REGIONE LAZIO

ROMA

PUNTO DIGITALE

Guida Completa alla Sicurezza Informatica

Proteggere i tuoi dispositivi, dati e identità digitale

A cura di

CODICI
Centro per i Diritti del Cittadino

Finanziato dall'Unione europea
NextGenerationEU

REPUBBLICA DIGITALE

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Capitolo 1

Cos'è la Sicurezza Informatica e perché è importante

La sicurezza informatica, o cybersecurity, è l'insieme di tecnologie, processi e pratiche progettate per proteggere dispositivi, reti, programmi e dati da attacchi, danni o accessi non autorizzati. In un mondo sempre più digitale, dove lavoro, comunicazioni, acquisti e servizi essenziali dipendono da internet, la sicurezza informatica non è più un lusso ma una necessità fondamentale.

IL MONDO DIGITALE E I SUOI RISCHI

Ogni giorno utilizziamo dispositivi connessi a internet: smartphone, computer, tablet, smart TV e persino elettrodomestici intelligenti. Ognuno di questi dispositivi rappresenta un potenziale punto di accesso per malintenzionati che vogliono rubare dati personali, informazioni bancarie, o semplicemente danneggiare i nostri sistemi.

I rischi sono molteplici e in costante evoluzione. Virus e malware possono infettare i dispositivi rallentandoli o rendendoli inutilizzabili. Gli hacker possono rubare password e identità digitali per accedere ai conti bancari o compiere frodi a nostro nome. I ransomware possono criptare tutti i nostri file chiedendo un riscatto per restituirceli. Le violazioni di dati aziendali possono esporre milioni di informazioni personali di utenti inconsapevoli.

PERCHÉ TUTTI SIAMO A RISCHIO

Un errore comune è pensare "a me non succederà mai" o "non ho nulla di interessante da rubare". La realtà è che tutti siamo potenziali bersagli. Gli attacchi informatici moderni sono in gran parte automatizzati: software malevoli scansionano continuamente internet cercando vulnerabilità, senza distinguere tra utenti importanti e comuni cittadini. Anche se non hai grandi somme in banca, i tuoi dati personali hanno valore per i criminali che possono usarli per compiere frodi o rivenderli sul dark web.

LA SICUREZZA COME RESPONSABILITÀ PERSONALE

La sicurezza informatica non può essere delegata completamente a software antivirus o a esperti. Ogni utente deve assumere un ruolo attivo nella protezione dei propri dati e dispositivi. Questo significa sviluppare consapevolezza dei rischi, adottare

comportamenti sicuri, utilizzare gli strumenti appropriati e mantenersi costantemente aggiornati sulle nuove minacce.

I PILASTRI DELLA SICUREZZA INFORMATICA

La sicurezza informatica si basa su tre principi fondamentali: confidenzialità (solo le persone autorizzate possono accedere ai dati), integrità (i dati non devono essere modificati o danneggiati), e disponibilità (i dati e i sistemi devono essere accessibili quando servono). Tutti i consigli e le pratiche di questa guida mirano a garantire questi tre elementi.

Capitolo 2

Virus, Malware e minacce digitali

Comprendere le diverse tipologie di minacce informatiche è il primo passo per difendersi efficacemente. Ogni tipo di attacco ha caratteristiche specifiche e richiede approcci di protezione differenti.

I VIRUS INFORMATICI

I virus sono programmi dannosi che si replicano inserendosi in altri file o programmi. Come i virus biologici, si diffondono da un computer all'altro attraverso file condivisi, allegati email o dispositivi USB infetti. Una volta attivati, possono danneggiare file, rallentare il sistema o aprire porte ad altri attacchi. I virus necessitano dell'azione dell'utente per attivarsi, ad esempio cliccando su un allegato o eseguendo un file scaricato.

I TROJAN (CAVALLI DI TROIA)

I trojan si mascherano da software legittimo o utile per ingannare l'utente e farsi installare volontariamente. Il nome deriva dal cavallo di Troia della mitologia greca: sembrano innocui ma nascondono funzioni dannose. Possono rubare password, registrare i tasti premuti sulla tastiera, attivare webcam e microfoni a nostra insaputa, o creare backdoor che permettono agli hacker di controllare il computer da remoto.

I RANSOMWARE

Tra le minacce più pericolose degli ultimi anni, i ransomware criptano tutti i file presenti sul computer rendendoli inaccessibili. Sullo schermo compare poi un messaggio che chiede il pagamento di un riscatto, solitamente in criptovalute, per ottenere la chiave di decriptazione. Anche pagando non c'è garanzia di recuperare i file, e il pagamento finanzia ulteriori attività criminali.

GLI SPYWARE E ADWARE

Gli spyware sono programmi che raccolgono informazioni sulle attività dell'utente senza il suo consenso: siti visitati, acquisti effettuati, password digitate. Gli adware mostrano pubblicità invasive e indesiderate, spesso rallentando il sistema. Anche se meno dannosi di virus o ransomware, rappresentano comunque violazioni della privacy e possono esporre a ulteriori minacce.

I ROOTKIT

I rootkit sono strumenti sofisticati che permettono agli attaccanti di mantenere accesso privilegiato a un sistema nascondendosi dal sistema operativo e dai software di sicurezza. Sono particolarmente difficili da rilevare e rimuovere perché operano a livello profondo del sistema.

COME AVVIENE L'INFEZIONE

Le vie di infezione più comuni sono: allegati email dannosi che sembrano documenti legittimi, download da siti non sicuri o da reti peer-to-peer, chiavette USB infette, sfruttamento di vulnerabilità in software non aggiornati, pubblicità malevole su siti web (malvertising), e installazione di software pirata contenente malware nascosto.

Capitolo 3

Password sicure e gestione delle credenziali

Le password sono la prima linea di difesa per proteggere i nostri account online. Purtroppo, sono anche spesso l'anello più debole della catena di sicurezza a causa di scelte inadeguate da parte degli utenti.

L'IMPORTANZA DI PASSWORD FORTI

Una password debole è come una porta di casa chiusa con un lucchetto facilmente scassinabile. Gli hacker usano software automatizzati che possono provare milioni di combinazioni al secondo per indovinare le password. Password comuni come "123456", "password", o il proprio nome seguito dall'anno di nascita possono essere violate in pochi secondi.

CARATTERISTICHE DI UNA PASSWORD SICURA

Una password veramente sicura deve essere lunga almeno 12-15 caratteri, meglio ancora se 20 o più. Deve contenere una combinazione di lettere maiuscole e minuscole, numeri e simboli speciali. Non deve contenere parole del dizionario, informazioni personali facilmente reperibili come nomi di familiari, date di nascita, o squadre del cuore. Deve essere unica e diversa per ogni servizio importante che utilizzi.

GLI ERRORI PIÙ COMUNI

Molte persone commettono errori che compromettono gravemente la sicurezza. Usare la stessa password per più servizi è estremamente pericoloso: se un sito viene violato e la password rubata, tutti gli altri account con la stessa password sono compromessi. Scrivere le password su post-it attaccati al monitor o in file non protetti sul desktop è come lasciare le chiavi di casa sotto lo zerbino. Usare password troppo semplici pensando "tanto chi vuoi che mi hackeri" sottovaluta gravemente i rischi.

I GESTORI DI PASSWORD (PASSWORD MANAGER)

La soluzione ideale per gestire decine di password complesse e diverse è usare un gestore di password. Questi programmi creano, memorizzano e inseriscono automaticamente password sicurissime per ogni sito. Servizi affidabili includono LastPass, 1Password, Bitwarden, o Dashlane.

Devi ricordare solo una password principale (che deve essere particolarmente robusta) e il software gestisce tutte le altre. Molti browser moderni includono anche gestori di password integrati.

L'AUTENTICAZIONE A DUE FATTORI (2FA)

Anche la password più forte può essere rubata. L'autenticazione a due fattori aggiunge un secondo livello di sicurezza richiedendo qualcosa che hai (oltre a qualcosa che sai). Tipicamente è un codice temporaneo inviato via SMS o generato da un'app come Google Authenticator o Microsoft Authenticator. Anche se un hacker ottiene la tua password, non potrà accedere al tuo account senza il secondo fattore. Attiva sempre la 2FA su servizi critici come email, banca, social media e cloud storage.

QUANDO CAMBIARE LE PASSWORD

Non è più considerato necessario cambiare le password regolarmente se sono già forti e uniche. Tuttavia, devi cambiarle immediatamente se: ricevi notifica di violazione di dati da un servizio che usi, sospetti che qualcuno possa averle scoperte, hai usato un computer pubblico o una rete Wi-Fi non sicura per accedere, o se scopri accessi non autorizzati ai tuoi account.

Capitolo 4

Proteggere il computer e i dispositivi

I dispositivi che utilizziamo quotidianamente – computer, smartphone, tablet – contengono una quantità enorme di informazioni personali e sensibili. Proteggerli adeguatamente è fondamentale.

ANTIVIRUS E ANTIMALWARE

Un buon software antivirus è essenziale su computer Windows. Oggi Windows Defender, integrato in Windows 10 e 11, offre una protezione solida e gratuita che per la maggior parte degli utenti è sufficiente. Se preferisci alternative, considera Bitdefender, Kaspersky, Norton o Avast. L'importante è sceglierne uno affidabile e mantenerlo sempre aggiornato. Su Mac il rischio malware è statisticamente inferiore ma non inesistente, quindi anche gli utenti Mac dovrebbero considerare un antivirus.

FIREWALL

Il firewall è una barriera che monitora e controlla il traffico di rete in entrata e uscita dal tuo dispositivo, bloccando connessioni sospette. Windows e macOS includono firewall integrati che dovrebbero essere sempre attivi. Verifica nelle impostazioni di sicurezza che il firewall sia effettivamente abilitato.

AGGIORNAMENTI DI SISTEMA E SOFTWARE

Uno degli aspetti più trascurati ma fondamentali della sicurezza è mantenere aggiornato il sistema operativo e tutti i programmi installati. Gli aggiornamenti non servono solo ad aggiungere funzionalità ma, soprattutto, a correggere vulnerabilità di sicurezza che potrebbero essere sfruttate dagli attaccanti. Abilita gli aggiornamenti automatici quando possibile e non rimandare l'installazione degli aggiornamenti di sicurezza.

SMARTPHONE E TABLET

Gli smartphone contengono spesso più dati personali dei computer ma ricevono meno attenzione in termini di sicurezza. Installa app solo dagli store ufficiali (Google Play Store o Apple App Store), verifica le autorizzazioni che le app richiedono prima di installarle, mantieni il sistema operativo aggiornato, usa un codice di blocco schermo forte o la biometria, e considera l'installazione di app di sicurezza anche su mobile.

BACKUP REGOLARI

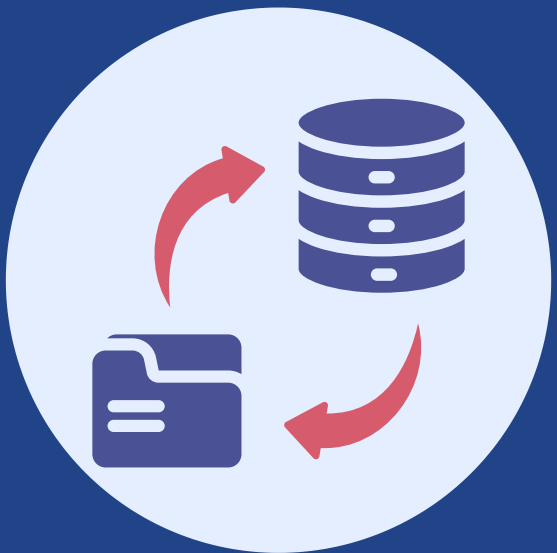
Il backup è una componente essenziale della sicurezza. Se il tuo dispositivo viene infettato da ransomware, rubato o semplicemente si rompe, avere copie di sicurezza dei dati ti salva da perdite catastrofiche. Segui la regola del 3-2-1: almeno 3 copie dei dati importanti, su 2 tipi di supporto diversi (es. hard disk esterno e cloud), con 1 copia conservata in posizione diversa. Esistono servizi cloud automatici come Google Drive, Dropbox, OneDrive o iCloud che semplificano enormemente il processo.

CRITTOGRAFIA DEL DISCO

Per dati particolarmente sensibili, considera di abilitare la crittografia completa del disco. Windows offre BitLocker, macOS offre FileVault. In caso di furto del dispositivo, i dati criptati sono praticamente inaccessibili senza la password corretta.

RETI WI-FI SICURE

Quando sei fuori casa, evita di accedere a servizi sensibili (banca, email) da reti Wi-Fi pubbliche non protette. Se devi farlo, usa una VPN (Virtual Private Network) che cripta il tuo traffico. A casa, proteggi la tua rete Wi-Fi con una password WPA3 (o almeno WPA2) robusta e cambia le credenziali predefinite del router.



Capitolo 5

Navigare in sicurezza su Internet

Internet è una risorsa straordinaria ma anche un ambiente potenzialmente pericoloso. Adottare comportamenti sicuri durante la navigazione riduce drasticamente i rischi di compromissione.

RICONOSCERE I SITI SICURI

Prima di inserire dati personali o informazioni sensibili su un sito, verifica sempre che la connessione sia sicura. L'indirizzo deve iniziare con "https://" (non solo "http://") e nella barra del browser dovrebbe apparire un'icona a forma di lucchetto. Cliccando sul lucchetto puoi vedere i dettagli del certificato di sicurezza del sito. Tuttavia, ricorda che https garantisce solo che la comunicazione è criptata, non che il sito sia affidabile.

I RISCHI DEL DOWNLOAD

Scarica software, app e file solo da fonti ufficiali e affidabili. Il sito ufficiale del produttore è sempre la scelta più sicura. Evita siti di download di terze parti che potrebbero inserire malware nei file. Non scaricare mai software pirata: oltre a essere illegale, è spesso veicolo di virus. Quando scarichi qualsiasi file, anche da fonti apparentemente affidabili, scansionalo con l'antivirus prima di aprirlo.

BROWSER E ESTENSIONI

Usa un browser moderno e mantenuto aggiornato come Chrome, Firefox, Edge o Safari. Considera l'installazione di estensioni che migliorano la sicurezza e la privacy come uBlock Origin (blocca pubblicità e tracker), HTTPS Everywhere (forza connessioni sicure quando disponibili), e Privacy Badger (blocca tracker invisibili). Tuttavia, installa solo estensioni da fonti affidabili perché anche le estensioni possono rappresentare rischi se provengono da sviluppatori non affidabili.

LA NAVIGAZIONE IN INCOGNITO

La modalità incognito o privata del browser impedisce che vengano salvati cronologia, cookie e dati dei moduli. È utile quando usi un computer condiviso, ma non ti rende anonimo su internet e non protegge da malware. Il tuo provider internet e i siti che visiti possono comunque vedere la tua attività.

I COOKIE E LA PRIVACY

I cookie sono piccoli file che i siti salvano sul tuo browser per ricordare informazioni. Alcuni sono necessari per il funzionamento dei siti, altri servono a tracciare le tue attività per scopi pubblicitari. Configura il browser per bloccare cookie di terze parti e cancella periodicamente i cookie memorizzati. Molti browser offrono ora opzioni per limitare il tracciamento.

ATTENZIONE AI POP-UP E PUBBLICITÀ

Non cliccare mai su pop-up sospetti, soprattutto quelli che avvisano di infezioni del computer o offrono "scansioni gratuite". Sono spesso tentativi di farti installare malware. Chiudi sempre questi pop-up usando la X della finestra o Alt+F4, mai cliccando sui pulsanti all'interno del pop-up.

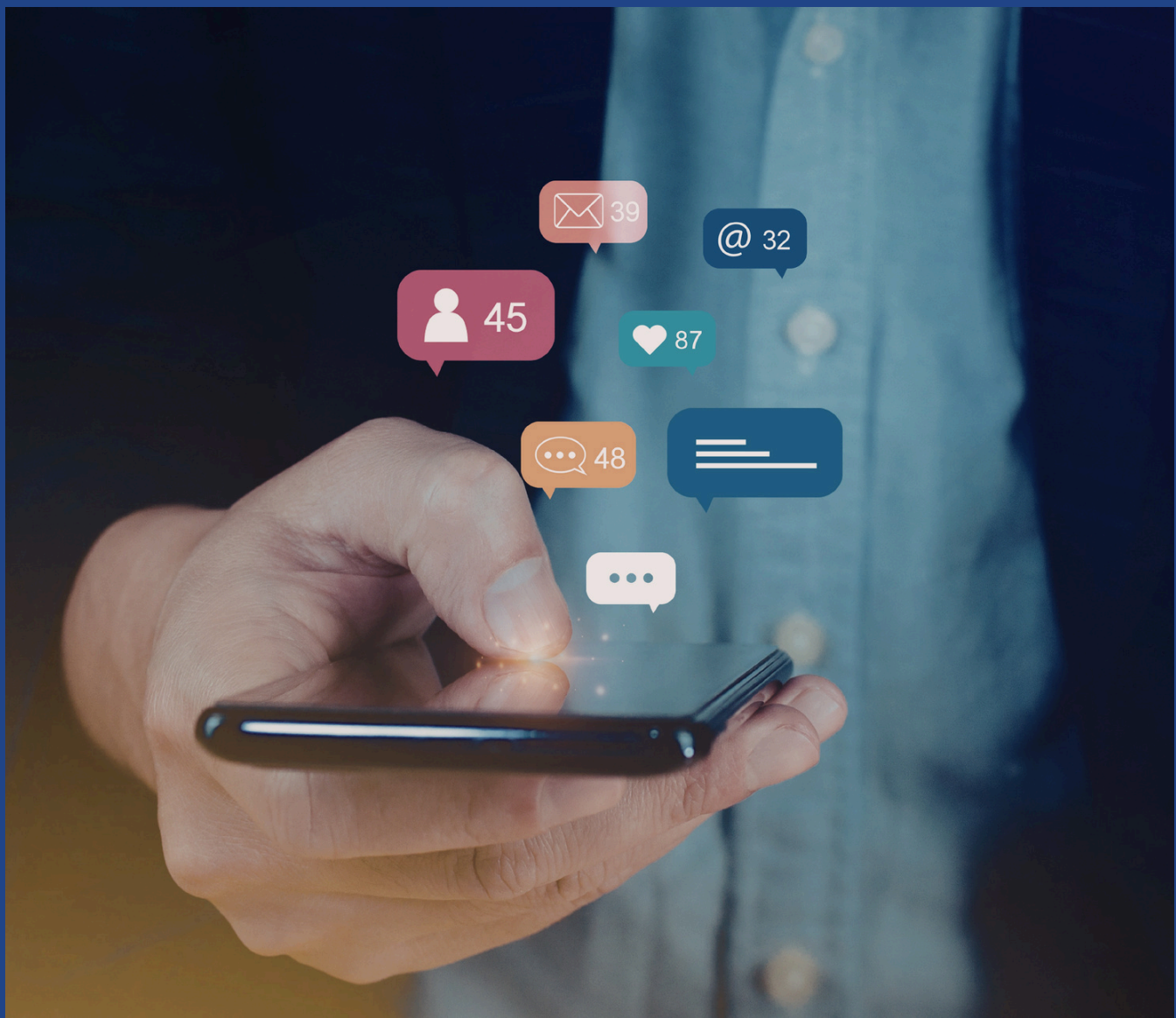
EMAIL E ALLEGATI

Non aprire email da mittenti sconosciuti e non cliccare mai su link o allegati in email sospette. Anche email apparentemente da mittenti conosciuti potrebbero essere falsificate. Prima di cliccare su un link, passa il mouse sopra per vedere l'URL reale (senza cliccare). Se un'email ti chiede di verificare account o fornire dati sensibili, vai direttamente sul sito ufficiale digitando l'indirizzo nel browser invece di cliccare sul link nell'email.

Capitolo 6

Social Media e privacy online

I social media sono parte integrante della vita moderna, ma comportano rischi significativi per la privacy e la sicurezza se non usati con consapevolezza.



COSA CONDIVIDI DICE CHI SEI

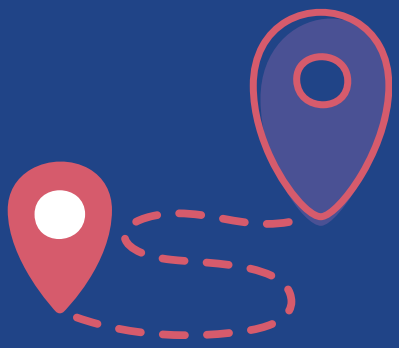
Ogni informazione che condividi sui social media contribuisce a creare la tua identità digitale. Nome completo, data di nascita, città di residenza, luogo di lavoro, nomi di familiari, abitudini quotidiane: tutte queste informazioni possono essere sfruttate da malintenzionati per truffe mirate, furti d'identità o attacchi di social engineering. Prima di pubblicare qualcosa, chiediti: "Questa informazione potrebbe essere usata contro di me?"

LE IMPOSTAZIONI SULLA PRIVACY

Tutti i principali social media offrono impostazioni di privacy che controllano chi può vedere i tuoi contenuti. Dedica tempo a configurarle correttamente. Imposta i tuoi profili come privati quando possibile, limita chi può vedere i tuoi post, le tue foto e le informazioni personali, controlla chi può taggarti nelle foto o nei post, rivedi periodicamente la lista di amici/contatti rimuovendo persone che non conosci realmente, e limita le informazioni visibili pubblicamente al minimo indispensabile.

IL PROBLEMA DEL GEOTAGGING

Molte foto scattate con lo smartphone contengono metadati GPS che indicano esattamente dove e quando sono state scattate. Pubblicare foto in tempo reale dalla tua posizione può rivelare dove ti trovi, dove abiti, dove lavori, o quando sei in vacanza (informazione preziosa per i ladri). Disattiva la geolocalizzazione nelle impostazioni della fotocamera o rimuovi i metadati prima di condividere le foto online.



ATTENZIONE ALLE RICHIESTE DI AMICIZIA

Non accettare richieste di amicizia da persone che non conosci realmente. I profili falsi sono comuni e vengono usati per raccogliere informazioni, diffondere spam, o perpetrare truffe. Se ricevi una richiesta da qualcuno che dice di conoscerti ma non lo ricordi, verifica attraverso altri canali prima di accettare.

QUIZ E APP DI TERZE PARTI

I quiz virali tipo "Quale personaggio di Game of Thrones sei?" o "Come sarà il tuo 2025?" sono spesso strumenti per raccogliere dati personali. Quando autorizzi queste app ad accedere al tuo profilo social, gli concedi l'accesso a molte informazioni tue e dei tuoi amici. Evita questi quiz o almeno controlla quali permessi richiedono prima di accettare.

L'OVERSHARING E LE CONSEGUENZE

Condividere troppo può avere conseguenze impreviste. Pubblicare foto di bambini in uniforme scolastica rivela quale scuola frequentano. Lamentarsi del capo su Facebook può costare il lavoro. Foto di party sfrenati possono compromettere opportunità professionali future. Pensa sempre a lungo termine prima di pubblicare.