ABI Associazione Bancaria Italiana

CERTFin

GUIDA CONTRO LE TRUFFE DIGITALI

Fidarsi è un click. Proteggersi, un po' di più. Come evitare le trappole del web

Dall'Intelligenza Artificiale ai grandi classici delle truffe: tutto quello che devi sapere per difendere i tuoi dati e i tuoi soldi

Con la diffusione dei canali digitali e dei servizi interconnessi, molte attività della vita quotidiana si svolgono oggi online. Ogni giorno utilizziamo strumenti digitali per informarci, comunicare, fare acquisti, gestire il conto, effettuare pagamenti e accedere a servizi sempre più connessi tra loro. Oggi, proteggere l'identità personale e digitale è una **necessità quotidiana** per muoversi in rete con serenità.

I moderni cybercriminali non colpiscono più soltanto i sistemi informatici, ma agiscono sul "**fattore umano**", cioè sulle emozioni, sulle abitudini e sui comportamenti delle persone. Utilizzano infatti tecniche evolute di **ingegneria sociale**, vale a dire strategie di manipolazione psicologica pensate per indurre le persone a compiere azioni rischiose, come comunicare informazioni riservate, condividere codici personali o autorizzare pagamenti. Queste tecniche possono essere rese ancora più credibili grazie a strumenti di ultima generazione, come il deepfake — immagini, video o audio creati o alterati con sistemi di Intelligenza Artificiale — e la clonazione della voce, che può far sembrare reale una richiesta proveniente da una persona conosciuta o da un soggetto apparentemente affidabile.

Sfruttando leve psicologiche ed emotive, come l'ansia per un finto conto bloccato, la paura di una sanzione o l'urgenza di una scadenza imminente, spingono le persone a fare un click di troppo, a condividere codici personali o ad autorizzare transazioni finanziarie.

Questa guida nasce per offrirti **indicazioni semplici e concrete** per riconoscere i principali tentativi di truffa, proteggere i tuoi dati personali e bancari e utilizzare gli strumenti digitali in modo più sicuro, consapevole e responsabile.

QUALI SONO LE PRINCIPALI NOVITA'? SCOPRILO NELLE PAGINE SUCCESSIVE

I TRUFFATORI COME SFRUTTANO L'IA (INTELLIGENZA ARTIFICIALE) PER TENDERE LE LORO TRAPPOLE?

I truffatori usano l'IA per clonare voci, generare e-mail, SMS e messaggi praticamente indistinguibili da quelli autentici, creare video falsi o chatbot che si spacciano per operatori della tua banca o per familiari.
L'obiettivo di queste tecniche è creare una situazione credibile e urgente, spingendoti ad agire d'impulso, ad esempio effettuando un pagamento o condividendo informazioni personali, senza darti il tempo di verificare.

Come puoi difenderti?

Anche se un messaggio, una voce o un video sembrano autentici, è sempre importante fermarsi, mantenere la calma e verificare l'identità dell'interlocutore attraverso canali ufficiali prima di compiere qualsiasi azione. Nel dubbio, interrompi la comunicazione e contatta direttamente il familiare, la tua banca o la Polizia Postale.

IN COSA CONSISTE LA TRUFFA DI FINTI OPERATORI CHE SEGNALANO LA PRESENZA DI OPERAZIONI SOSPETTE SUL TUO CONTO?

In questo tipo di truffa, un malintenzionato si finge operatore della banca o agente delle forze dell'ordine (ad esempio della Polizia Postale) e ti contatta sostenendo che i tuoi risparmi sono a rischio a causa di presunte operazioni sospette.
Per aumentare la pressione, viene creata una situazione di urgenza e ti viene detto che l'unico modo per mettere al sicuro il denaro è trasferirlo immediatamente su un cosiddetto "conto sicuro". In realtà, quel conto è sotto il controllo del truffatore, e il denaro trasferito viene sottratto definitivamente.

Come puoi difenderti?

Diffida di chi ti contatta chiedendo di spostare denaro con urgenza; ricorda che né la banca né le Forze dell'Ordine chiedono mai trasferimenti su altri conti; non seguire istruzioni ricevute telefonicamente, soprattutto se riguardano pagamenti o codici di sicurezza.
In caso di dubbio, interrompi la comunicazione e verifica contattando la tua banca o le autorità tramite canali ufficiali.

TI VIENE CHIESTO DI COMUNICARE UN CODICE OTP (ONE TIME PASSWORD – PASSWORD DA UTILIZZARE UNA SOLA VOLTA) O DI AUTORIZZARE UN'OPERAZIONE TRAMITE L'APP BANCARIA?

Nessuna banca, Forza dell'Ordine o ente legittimo ti chiederà mai di comunicare un codice OTP, una password o di autorizzare un'operazione sul conto via telefono, e-mail o messaggio. Se ricevi una richiesta di questo tipo, potresti essere di fronte a un tentativo di truffa.

Come puoi difenderti?

Interrompi la comunicazione e contatta direttamente la banca utilizzando i canali ufficiali.

COME RICONOSCERE I SITI WEB BANCARI CONTRAFFATTI?

Sono siti quasi identici a quelli ufficiali delle banche, spesso con una finestra pop-up in cui inserire le credenziali, ma ricorda, i siti ufficiali non usano pop-up.

Come puoi difenderti?

In passato questi siti si riconoscevano da design scadente ed errori di ortografia. Oggi però possono apparire perfetti. La difesa più efficace resta non fidarsi mai dei link ricevuti e digitare l'indirizzo manualmente o usare l'app ufficiale. E ricorda… se la banca deve comunicarti qualcosa di importante, te lo segnalerà quando accedi al tuo Internet banking.
In caso di dubbio, chiama il servizio clienti della Banca.

GHOST BROKING (POLIZZE FANTASMA)

Il ghost broking è la truffa delle polizze fantasma: paghi per un'assicurazione che in realtà non viene mai attivata.

Attratto da prospettive di risparmio incredibili, ti ritrovi con una copertura non valida; nelle r.c. auto, oltre a multe e fermo del veicolo, in caso di incidente rischi di dover pagare di tasca tua i danni. I siti sembrano quelli di compagnie reali e a volte rubano l'identità a intermediari iscritti al RUI (Registro Unico Intermediari), consultabile sul sito dell'IVASS.

Come puoi difenderti?

Diffida delle offerte assicurative a prezzi fuori mercato; controlla i dati dell'intermediario consultando il RUI; pretendi un preventivo dettagliato e verificalo contattando direttamente la compagnia.
Non pagare mai soggetti non iscritti al RUI e diffida di chi comunica solo via chat.

DOWNLOAD PERICOLOSI E MALWARE

Scaricando file da siti, e-mail o SMS potresti installare un malware (da «malicious» e «software»): programmi nascosti in allegati, giochi o app gratuite, fatti per rubare i tuoi dati o controllare a distanza il dispositivo.

Sebbene alcuni dispositivi infetti possano mostrare rallentamenti, pop-up frequenti o malfunzionamenti, molte minacce informatiche moderne agiscono senza sintomi facilmente riconoscibili.

Come puoi difenderti?

Scarica file e app solo da fonti attendibili e store ufficiali; mantieni attive le protezioni di sicurezza del sistema operativo e, dove previsto, utilizza antivirus aggiornati; non aprire allegati provenienti da mittenti sconosciuti.
Fai attenzione anche a quelli inviati dagli amici, i cui dispositivi potrebbero essere infetti a loro insaputa.

TI VIENE PROPOSTO UN INVESTIMENTO CON GUADAGNI FACILI O RENDIMENTI GARANTITI?

Fai molta attenzione. Diffida delle offerte che promettono guadagni elevati senza rischi, utilizzano immagini di personaggi famosi o prevedono contatti insistenti tramite telefono, social network o WhatsApp. Nessun investimento legittimo può garantire rendimenti elevati e privi di rischio.

Come puoi difenderti?

Prima di investire, verifica sempre l'affidabilità dell'intermediario e non prendere decisioni sotto pressione.

I GRANDI CLASSICI: PERCHÉ NON DOBBIAMO ABBASSARE LA GUARDIA

Se l'Intelligenza Artificiale e i falsi e-commerce rappresentano le nuove frontiere del cybercrimine, ci sono tecniche storiche che non passano mai di moda. Parliamo di phishing, smishing e vishing.

Anche se ne sentiamo parlare da anni, queste trappole continuano a mietere vittime perché sanno rinnovarsi, cambiando "abito" e sfruttando le nostre distrazioni quotidiane.

Come puoi difenderti?

Per un ripasso su come riconoscere e difendersi da phishing, smishing e vishing, consulta la guida dedicata già pubblicata.

E infine… Se pensi di essere stato vittima di una truffa?

Agisci rapidamente per limitare eventuali danni:

- blocca immediatamente carte e strumenti di pagamento eventualmente compromessi;
- contatta il Servizio Clienti della tua banca per segnalare l'accaduto;
- modifica le password e le credenziali che potrebbero essere state esposte;
- conserva e-mail, messaggi, ricevute e qualsiasi altra prova utile;
- presenta una denuncia alla Polizia Postale o alle altre Forze dell'Ordine competenti;
- controlla con attenzione il conto e i movimenti della carta nei giorni successivi.

Ricorda: intervenire tempestivamente può contribuire a ridurre le conseguenze della truffa e facilitare eventuali procedure di contestazione o rimborso.

Guide realizzate da ABI e CertFin in collaborazione con le Associazioni dei Consumatori