esclusione, promuovendone l'autonomia e l'inclusione. Il percorso formativo si ispira al quadro europeo DigComp 2.2.

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