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

TRAPPOLE DIGITALI E TRUFFE ONLINE

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 Trappole Digitali e alle Truffe Online, sviluppato nell'ambito del progetto Digita Facile Campania, Tema B — Sicurezza e Uso Consapevole dei Servizi Digitali. Si rivolge a chiunque usi internet nella vita quotidiana per fare acquisti, gestire il conto corrente, comunicare con amici e istituzioni e vuole imparare a riconoscere e a evitare le insidie digitali più diffuse.

Il percorso è organizzato in due grandi blocchi tematici. Il primo, Navigare in Piena Consapevolezza e Sicurezza, esplora i meccanismi invisibili che accompagnano la navigazione quotidiana: i cookie e le loro implicazioni sulla privacy, le tracce visibili che lasciamo nel browser, la navigazione in incognito e i suoi limiti reali, la VPN come strumento di protezione avanzata, e le tecniche per verificare l'autenticità di siti e notizie. Il secondo, Truffe e Trappole in Ambiente Digitale, smonta le principali tecniche di manipolazione psicologica usate dai cybercriminali e descrive in dettaglio gli scenari di truffa più diffusi, da quelli più semplici ai più sofisticati, ognuno con la strategia di difesa specifica.

Questa dispensa è costruita attorno a un principio fondamentale: la migliore difesa non è tecnica, è culturale. Chi conosce le trappole difficilmente ci cade. Chi sa come funziona il phishing non clicca il link. Chi riconosce il social engineering si ferma prima di agire. La conoscenza è lo strumento più potente che abbiamo contro la cybercriminalità e questa dispensa è pensata per renderla accessibile a tutti, indipendentemente dal livello di competenza digitale di partenza.

> Il messaggio centrale di questo percorso è che le truffe digitali sfruttano sempre le stesse tre leve emotive: paura, urgenza e avidità. Ogni volta che un messaggio online ti fa sentire una di queste emozioni in modo intenso e improvviso, fermati un momento per verificare meglio.

Navigare lascia tracce: cosa succede davvero online

Truffe online: fenomeno in crescita

I soldi fisici stanno scomparendo. I nostri risparmi, la pensione, lo stipendio sono solo "numeri" su un server bancario accessibile via app. Ma non solo. Anche la nostra identità è sempre più “digitale” con SPID e CIE che permettono l’accesso ai servizi della Pubblica Amministrazione.

Tutto questo rende i nostri dati “il nuovo oro”. Lo sono per le Agenzie di Marketing, che studiano sistemi sempre più sofisticati per venire incontro agli interessi degli utenti e aumentare la conversione in acquisti. Lo sono per i Cybercriminali, il cui obiettivo è trovare un modo per derubarci.

Nel 2024 le truffe digitali — soprattutto legate a pagamenti elettronici — hanno colpito circa 2,9 milioni di italiani, con un danno economico stimato in 880 milioni di euro. In Campania, nel 2024-2025, sono stati sequestrati oltre 2.000 SIM card utilizzate per frodi digitali, e risultano 23 indagati per phishing e furto di dati personali.

Alla base di questo fenomeno, ci siamo noi e il nostro comportamento. Utilizzare consapevolmente la tecnologia digitale e navigare sul web sapendo individuare le trappole digitali, resta la prima arma contro le truffe.

I nostri dati sono il "nuovo oro"

Nel 2024 è emerso che la società americana Cox Media Group aveva dichiarato ai propri clienti di offrire una tecnologia chiamata Active Listening, basata sull'analisi dei dati vocali degli utenti attraverso i microfoni dei dispositivi smart. L'episodio, pur smentito da Meta e Google che hanno rimosso CMG dai loro programmi pubblicitari, dimostra che la prudenza nella gestione dei permessi delle app non è paranoia, ma buon senso.

Quante volte accettiamo i cookie senza valutarne i termini? Quante volte scarichiamo un'app e concediamo autorizzazioni sensibili come l'accesso al microfono e alla geolocalizzazione nostro smartphone? Stiamo rivelando informazioni preziose su di noi, che oggi possono migliorare l'offerta pubblicitaria, ma domani?

Il Regolamento Generale sulla Protezione dei Dati, entrato in vigore nel 2018 per sostituire le vecchie leggi sulla privacy degli anni Novanta, ha cercato di restituire ai cittadini europei il pieno controllo sulle proprie informazioni digitali, imponendo a tutte le aziende, compresi i giganti del web extra-europei, di raccogliere i dati in modo trasparente e solo dopo aver ottenuto un consenso esplicito. Il ruolo del Garante è quello di far applicare concretamente il regolamento europeo in Italia, operando come un vero e proprio "arbitro" che vigila sul comportamento di aziende e pubbliche amministrazioni.

Ma la protezione dei dati personali e dei nostri conti passa inevitabilmente dal nostro comportamento.

MODULO 1 — PARTE A

Cookie, Tracce e Privacy nella Navigazione

Obiettivi

Al termine di questa sezione saprai cosa sono i cookie e come gestirli in modo consapevole. Comprenderai la differenza tra tracce visibili e invisibili lasciate durante la navigazione. Conoscerai i limiti reali della navigazione in incognito e il funzionamento di una VPN.

Le tracce invisibili: i cookie. Biscotti dolci o amari?

Il cookie informatico (dal termine inglese che significa letteralmente "biscotto") è un piccolo file di testo che un sito web salva nel browser dell'utente durante una visita, per recuperare quelle informazioni nelle visite successive. La Treccani lo definisce con precisione: 'file di testo di ridotte dimensioni che un sito web invia al browser dell'utente, dove vengono memorizzati per essere poi ritrasmessi allo stesso sito alla visita successiva.'

Non tutti i cookie sono uguali. Esistono tre categorie principali con finalità molto diverse tra loro, e capire la differenza è fondamentale per fare scelte consapevoli quando compare il banner del consenso.

Cookie tecnici: sono essenziali per il funzionamento del sito e non possono essere rifiutati senza compromettere l'esperienza. Sono quelli che ricordano cosa hai messo nel carrello di un e-commerce, che mantengono attiva la tua sessione di accesso dopo il login, che salvano le preferenze di lingua o di visualizzazione. Senza questi cookie, i siti moderni semplicemente non funzionerebbero. Non c'è nessun motivo valido per bloccarli.

Cookie analitici e statistici: misurano il comportamento degli utenti sul sito, come quante persone lo visitano, da dove arrivano, quali pagine guardano di più, per quanto tempo rimangono, con l'obiettivo di migliorare il servizio offerto. Possono essere completamente anonimi o pseudo-anonimi. Sono generalmente meno invasivi dei cookie di profilazione, ma contribuiscono comunque alla raccolta di dati comportamentali.

Cookie di profilazione e marketing: sono i più controversi e i più impattanti sulla privacy. Tracciano il comportamento dell'utente non solo su un singolo sito, ma attraverso decine o centinaia di siti diversi, grazie ai cosiddetti cookie di terze parti, installati da domini diversi da quello che si sta visitando, costruendo nel tempo un profilo dettagliatissimo degli interessi, delle abitudini di consumo e dei comportamenti di ciascuna persona. Questo profilo viene venduto a reti pubblicitarie che lo usano per inviare pubblicità altamente personalizzata. Sono questi che permettono al sito di scarpe di 'seguirti' con le sue pubblicità su altri siti dopo che hai chiuso la pagina.

Quando appare il banner del consenso ai cookie, hai sostanzialmente tre opzioni. Accettare tutto è come lasciare la porta di casa spalancata: comodo, ma massimizza la raccolta di dati su di te. Rifiutare tutto è come murare la porta: protegge la privacy ma può compromettere la funzionalità di alcuni siti. La scelta

più equilibrata e consigliata è bloccare i cookie di terze parti: mantieni i cookie tecnici che servono al funzionamento dei siti e rinunci soltanto alla profilazione pubblicitaria inter-sito.

> **Come fare: Su Chrome**: Impostazioni → Privacy e sicurezza → Cookie di terze parti → Blocca cookie di terze parti in modalità Incognito (o sempre per più protezione). **Su Firefox:** Preferenze → Privacy e sicurezza → Protezione antitracciamento avanzata. **Su Safari** è già attiva per default la protezione contro il tracciamento inter-sito.

Le tracce invisibili: il Fingerprinting. Come un'impronta

Mentre i cookie funzionano come un 'post-it' o una targhetta che un sito web attacca fisicamente sul vostro computer per riconoscervi quando tornate, il fingerprinting non ha bisogno di installare assolutamente nulla. Funziona in modo passivo: il sito web interroga il vostro browser e raccoglie un mix di dettagli tecnici. Qual è il vostro sistema operativo? Che risoluzione ha il vostro schermo? Quali font avete installato? Che fuso orario usate? Che scheda grafica avete? Prese singolarmente, queste informazioni sono innocue. Ma combinate insieme, creano un'**impronta digitale praticamente unica**. La differenza sostanziale con i cookie è tutta qui: i cookie li potete cancellare o bloccare perché sono file salvati sul vostro dispositivo. Il fingerprinting, invece, vi riconosce semplicemente 'guardando' come è fatto il vostro dispositivo.

La soluzione in questo caso è più complessa. Se si accede da PC, è utile scaricare estensioni del browser che lo aiutino a bloccare il tracciamento. A meno che non si utilizza un browser molto restrittivo come Brave, che è un'ottima soluzione anche per navigazione da Smartphone. Laddove, se si esce dall'app del browser, l'unica soluzione è usare app terze che bloccano il tracciamento e la pubblicità sulle singole app in uso.

Per passare ad un *Livello Hard* di protezione della privacy su PC e Smartphone, puoi scaricare la dispensa relativa inquadrando il QR code in calce al Modulo 1.

Le tracce visibili: cronologia e storico delle ricerche

Accanto ai cookie e al fingerprinting (tracce salvate prevalentemente sui server) il browser registra anche tracce locali nel dispositivo stesso, visibili a chiunque abbia accesso fisico al computer o allo smartphone.

La **cronologia** è l'elenco completo di tutti i siti visitati, organizzato per data e ora. È uno strumento genuinamente utile, dato che permette di ritrovare rapidamente un sito visto giorni fa senza ricordarne l'indirizzo esatto, ma è anche una mappa dettagliata delle tue attività online: i tuoi interessi, le tue preoccupazioni di salute, i tuoi acquisti, le persone che hai cercato, le notizie che hai seguito. Chiunque abbia accesso fisico al tuo dispositivo e sappia come aprire la cronologia del browser può leggere questa mappa. Il classico esempio del regalo di Natale scoperto perché si condivide lo stesso PC in famiglia.

Lo **storico delle ricerche** mantiene traccia di tutte le parole chiave inserite nel motore di ricerca, mentre la barra degli indirizzi URL memorizza gli indirizzi digitati manualmente. Entrambi sono visibili a chiunque usi lo stesso dispositivo e, in molti casi, alle piattaforme dei motori di ricerca che li usano per

personalizzare i risultati futuri. Cancellare periodicamente cronologia, storico e cache del browser, attraverso le Impostazioni → Cancella dati di navigazione in tutti i principali browser, è una buona abitudine di igiene digitale che vale la pena sviluppare.

La navigazione in incognito: un mantello parziale

La **navigazione in incognito**, chiamata anche navigazione privata o anonima a seconda del browser è probabilmente lo strumento di privacy più frainteso nell'uso quotidiano di internet. L'icona dell'omino con cappello e occhiali scuri ha contribuito a creare l'impressione che attivando questa modalità si diventi totalmente invisibili online. Non è così.

Ecco cosa fa concretamente la navigazione in incognito: al termine della sessione, non lascia tracce locali sul dispositivo. Non salva la cronologia delle pagine visitate. Non memorizza i cookie dopo la chiusura della finestra. Non salva le informazioni inserite nei moduli e nelle ricerche per la compilazione automatica futura. In sostanza: dopo aver chiuso la finestra in incognito, il dispositivo che stai usando non conserva nessuna traccia di quella sessione.

Ma ecco cosa la navigazione in incognito non fa, e qui sta il principale malinteso: **non nasconde la tua attività al tuo fornitore di connessione internet**, di fatti TIM, Vodafone, Fastweb, WindTre e tutti gli altri continuano a vedere i siti che visiti. Non nasconde la tua attività **ai siti web che visiti**, che continuano a registrare il tuo indirizzo IP e il tuo comportamento. Non ti protegge **da chi monitora la rete**, incluso il datore di lavoro se usi la rete aziendale, o un potenziale hacker su una rete Wi-Fi pubblica. Non è un sistema di anonimizzazione: è un sistema di pulizia locale.

Le due situazioni in cui la navigazione in incognito è genuinamente utile sono: quando si usa un computer che non è il proprio, ad esempio in hotel, in biblioteca; a casa di amici, per non lasciare account aperti o informazioni personali salvate; e quando si condivide un dispositivo con qualcuno e si vuole mantenere riservata una sessione specifica.

> La navigazione in incognito NON ti rende anonimo su internet. Ti rende invisibile soltanto sul dispositivo che stai usando in quel momento. Il tuo fornitore di internet, i siti che visiti e chiunque monitori la rete continuano a vedere ogni tua mossa.

La VPN: il vero scudo della navigazione

La VPN — **Virtual Private Network, Rete Privata Virtuale** — è lo strumento che offre una protezione della privacy molto più sostanziale rispetto alla sola navigazione in incognito. La definizione tecnica è precisa: è una tecnologia che crea un tunnel di comunicazione cifrato tra il dispositivo dell'utente e un server remoto, attraverso cui passa tutto il traffico internet. Dall'esterno, chiunque monitori la rete vede soltanto che c'è una connessione cifrata verso il server VPN, ma non vede cosa contiene quella connessione né dove è diretta in definitiva.

Le quattro caratteristiche principali di una VPN nella vita quotidiana. **La crittografia** dei dati trasforma le informazioni trasmesse in un codice illeggibile per chiunque le intercetti: come inviare una lettera in

una cassaforte blindata invece che su una cartolina aperta. Il **mascheramento dell'indirizzo IP** sostituisce il tuo indirizzo di rete reale con quello del server VPN: i siti che visiti vedono la posizione del server, non la tua. L'**aggiramento di restrizioni geografiche** consente di navigare come se si fosse in un paese diverso. **La protezione sulle reti pubbliche** è forse l'uso più importante nella vita quotidiana: usare una VPN su un Wi-Fi pubblico (al bar, in aeroporto, in hotel) rende i propri dati illeggibili per chiunque stia monitorando quella rete.

Esistono VPN gratuite e a pagamento. Le VPN a pagamento di fornitori affidabili (NordVPN, ExpressVPN, ProtonVPN) offrono garanzie di privacy più robuste e connessioni più stabili. Le VPN gratuite vanno usate con cautela: alcune finanziano il servizio gratuito raccogliendo e vendendo i dati degli utenti, che è esattamente il contrario di quello che si vuole ottenere usando una VPN.

E il Fingerprinting? La cosa più critica è che funziona anche se navigate in incognito o usate una VPN perché le caratteristiche della VPN non nascondono le caratteristiche del dispositivo. Puoi difenderti usando alcune strategie principali: usare un browser anti-tracciamento (La soluzione migliore) o bloccare gli script alla radice (usando estensioni Ad Blocker e antitracciamento). Puoi valutare i principali strumenti per Browser PC e Smartphone che difendono la nostra privacy inquadrando il QR code e scaricando la dispensa.

Digita Facile
Campania

Active Listening: gli smartphone ci ascoltano?

Nel 2024 CMG afferma di poter offrire ai clienti una tecnologia chiamata Active Listening (ascolto attivo) «*una tecnologia pubblicitaria innovativa basata sull'analisi dei dati vocali e comportamentali degli utenti. Questa tecnologia sfrutta i microfoni dei dispositivi smart per raccogliere dati sulle conversazioni in tempo reale*». Salvo poi ritrattare.

In molti, tuttavia, sono pronti a giurare di aver ricevuto un messaggio pubblicitario strettamente legato alla conversazione appena avuta. Sebbene la tecnologia esista (come ha tentato di vendere l'agenzia Cox Media), l'ascolto segreto a scopo di marketing è di fatto illegale. Le tutele del GDPR e la vigilanza del Garante (GPDP) sono così stringenti che le grandi multinazionali tecnologiche rifiutano categoricamente queste pratiche per non incorrere in sanzioni milionarie.

Se non ci ascoltano, come fanno a indovinare i nostri desideri? La risposta è nell'incrocio massiccio di dati. Gli algoritmi uniscono il nostro ID pubblicitario, la cronologia web, l'uso delle carte fedeltà e persino le posizioni GPS (per capire chi frequentiamo fisicamente), deducendo i nostri interessi con una precisione che sembra, a torto, telepatica.

L'unico vero rischio di essere "ascoltati" dal telefono non viene dal marketing, ma dal cybercrimine o dallo spionaggio tramite *trojan*. Scaricare app di dubbia provenienza o concedere autorizzazioni alla cieca espone al rischio di installare software malevoli capaci di attivare fraudolentemente il microfono a nostra insaputa.

I permessi delle app: come comportarsi

Le app che installiamo sullo smartphone chiedono spesso **permessi di accesso** a funzionalità del dispositivo: microfono, fotocamera, geolocalizzazione, galleria foto, contatti, messaggi SMS. Questi permessi sono a volte legittimamente necessari per le funzioni dell'app, ma spesso vengono richiesti senza una vera utilità funzionale, oppure con finalità non dichiarate di raccolta dati.

Il **principio del privilegio minimo** suggerisce di concedere a ogni app soltanto e unicamente i permessi che hanno un'effettiva e chiara funzionalità per le funzioni che si intende usare. Un'app torcia non ha alcuna ragione legittima per accedere ai contatti o alla posizione. Un'app di gioco non ha bisogno del microfono. Un'app meteo non ha bisogno della fotocamera. Quando un'app richiede permessi che non corrispondono alle sue funzioni dichiarate, è un segnale di allarme: quella richiesta serve probabilmente a raccogliere dati per scopi non dichiarati.

Le **autorizzazioni più sensibili** da monitorare con attenzione sono cinque: il microfono e la fotocamera, perché permettono la raccolta di contenuti audio e visivi dall'ambiente in cui ci si trova; la

geolocalizzazione, perché costruisce nel tempo una mappa precisa dei luoghi frequentati; la galleria foto, che contiene spesso informazioni personali molto dettagliate, come luoghi, persone, documenti fotografati; i contatti, che rivelano l'intera rete sociale della persona; i messaggi SMS, permesso particolarmente critico perché intercettando gli SMS si possono rubare i codici OTP della banca.

Per ognuna di queste autorizzazioni, i sistemi operativi moderni offrono tre livelli di accesso: nessun accesso, accesso sempre (anche quando l'app è chiusa) e accesso solo **mentre l'app è in uso**. La scelta equilibrata e raccomandata è quasi sempre 'solo mentre l'app è in uso: permette all'app di funzionare quando si sta usando attivamente, ma impedisce la raccolta di dati in background.

> Come controllare i permessi: su **iPhone**, vai in **Impostazioni → Privacy e sicurezza**, dove puoi vedere quali app hanno accesso a ogni tipo di risorsa. Su **Android**, vai in **Impostazioni → App → Gestione permessi.** Controlla regolarmente ogni tre o sei mesi e revoca i permessi che non ricordi di aver concesso o che non ti sembrano giustificati.

Le app che installiamo sullo smartphone chiedono spesso **permessi di accesso** a funzionalità del dispositivo: microfono, fotocamera, geolocalizzazione, galleria foto, contatti, messaggi SMS. Questi permessi sono a volte legittimamente necessari per le funzioni dell'app, ma spesso vengono richiesti senza una vera utilità funzionale, oppure con finalità non dichiarate di raccolta dati.

ID Pubblicitario: il Santo Graal del marketing

Il Browser web sta ai Cookie esattamente come il Sistema Operativo dello smartphone (iOS o Android) sta all'ID Pubblicitario. Se i Cookie di terze parti ti seguono mentre salti da un sito all'altro (es. da un e-commerce a Facebook via web), l'ID Pubblicitario ti segue mentre salti da un'app all'altra (es. dall'app del negozio all'app di Instagram). Mentre nel browser i siti installano *tanti* piccoli cookie diversi (tanti file di testo fisici), nello smartphone l'ID pubblicitario è uno solo. È un **unico "codice a barre" centralizzato** e di sistema fornito direttamente da Apple o Google. Questo lo rende, di fatto, ancora più potente e ordinato di un normale cookie, perché tutte le app leggono esattamente la stessa etichetta universale senza dover installare nulla di nuovo sul tuo telefono.

Come funziona: l'ID pubblicitario è una semplice stringa alfanumerica invisibile (ad esempio: 1A2B3C4D-5678-90EF...) assegnata dal sistema operativo al tuo dispositivo. Questo codice è condiviso tra tutte le app. Se apri l'app di un negozio di abbigliamento, l'app legge il tuo ID e lo invia a una rete pubblicitaria dicendo: "*L'utente 1A2B3C sta guardando giacche a vento*". Quando poi apri un giochino gratuito, il giochino invia lo stesso ID alla rete pubblicitaria per chiedere quale banner mostrare. La rete riconosce l'ID e ti compare la pubblicità della giacca a vento.

Le implicazioni sono le stesse dei cookie: quanta privacy siamo disposti a cedere in cambio della gratuità dei contenuti e dei servizi offerti?

> Come disattivare l'ID pubblicitario: su **iPhone**, basta andare su **Impostazioni** > **Privacy e sicurezza** > **Tracciamento**. In cima alla schermata c'è un interruttore generale chiamato

"Richiesta tracciamento attività". Su **Android**, vai in **Impostazioni** > **Google** > **Annunci** dove troverai: **"Elimina ID pubblicitario"**.

MODULO 2 — PARTE A

Social Engineering: la psicologia della truffa

Cos'è il social engineering

La maggior parte delle truffe digitali non richiede competenze informatiche sofisticate. Non sfrutta vulnerabilità tecniche nei sistemi (buchi nei software, debolezze nei protocolli di rete) ma vulnerabilità umane: la paura, la fretta, la curiosità, la fiducia, il desiderio di un guadagno facile. Questo approccio si chiama social engineering, ossia ingegneria sociale, ed è definito dalla Treccani come il complesso di strategie e metodi di manipolazione psicologica e di persuasione volto a indurre un utente a rivelare informazioni riservate. Il social engineering è così efficace e così diffuso perché aggira completamente i sistemi tecnologici di sicurezza. Non serve bucare un firewall sofisticato se puoi convincere l'utente a consegnare volontariamente le sue credenziali. Non serve installare un malware complesso se puoi convincere qualcuno a chiamare un numero falso e fornire i dati bancari di persona. La tecnologia è la scena del crimine, ma il crimine vero è psicologico. E la psicologia umana ha vulnerabilità che nessun aggiornamento software può correggere.

I tre grimaldelli emotivi

Ogni truffa digitale efficace sfrutta almeno uno di tre meccanismi emotivi fondamentali. Riconoscerli è la difesa più potente che esiste, più di qualsiasi software o protezione tecnica.

La paura: messaggi che creano un allarme immediato e paralizzante. “Il tuo conto è stato bloccato per attività sospette!”, “È stato rilevato un virus nel tuo computer!”, “La Polizia Postale ha aperto un'indagine a tuo nome!”. La paura attiva la risposta di emergenza del sistema nervoso autonomo: il ragionamento critico rallenta o si spegne del tutto, e il corpo spinge ad agire immediatamente per eliminare la minaccia. Chi si trova in questo stato emotivo non rallenta per verificare, non chiama il numero ufficiale, non legge i dettagli con attenzione: clicca subito, chiama subito, paga subito.

L'urgenza: messaggi che creano una pressione temporale artificiale. “Hai solo 24 ore per rispondere prima che il conto venga chiuso!”, “L'offerta scade tra 10 minuti!”, “Conferma ora o perdi definitivamente l'accesso!”. L'urgenza ha un effetto preciso e documentato sul processo decisionale: elimina il tempo necessario per riflettere e verificare. Chi è di fretta prende scorciatoie cognitive si affida alle apparenze, non controlla i dettagli, si fida della fonte apparente senza verificarla.

L'avidità e la curiosità: messaggi che promettono ricompense improbabili o stuzzicano una curiosità intensa. “Hai vinto un iPhone 15!”, “C'è un rimborso fiscale di 847€ in attesa di riscossione!”, “Guarda la foto scandalosa di [nome famoso]!”. L'eccitazione generata da una promessa di guadagno inaspettato, o

da una curiosità molto intensa, produce lo stesso effetto degli altri due grimaldelli: il pensiero critico viene bypassed dal desiderio di vedere, di sapere, di ottenere.

> La regola d'oro contro il social engineering: se un messaggio ti fa sentire paura, urgenza o eccitazione intensa in modo improvviso, FERMATI. Non fare nulla per almeno cinque minuti. In quasi tutti i casi, la truffa si svela da sola quando si dà al cervello il tempo di tornare a funzionare normalmente.

I tre canali della truffa digitale

I cybercriminali usano tre canali principali per raggiungerti, tutti nominati con varianti del termine 'phishing' (che viene dall'inglese fishing, pescare) perché l'immagine dell'amo che pesca vittime ignare descrive perfettamente la tecnica.

Phishing: l'amo arriva via email. È la forma più antica e ancora la più diffusa e redditizia della truffa digitale. Il truffatore invia un'email che imita graficamente una comunicazione ufficiale della banca, delle Poste, di Amazon, di PayPal, dell'Agenzia delle Entrate, con loghi riprodotti fedelmente, toni formali, firme plausibili, e un link che porta a una pagina che copia quasi perfettamente il sito originale. Lo scopo è sempre lo stesso: far inserire all'utente le proprie credenziali, username e password, su un sito falso che le registra e le invia ai truffatori.

Smishing: l'amo arriva via SMS o WhatsApp. Segue la stessa logica del phishing ma sfrutta la maggiore fiducia che le persone tendono a riporre nei messaggi diretti rispetto alle email. Il messaggio sembra provenire da Poste Italiane, da un corriere, dalla propria banca o da un ufficio governativo. “Il tuo pacco è in giacenza: paga 1,99€ di spese amministrative tramite questo link” è uno degli scenari più frequenti. La sensazione che il messaggio sia personale (è arrivato direttamente sul mio telefono) abbassa la guardia.

Vishing: l'amo arriva a voce, attraverso una telefonata. Qualcuno si finge un operatore del servizio clienti bancario, un tecnico di supporto di Microsoft o Apple, un funzionario dell'Agenzia delle Entrate, un agente della Polizia Postale. La voce umana crea un senso di autenticità molto difficile da ignorare, e la conversazione in tempo reale non dà il tempo fisico di verificare l'identità del chiamante o di consultare qualcuno. È il canale più difficile da cui difendersi perché attiva tutti e tre i grimaldelli contemporaneamente: la paura dell'autorità, l'urgenza della situazione, la pressione della conversazione in corso.

MODULO 2 — PARTE B
Gli Scenari di Truffa: riconoscere e difendersi

Il finto pacco — Smishing

Scenario 1: Il corriere fantasma

Lo scenario: Arriva un SMS: "Il tuo pacco (codice IT849302) è in giacenza presso il nostro deposito. Paga €1,99 di spese di gestione per autorizzare la consegna entro oggi: [link]." Il messaggio sembra autentico, usa un numero di tracking plausibile e crea urgenza con la scadenza giornaliera.

La verità: Non stai aspettando nessun pacco, o se lo aspetti, nessun corriere legittimo chiede pagamenti via SMS su link esterni. Quel link porta a una pagina che imita il sito del corriere e raccoglie i dati della tua carta di credito. I pochi euro chiesti sono un pretesto: i tuoi dati bancari valgono molto di più.

Difesa: Non cliccare il link, mai. Non pagare. Blocca il numero mittente e segnala il messaggio come spam nelle opzioni del messaggio. Se aspetti davvero un pacco, vai direttamente sul sito ufficiale del corriere digitando tu l'indirizzo nel browser, e inserisci manualmente il numero di tracking.

Lo spear phishing — Il phishing personalizzato

Scenario 2: Il messaggio dall'amico o dal capo

Lo scenario: Arriva un'e-mail che sembra provenire da un tuo collega, dal tuo responsabile o da un'istituzione con cui hai effettivamente rapporti. Il messaggio contiene dettagli specifici su di te (il tuo nome completo, la tua azienda, un progetto a cui stai lavorando) che la rendono molto più credibile di un phishing generico.

La verità: Il truffatore ha studiato la vittima in anticipo: ha raccolto informazioni dai profili LinkedIn e Facebook, da violazioni precedenti di database, da ricerche sul nome online. Lo spear phishing è un attacco su misura, molto più difficile da riconoscere rispetto al phishing di massa.

Difesa: Verifica sempre, anche con i tuoi contatti più fidati, se una richiesta insolita è legittima. Usa un canale diverso da quello in cui hai ricevuto la richiesta: se l'e-mail sembra del tuo capo ma contiene una richiesta strana, chiamalo al telefono. Non cliccare mai link in e-mail inaspettate, anche se sembrano provenire da mittenti conosciuti.

La truffa e-commerce — L'affare del secolo

Scenario 3: Il prezzo impossibile

Lo scenario: Una pubblicità su Facebook o Instagram propone: "Bici elettrica ultima generazione a €49 invece di €599! Offerta esclusiva solo per oggi, disponibilità limitata!" Le foto sembrano professionali e i commenti alla pubblicità sono tutti entusiasti.

La verità: Paghi con carta di credito su un sito che sembra professionale e non ricevi nulla, oppure ricevi un pacco con un articolo completamente diverso e di bassissima qualità. In più, hai consegnato i dati della tua carta a un sito criminale che potrebbe usarli per altri acquisti non autorizzati.

Difesa: Prima di acquistare su un sito sconosciuto: cerca le recensioni su Trustpilot e Google Reviews. Cerca su Google il nome del sito seguito dalla parola 'truffa'. Verifica che esista un indirizzo fisico reale, una partita IVA e un numero di telefono funzionante. I commenti entusiasti sotto una pubblicità di Facebook possono essere falsi o filtrati dall'inserzionista. Se il prezzo sembra troppo bello per essere vero, è quasi certamente una truffa.

Il romance scam — Il principe azzurro digitale

Scenario 4: L'amicizia che diventa emergenza

Lo scenario: Qualcuno di molto affascinante ti chiede l'amicizia sui social o su un'app di incontri. Si presenta come un professionista all'estero: un militare in missione, un medico con una ONG, un ingegnere su una piattaforma petrolifera. Le conversazioni diventano quotidiane, affettuose, quasi romantiche, spesso per settimane o mesi.

La verità: Dopo aver investito molto tempo e molte emozioni nel costruire la relazione, arriva l'imprevisto drammatico: un incidente, un'operazione medica urgente, un blocco burocratico che impedisce il rientro. Ha bisogno di soldi subito. Non chiede tutto in una volta, inizia con cifre piccole e aumenta progressivamente.

Difesa: Non inviare mai denaro a qualcuno che non hai mai incontrato di persona, indipendentemente da quanto la relazione sembri reale. Fai una ricerca inversa per immagini sulla foto del profilo: spesso si scopre che appartiene a un'altra persona, trovata su internet. Se hai dubbi, parla con qualcuno di cui ti fidi prima di agire.

Il tech support scam — Il finto tecnico

Scenario 5: L'allarme a schermo

Lo scenario: Mentre navighi appare improvvisamente un pop-up che occupa l'intero schermo, lampeggia di rosso e riproduce un suono d'allarme: "VIRUS CRITICO RILEVATO! IL TUO COMPUTER È STATO COMPROMESSO. CHIAMA IMMEDIATAMENTE IL SUPPORTO MICROSOFT AL NUMERO 0800-xxx-xxx PER EVITARE LA PERDITA DI TUTTI I TUOI DATI!"

La verità: Non c'è nessun virus. È una normale pagina web progettata per sembrare un allarme di sistema — sfrutta l'HTML per bloccare la schermata e JavaScript per i suoni. Il

"tecnico" che risponde chiederà di installare un programma di accesso remoto per 'pulire il computer': in realtà sta prendendo il controllo del dispositivo per rubare dati, installare malware o estorcere denaro.

Difesa: Non chiamare il numero. Non installare nessun programma. Chiudi il browser con il tastiera — Ctrl+W o Cmd+W — o spegni il PC forzatamente se lo schermo è completamente bloccato. Quando riapri, tutto sarà sparito. Microsoft, Apple e Google non contattano mai proattivamente gli utenti con avvisi di questo tipo.

Il phishing bancario — La banca in panico

Scenario 6: L'email urgente della banca

Lo scenario: Arriva un'e-mail con il logo ufficiale della tua banca, la grafica perfetta, il tono formale: "Abbiamo rilevato un accesso sospetto al suo conto corrente dall'indirizzo IP 185.xxx.xxx. Per sicurezza, il suo account è stato temporaneamente limitato. Clicchi qui entro 24 ore per verificare la sua identità e ripristinare l'accesso, altrimenti il conto verrà bloccato permanentemente."

La verità: LA BANCA NON TI CHIEDE MAI DATI SENSIBILI VIA EMAIL O SMS. Questa è la regola assoluta del settore bancario, senza eccezioni. Il link porta a un sito che imita perfettamente il portale della tua banca, ma i dati inseriti (username, password, codice dispositivo) vengono catturati dai truffatori che li useranno immediatamente.

Difesa: Non cliccare mai il link. Non inserire credenziali su pagine raggiunte tramite link ricevuti. Se hai un dubbio reale sulla sicurezza del tuo conto, chiama il numero verde della banca che trovi sul retro della tua carta di credito, oppure accedi all'app bancaria ufficiale. Segnala l'e-mail come phishing al tuo provider e-mail.

Il man in the middle — L'intercettazione sul Wi-Fi

Scenario 7: Il bonifico intercettato

Lo scenario: Sei seduto in un bar. Usi il Wi-Fi gratuito per accedere all'app della tua banca e fare un bonifico. L'operazione sembra andare a buon fine, vedi la schermata di conferma. Qualche ora dopo scopri che i soldi sono arrivati su un conto completamente diverso da quello che avevi indicato.

La verità: Su una rete Wi-Fi pubblica non protetta, un attaccante tecnicamente preparato può posizionarsi tra te e il server della banca. Intercettando la comunicazione, può modificare in tempo reale le coordinate bancarie del destinatario prima che raggiungano il server, oppure continuare a usare la tua sessione bancaria dopo che hai completato l'operazione senza fare logout.

Difesa: Per qualsiasi operazione bancaria o finanziaria usa sempre la tua connessione dati mobile non il Wi-Fi pubblico. Se sei costretto a usare un Wi-Fi non fidato, attiva una VPN prima di aprire l'app bancaria. Fai sempre logout esplicito dall'app bancaria dopo ogni uso, specialmente su reti pubbliche.

I trojan bancari — Le spie in tasca

Scenario 8: L'app innocua che non lo è

Lo scenario: Scarichi un'app che sembra del tutto innocua: una torcia potente, un gioco gratuito di successo, un'utility per "pulire la memoria del telefono e velocizzarlo". L'app funziona, sembra legittima. Qualche settimana dopo la tua banca ti contatta: qualcuno ha effettuato operazioni non autorizzate dal tuo conto.

La verità: Quella app conteneva un trojan bancario. Questo tipo di malware usa due tecniche sofisticate. L'overlay: quando apri l'app ufficiale della tua banca, il trojan sovrappone una finestra trasparente identica allo schermo della banca. Tu vedi la tua banca, digiti le credenziali, ma stai digitando su una replica gestita dal malware. Il furto dell'OTP: alcuni trojan chiedono il permesso di "leggere gli SMS" e lo usano per intercettare i codici di conferma che la banca ti manda, permettendo di completare operazioni non autorizzate.

Difesa: Scarica le app solo dagli store ufficiali, App Store di Apple o Google Play Store. Prima di installare, controlla i permessi che l'app richiede: un'app torcia che chiede di leggere gli SMS o accedere ai contatti è quasi certamente malevola. Non concedere il permesso di 'Leggere gli SMS' a nessuna app tranne quella della tua banca ufficiale.

E-commerce in sicurezza: comprare online senza sorprese

1. Cosa osservare in un sito E-commerce
Prima di inserire i dati della tua carta, analizza questi elementi fondamentali:

Protocollo HTTPS: Verifica sempre che l'indirizzo inizi con https:// e che sia presente l'icona del lucchetto nella barra del browser, a indicare una connessione crittografata.

Dati Societari: Un sito serio deve esporre chiaramente nel "footer" (la parte bassa della pagina) la Partita IVA, la sede legale e i contatti (e-mail o telefono).

Politiche Legali: Controlla la presenza delle pagine relative alla Privacy Policy e, soprattutto, alle Condizioni di Reso e Rimborso. Se mancano, è un segnale di allarme.

Prezzi Irreali: Diffida di sconti eccessivi (es. un iPhone nuovo a 200€). Se l'offerta è troppo bella per essere vera, probabilmente è una truffa.

Segnali di Phishing: Presta attenzione a elementi grafici insoliti, come punti esclamativi gialli o avvisi che creano urgenza ingiustificata.

Gestione Cookie: Anche se comuni, popup di "GESTIONE DEI COOKIE" eccessivamente invasivi o con grafiche cartoonesche (come biscotti con braccia e gambe) in siti non familiari possono essere usati per mascherare script malevoli.

2. Strumenti esterni per valutare l'affidabilità

Non fidarti solo di ciò che vedi sul sito; usa queste "terze parti":

Trustpilot / SiteJabber: Cerca il nome del negozio su queste piattaforme per leggere le recensioni degli altri utenti. Attenzione alle recensioni troppo simili tra loro o scritte in un italiano stentato.

ScamAdviser: Inserisci l'URL del sito per ottenere un punteggio di affidabilità basato su algoritmi che analizzano l'età del dominio e la sua collocazione geografica.

Verifica Partita IVA: Puoi usare il sito dell'Agenzia delle Entrate per verificare se la Partita IVA indicata sul sito esiste ed è attiva.

3. Come smascherare truffe dei rivenditori sui Marketplace

Sulle piattaforme di compravendita tra privati, il rischio è maggiore. Ecco come difenderti:

Analisi delle Foto: Diffida di foto generiche prese dal web o da cataloghi. Chiedi sempre al venditore delle foto reali del prodotto, magari con un foglietto accanto con scritta la data odierna.

Comunicazione Esterna: Se un venditore ti chiede di spostare la conversazione fuori dalla piattaforma (es. su WhatsApp o Telegram), rifiuta sempre. Le chat ufficiali ti proteggono legalmente.

Metodi di Pagamento: Mai accettare pagamenti tramite ricarica Postepay, bonifici istantanei o "Invio di denaro ad amici" su PayPal. Questi metodi non sono rimborsabili.

Urgenza e Pressione: I truffatori spesso usano un linguaggio allarmante ("Azione richiesta", "L'offerta scade tra un'ora") per non farti riflettere.

Errori e Link: Fai attenzione a messaggi con errori grammaticali o ortografici e non cliccare mai su link sospetti che sembrano portare a pagine di login della piattaforma.

Buone pratiche per scongiurare una Truffa

Proteggere i propri dispositivi:

1. Attiva l'Autenticazione a Due Fattori (2FA): Fallo su tutti gli account (e-mail, social, banca). Questo impedisce agli hacker di accedere anche se conoscono la tua password.

2. Usa Password Forti e Diverse: Non utilizzare la stessa password per più servizi. Utilizza un Password Manager per generare e conservare password complesse.

3. Aggiorna il Software: Mantieni sempre aggiornati il sistema operativo, il browser e l'antivirus. Gli

aggiornamenti contengono patch di sicurezza contro le vulnerabilità note.

4. Permessi alle App: Perché una App "Torcia" vuole leggere i tuoi SMS? Perché un "Solitario" vuole accedere ai contatti? Se un'app chiede permessi strani, NON installarla.

Setup pratico per l'autenticazione a 2 fattori sulle principali piattaforme.
Google/Gmail Account Google -> Sicurezza -> Verifica in due passaggi.
Facebook / Meta: Impostazioni e Privacy -> Password e Sicurezza -> Autenticazione a due fattori.
Amazon: Il mio account -> Accesso e sicurezza -> Verifica in due fasi.
WhatsApp: Impostazioni -> Account -> Verifica in due passaggi (Qui è un PIN che protegge il numero).
App Bancarie: Entrare nelle impostazioni dell'app e cercare la voce Sicurezza, Privacy e Account

Comandamenti della Banca online

1. **L'App Ufficiale è il Porto Sicuro:** Non entrate nel conto dal browser (Chrome/Safari) del telefono cercando "Banca X" su Google (potreste finire su un sito clone). Usate solo l'App ufficiale scaricata dallo Store.

2. Monitora gli Estratti Conto Controlla regolarmente le transazioni bancarie. Segnala immediatamente alla banca qualsiasi operazione non autorizzata.

3. Effettua sempre il Logout: quando finisci di usare l'app, entra nelle opzioni ed effettua il logout.

4. Notifiche Push attive: Sarai sempre avvisato in tempo delle operazioni effettuate dal tuo conto; se non hai autorizzato l'operazione, la Notifica ti permette di saperlo in anteprima e bloccare il conto.

5. Fuori casa, usa i TUOI dati: Se devi controllare il conto fuori casa, spegni il Wi-Fi e usa la tua connessione 4G/5G. È molto più difficile da intercettare.Non c'è campo? Usal la VPN.

6. Link SMS non si clicca: Se la banca ti scrive "Conto bloccato", non cliccare. Apri l'App ufficiale e controlla lì. Se è vero, troverai un avviso dentro l'App

7. **Aggiornamenti** Tieni aggiornata l'app e il sistema operativo del telefono

Riepilogo dei concetti fondamentali

Questo percorso ha costruito una comprensione operativa completa delle trappole digitali e delle truffe online, muovendo dai meccanismi invisibili della navigazione quotidiana fino alle tecniche di manipolazione psicologica più sofisticate usate dalla cybercriminalità.

La navigazione online lascia tracce continue e spesso invisibili: cookie tecnici, analitici e di profilazione; cronologia e storico delle ricerche nel browser; indirizzo IP registrato da ogni sito visitato. Gestire consapevolmente queste tracce bloccando i cookie di terze parti, cancellando periodicamente la cronologia, usando la navigazione in incognito sui dispositivi non propri, è la base di una vita digitale più rispettosa della propria privacy.

La navigazione in incognito protegge soltanto dalle tracce locali sul dispositivo, non rende anonimi verso il fornitore di internet o i siti visitati. La VPN offre una protezione molto più profonda: cifra tutto il traffico, nasconde l'indirizzo IP e protegge le comunicazioni anche su reti Wi-Fi pubbliche. Verificare l'URL prima di inserire dati sensibili (controllando HTTPS, il lucchetto, il dominio reale) e applicare il principio del privilegio minimo ai permessi delle app sono due delle competenze di sicurezza più importanti e immediatamente applicabili.

Il social engineering è il cuore di quasi tutte le truffe digitali: manipola le emozioni invece di attaccare i sistemi. I tre grimaldelli (paura, urgenza, avidità) si riconoscono dallo stesso schema: un messaggio che provoca una reazione emotiva intensa e chiede un'azione immediata. Fermarsi cinque minuti prima di agire è la difesa più semplice e più efficace. Phishing, smishing e vishing sono i tre canali principali attraverso cui questi grimaldelli vengono consegnati.

Gli otto scenari descritti, dal finto pacco al romance scam, dal phishing bancario al man in the middle e ai trojan bancari, condividono la stessa struttura: una situazione plausibile, una verità nascosta e una strategia di difesa specifica. I quattro comandamenti della banca online (app ufficiale, rete mobile, no ai link via SMS, controllo dei permessi) sono la sintesi pratica applicabile ogni giorno.

> La difesa migliore contro le truffe digitali non è tecnica: è culturale. Chi conosce le trappole raramente ci cade. Chi sa come funziona il social engineering si ferma prima di agire. La conoscenza è il migliore antivirus che esiste e non ha bisogno di aggiornamenti.

Test di autovalutazione

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

1. Quale tipo di cookie traccia il comportamento dell'utente attraverso molti siti diversi per creare profili pubblicitari? a) Cookie tecnici. b) Cookie analitici. c) Cookie di terze parti e profilazione.

2. La navigazione in incognito nasconde la tua attività: a) Al tuo fornitore di internet. b) Al sito che stai visitando. c) Soltanto alle altre persone che usano lo stesso dispositivo.

3. Qual è la principale differenza tra phishing e spear phishing? a) Il phishing usa l'email, lo spear phishing usa gli SMS. b) Lo spear phishing è personalizzato sulla vittima, il phishing è generico. c) Il phishing è più pericoloso.

4. Quale di questi URL è sicuro per accedere a Facebook? a) https://facebook-login.com — b) http://www.facebook.com — c) https://m.facebook.com — d) https://faceboook.com

5. Quale grimaldello emotivo usa il messaggio: 'Il tuo conto sarà bloccato in 24 ore!'? a) Avidità. b) Paura e urgenza. c) Curiosità.

6. Cosa fare quando appare un pop-up che dice "VIRUS RILEVATO! Chiama il supporto al numero..."? a) Chiamare subito il numero. b) Non chiamare, chiudere il browser o spegnere il PC. c) Scaricare il programma di pulizia suggerito.

7. Perché è rischioso fare operazioni bancarie su Wi-Fi pubblico? a) Le reti pubbliche sono lente e le transazioni potrebbero fallire. b) Un attaccante sulla stessa rete potrebbe intercettare o modificare le comunicazioni. c) Le app bancarie bloccano l'accesso da Wi-Fi pubblico.

8. Quale permesso non dovrebbe avere quasi nessuna app, tranne quella bancaria ufficiale? a) L'accesso alla posizione solo mentre l'app è in uso. b) La lettura degli SMS. c) L'accesso alla fotocamera per fare foto.

Risposte: 1-c / 2-c / 3-b / 4-c / 5-b / 6-b / 7-b / 8-b

Autovalutazione delle competenze DigComp 2.2

Compila questa scheda prima e dopo il percorso formativo. Per ciascuna voce, indica il tuo livello su una scala da 1 a 5, dove 1 significa "non mi sento ancora in grado" e 5 significa "mi sento completamente autonomo".

Competenza	Prima (1–5)	Dopo (1–5)
So cosa sono i cookie e come gestirli consapevolmente		
Conosco i limiti reali della navigazione in incognito		
So verificare la sicurezza di un URL prima di inserire dati		
Riconosco i tre grimaldelli emotivi del social engineering		
So distinguere phishing, smishing e vishing		
Conosco i 4 comandamenti della sicurezza bancaria online		
So come comportarmi su reti Wi-Fi pubbliche		
So gestire i permessi delle app secondo il principio del privilegio minimo		

Competenza	Prima (1–5)	Dopo (1–5)
So cosa fare se ricevo un messaggio sospetto dalla mia banca		
So come segnalare una truffa alle autorità competenti		

Glossario essenziale

Clickbaiting: tecnica di manipolazione che usa titoli emotivamente intensi, incompleti o iperbolici per indurre clic su contenuti di scarsa qualità o fuorvianti. Sfrutta curiosità, paura e indignazione come leve.

Cookie: piccolo file di testo salvato nel browser durante una visita a un sito web, usato per ricordare informazioni tra una sessione e l'altra. Esistono in tre categorie principali: tecnici, analitici, di profilazione.

Cookie di terze parti: cookie installati da domini diversi dal sito che si sta visitando, usati da reti pubblicitarie per tracciare il comportamento dell'utente attraverso molti siti diversi e costruire profili commerciali.

HTTPS: protocollo di comunicazione cifrato (la "S" sta per Secure) che garantisce la trasmissione sicura dei dati tra browser e sito. Necessario — ma non sufficiente — per fidarsi di un sito con dati sensibili.

Man in the Middle: attacco informatico in cui un terzo si inserisce tra due comunicanti su una rete non sicura, intercettando o modificando i dati trasmessi. Particolarmente pericoloso sulle reti Wi-Fi pubbliche.

Navigazione in incognito: modalità del browser che non salva cronologia, cookie e dati localmente sul dispositivo. Non garantisce l'anonimato verso ISP, siti visitati o chi monitora la rete.

Phishing: frode digitale via e-mail che imita comunicazioni ufficiali per indurre l'utente a inserire credenziali su siti falsi. Le varianti per canale: smishing (SMS/WhatsApp), vishing (telefono).

Principio del privilegio minimo: regola di sicurezza che suggerisce di concedere a programmi e app solo i permessi strettamente necessari alle loro funzioni dichiarate, revocando tutto il resto.

Romance scam: truffa basata sulla costruzione artificiale di una relazione affettiva online, seguita da richieste di denaro urgenti motivate da emergenze inventate.

Session hijacking: furto di una sessione di navigazione attiva — tipicamente bancaria — da parte di un attaccante che si trova sulla stessa rete e non effettua il logout.

Social engineering: manipolazione psicologica sistematica per indurre le persone a rivelare informazioni riservate o compiere azioni dannose. Bypassa i sistemi tecnici di sicurezza agendo sulle vulnerabilità umane.

Spear phishing: variante personalizzata del phishing in cui l'attaccante ha studiato preventivamente la vittima per rendere il messaggio più credibile e difficile da riconoscere.

Tech support scam: truffa del finto supporto tecnico, realizzata attraverso falsi pop-up d'allarme che inducono la vittima a chiamare un numero e a concedere l'accesso remoto al dispositivo.

Trojan bancario: malware camuffato da app innocua che sovrappone interfacce false alle app bancarie reali per sottrarre credenziali, oppure intercetta gli SMS con i codici OTP.

Typosquatting: tecnica di truffa che registra domini con piccoli errori tipografici rispetto a quelli originali (es. faceboook.com) per ingannare gli utenti distratti.

VPN (Virtual Private Network): tecnologia che crea un tunnel cifrato per tutto il traffico internet, nascondendo l'indirizzo IP reale dell'utente e proteggendo le comunicazioni anche su reti pubbliche.

Contatti utili in caso di truffa

Polizia Postale: commissariatodips.it — sportello online per segnalare reati informatici, truffe online e phishing, attivo 24 ore su 24.

Garante per la Protezione dei Dati Personali: gpdp.it — per segnalare violazioni della privacy e richiedere informazioni sui propri diritti digitali.

AGCM — Antitrust: agcm.it — per segnalare pratiche commerciali scorrette e truffe nell'e-commerce.

CERT-AgID: cert-agid.gov.it — pubblica aggiornamenti in tempo reale sulle campagne di phishing e malware in circolazione in Italia.

Arbitro Bancario Finanziario: arbitrobancariofinanziario.it — per ricorsi in caso di controversie con banche o intermediari finanziari relativi a operazioni non autorizzate.

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 percorso si inserisce nel Tema B — Sicurezza e Uso Consapevole dei Servizi Digitali — e risponde alle competenze 4.1 (Proteggere i dispositivi), 4.2 (Proteggere i dati personali e la privacy) e 4.4 (Proteggere la salute e il benessere) del 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.