
BUY
I NAVIGATI
INFORMATI E SICURI

Consigli per navigare in sicurezza

Il mondo del web è meraviglioso, ma può nascondere delle insidie!

Quali sono i principali rischi online e come ti puoi difendere?

Scoprilo insieme a "i Navigati", una famiglia esperta di cybersecurity!

Cos'è il Social engineering?

Nel social engineering i frodatori usano diverse tecniche per manipolarti psicologicamente, acquisire la tua fiducia e spingerti con l'inganno a comunicare i tuoi dati personali, con lo scopo di rubare la tua identità, accedere al tuo conto corrente, usare le tue carte per fare acquisti, attivare nuovi conti bancari o svolgere attività illegali a tuo nome.

Come funziona?

Per convincerti a fornire informazioni riservate il frodatore fa leva sulla tua emotività, curiosità, fiducia o paura attraverso messaggi di allarmismo e urgenza.

Cosa fare?

- Presta molta attenzione alle **informazioni che diffondi online**, ad esempio sui social: puoi fornire materiale utile ai frodatori.
- **Accertati della reale identità** di chi ti contatta, perché i criminali si spacciano per persone di cui pensiamo di poterci fidare, come un superiore o un operatore della tua banca.
- Chiediti se la situazione che ti viene presentata è realistica e, **se non sei sicuro, verifica.**
- Se una situazione ti sembra sospetta non avere fretta e non fornire i tuoi dati riservati o i tuoi documenti di identità.
- **Non condividere le tue credenziali** di internet banking o i dati delle tue carte di pagamento. La tua banca non ti contatta mai per chiederti queste informazioni.
- Se pensi di aver condiviso informazioni personali o bancarie con un frodatore contatta subito la tua banca.

Cos'è il Vishing?

Il Vishing (voice + phishing) è una frode che usa le chiamate telefoniche per ingannarti e rubare i tuoi dati.

Come funziona?

Il frodatore si presenta al telefono come un operatore del servizio clienti o del reparto antifrode della tua banca. Una volta ottenuta la tua fiducia, cercherà di carpire informazioni riservate e finanziarie e proverà con una scusa a farti autorizzare dei pagamenti o trasferire denaro.

Cosa fare?

- Fai attenzione alle chiamate indesiderate che creano senso di **urgenza** o **pressione** e **non ti fidare** se ti vengono chiesti al telefono dati di accesso al conto, codici delle carte o pin dispositivi.
- **Verifica il numero di telefono sul web**, potresti non essere il primo ad aver subito questo tentativo di frode!
- Se hai dubbi, **non avere fretta e non fornire dati**. Chiudi la telefonata e chiama l'assistenza clienti della tua banca.
- **Non condividere** il pin delle carte, le tue credenziali di accesso al conto online o altre **informazioni riservate**.
- **Non trasferire denaro** ad account sconosciuti e **non fornire codici** per autorizzare pagamenti.
- Se pensi di essere rimasto vittima di una truffa o di aver condiviso per errore i tuoi dati con i frodatori, contatta immediatamente la tua banca.

Cos'è lo Smishing?

Lo Smishing è una frode utilizzata per tentare di acquisire le tue informazioni riservate o bancarie tramite SMS.

Come funziona?

Ad esempio, fingendo nell'SMS di essere la tua banca, il tuo e-commerce preferito o il tuo gestore telefonico, i frodatori ti invitano con una scusa a cliccare su un link o a chiamare un numero di telefono per verificare operazioni sospette o riattivare il tuo account. Attento! In realtà il link porta a un sito falso e al numero di telefono risponde un frodatore che cercherà di rubare i tuoi dati!

Cosa fare?

- Se ti arriva un SMS con un link **non cliccare** e **non inserire i tuoi dati**, nemmeno se ti dice che hai meno di 5 minuti per riattivare il tuo conto!
- Verifica online il numero di telefono o confrontalo con i contatti ufficiali della tua banca.
- Anche se il numero che ti scrive sembra quello della tua banca, **non fidarti** se contiene link o se ti vengono chiesti i dati bancari.
- La tua banca non ti contatterà mai via SMS per invitarti a cliccare su un link o chiederti informazioni di sicurezza come username, pin, password o codici autorizzativi del tuo conto online o delle tue carte di pagamento.
- Se pensi di essere rimasto vittima di una frode o di aver condiviso per errore i tuoi dati con i truffatori, contatta immediatamente la tua banca.

Cos'è lo Spoofing?

Lo Spoofing è una tecnica con cui **il frodatore riesce a mascherare il suo reale numero** per far apparire come mittente di un SMS o numero chiamante un contatto legittimo della tua banca, come ad esempio quello di una filiale o del Servizio Clienti.

Come funziona?

Attraverso lo spoofing il frodatore riesce a inviare comunicazioni (tramite chiamata telefonica o SMS) da un numero di telefono o da un contatto che sembra essere quello autentico di una banca.
Se ricevi una telefonata o un SMS di questo tipo, potresti erroneamente fidarti e mettere in atto le azioni richieste dal frodatore, come ad esempio cliccare su un link, autenticarti su un sito, comunicare dati sensibili o effettuare operazioni online.

Cosa fare?

- **Sospetta** di chiamate e sms che creano senso di **urgenza** o **pressione**.
- Ricorda che il nome o il numero del chiamante / mittente che leggi sul display del tuo telefono può non essere autentico!
- **Non fornire le tue credenziali** di internet banking o i dati delle tue carte di pagamento.
- **Non trasferire denaro** ad account sconosciuti se la richiesta non ti convince.

Cos'è la Truffa sentimentale?

Nelle truffe sentimentali i malintenzionati prendono di mira le vittime sui social network, ma possono utilizzare anche i siti di incontri online o le email per prendere contatto.

Come funziona?

Qualcuno che hai recentemente incontrato online dichiara di provare forti sentimenti per te e ti chiede di chattare in privato.
Una volta ottenuta la tua fiducia, con un pretesto ti chiederà denaro, regali oppure i dati della tua carta di credito.

Cosa fare?

- Fai attenzione alle informazioni personali che condividi sui social.
- **Cerca le foto** delle persone con cui chatti **sui motori di ricerca online** per verificare che siano autentiche e che non siano già state utilizzate da altri profili.
- **Fai attenzione a errori** di ortografia e grammatica, **incongruenze** nelle loro storie e scuse poco plausibili.
- **Non inviare mai denaro** e non fornire i dettagli delle tue carte di pagamento, del conto online o copie di documenti personali.
- **Controlla il tuo conto** e verifica eventuali pagamenti effettuati senza la tua autorizzazione.
- Se pensi di aver condiviso queste informazioni con un truffatore contatta subito la tua banca.

Cos'è la truffa degli Acquisti online?

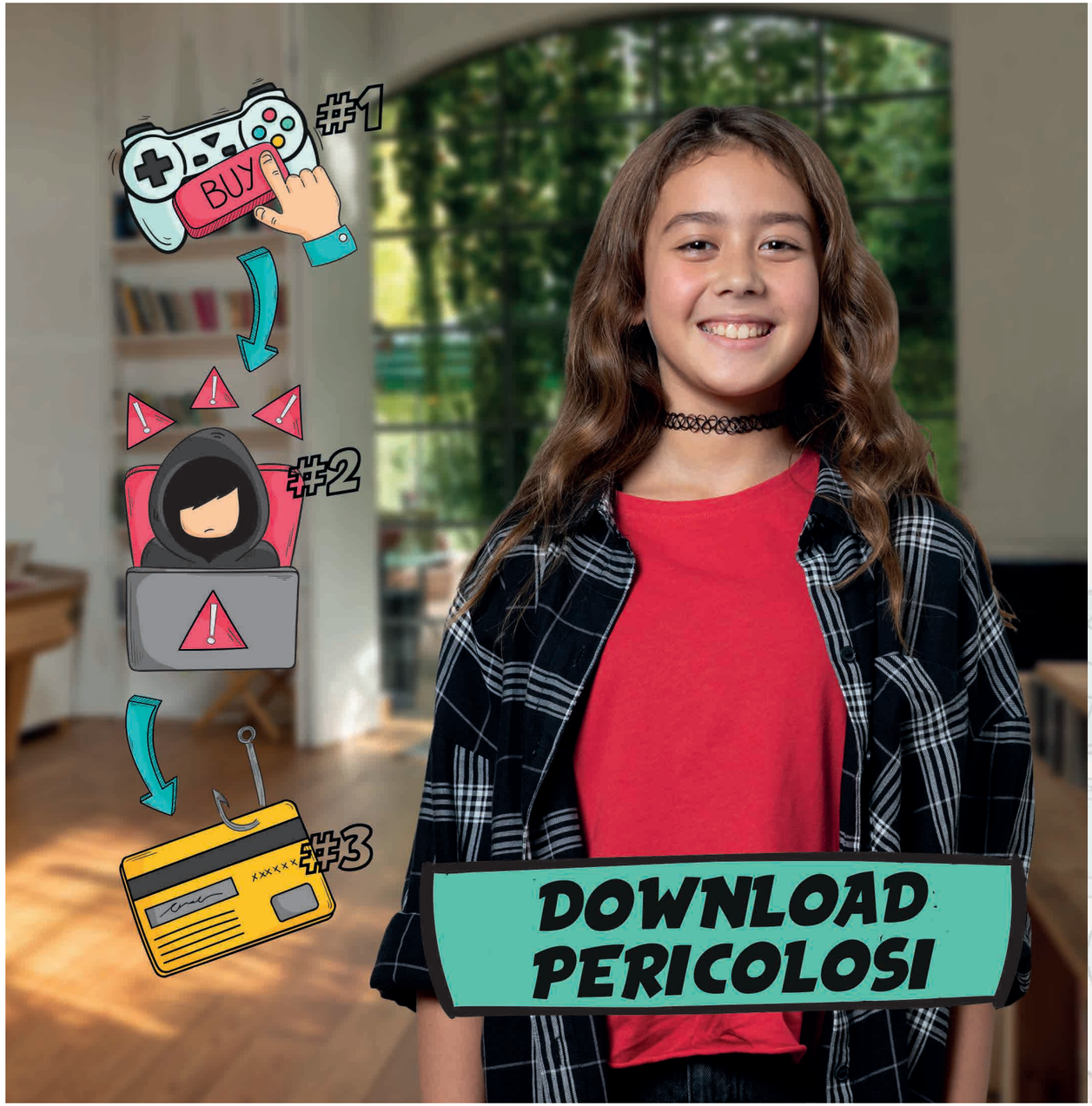
Nella truffa degli acquisti online i truffatori cercano di manipolarti per acquisire le tue informazioni personali e finanziarie o per ricevere pagamenti facendo leva su offerte imperdibili e sconti pazzeschi.

Come funziona?

I truffatori, utilizzando **falsi siti di e-commerce** spesso simili a quelli ufficiali, ti propongono acquisti vantaggiosi, **offerte, premi, sconti o prodotti miracolosi**. Oltre a richiedere pagamenti per acquisti che potresti non ricevere mai, sfruttando il falso sito di e-commerce potrebbero rubare i dati e le tue informazioni finanziarie e di pagamento, come i codici della tua carta.

Cosa fare?

- Leggi sempre i commenti e i feedback di altri acquirenti e, in generale, **fai ricerche sul venditore** prima di acquistare online.
- Assicurati che il sito su cui acquisti sia noto e riporti informazioni sull'azienda e dati di contatto del venditore.
- Effettua il pagamento solo attraverso una **connessione Internet sicura**: evita di utilizzare wifi pubblici o non protetti.
- Preferisci siti che, per proteggere il tuo pagamento online, richiedono, dopo l'inserimento dei dati della carta, di confermare l'operazione ad es. tramite impronta digitale, riconoscimento facciale, notifica push o codice via SMS.
- Attenzione agli annunci di affari spropositati o prodotti miracolosi: **se ti sembra troppo bello per essere vero, probabilmente è una truffa!**



Cosa sono i Download pericolosi?

Quando effettui un download da siti, email o SMS potresti scaricare dei software malevoli progettati dai frodatori per rubare le tue informazioni personali, finanziarie e di sicurezza.

Come funzionano?

Utilizzando siti ad hoc, email o SMS, i frodatori ti spingono a scaricare allegati, giochi online o app gratuite. In realtà quello che scarichi è un software malevolo che viene utilizzato per rubare i tuoi dati o per controllare a distanza i tuoi dispositivi.

Cosa fare?

- Scarica file e app solo da **fonti attendibili** e **store ufficiali**.
- Installa un **antivirus** su computer, smartphone e tablet e mantienilo sempre aggiornato.
- Fai periodicamente il **backup** dei tuoi dati e tieni sempre aggiornato il sistema operativo dei tuoi dispositivi.
- **Non aprire allegati di email o SMS ricevuti da mittenti sconosciuti**.
- Fai attenzione anche alle email con allegato ricevute dagli amici: i loro dispositivi potrebbero essere stati infettati a loro insaputa.

Cos'è il SIM swap?

Significa letteralmente **"scambio della SIM"**: i frodatori convincono con l'inganno il tuo gestore di telefonia mobile a spostare il tuo numero su una nuova scheda SIM controllata da loro. Sulla nuova SIM intercettano tutti gli SMS, fra cui quelli inviati dalla tua banca, che utilizzano per operare sul tuo conto bancario.

Come funziona?

Prima dello scambio, per rubare i tuoi dati i frodatori utilizzano tecniche di hacking o di social engineering. Con i tuoi dati creano falsi documenti con cui **chiedono all'operatore telefonico una nuova SIM**, con la scusa di averla persa o danneggiata. La tua SIM smette improvvisamente di funzionare e i frodatori, attraverso lo stesso numero telefonico (ora in loro possesso), ottengono dalla tua banca le autorizzazioni per operare sul tuo conto online.

Cosa fare?

- Se noti che il tuo telefono ha perso inaspettatamente il segnale **contatta** subito **il tuo gestore telefonico**, potrebbe riuscire a bloccare lo scambio della SIM prima che quella del frodatore venga attivata.
- **Non spegnere il telefono** anche se ricevi chiamate fastidiose.
- Se il tuo gestore telefonico ti avvisa di un improvviso blocco della linea potrebbe essere in corso la clonazione della SIM: contattalo immediatamente e verifica l'informazione ricevuta.
- **Controlla il tuo conto** e verifica eventuali pagamenti effettuati senza la tua autorizzazione.
- Se pensi di essere vittima di SIM swap contatta subito la tua banca per mettere in sicurezza il conto e le tue carte di pagamento.

Cos'è il Money Muling?

Il Money Muling è una truffa che prevede trasferimento o riciclaggio di denaro illegale, dietro facile compenso e talvolta in modo inconsapevole da parte della vittima.

Come funziona?

I truffatori attraverso falsi annunci di lavoro, social media o contatti diretti convincono con l'inganno le vittime a trasferire denaro ottenuto illegalmente tra diversi conti bancari, anche esteri, sotto il controllo dei truffatori.
I money mule ricevono in cambio il pagamento di una commissione per il servizio fornito. Anche se non sono coinvolti direttamente nei crimini da cui proviene il denaro, svolgono un'attività illegale perché aiutano, anche inconsapevolmente, i criminali a riciclare facilmente denaro in tutto il mondo rimanendo anonimi.

Cosa fare?

- **Fai qualche ricerca** prima di accettare un'offerta di lavoro che sembra imperdibile.
- **Verifica i dettagli di contatto dell'azienda** che ti fa un'offerta di lavoro e controlla che sia registrata nel tuo Paese.
- Diffida in particolare delle offerte di lavoro inattese da parte di persone o aziende all'estero, perché è più difficile per te scoprire la loro legalità.
- **Non comunicare le coordinate del tuo conto bancario** o altri dati personali a persone di cui non hai piena fiducia.
- Sii molto cauto con le email o i contatti non richiesti sui social media che promettono facili guadagni.

Cos'è il Ghost Broking?

Per Ghost Broking intendiamo la truffa delle polizze fantasma, in cui la vittima paga per dei servizi assicurativi che in realtà non vengono attivati.

Come funziona?

Le persone si lasciano incantare da prospettive di risparmio incredibili e acquistano delle polizze spinte da offerte vantaggiose, ma poi si ritrovano con una **copertura assicurativa non valida**.
Nel caso delle polizze r.c. auto, oltre a multe e fermo amministrativo del veicolo, in caso di incidente il responsabile rischia anche di dover pagare i danni causati!
I siti che offrono queste polizze false sembrano simili a quelli di compagnie e intermediari realmente esistenti. A volte i truffatori, per trarre in inganno le vittime, usano marchi di compagnie note e rubano l'identità a intermediari assicurativi realmente iscritti nel **RUI (Registro Unico Intermediari)**.

Cosa fare?

- Diffida di offerte assicurative a **prezzi fuori mercato**.
- Controlla sempre i **dati identificativi** degli intermediari consultando il RUI.
- Pretendi la consegna di un **preventivo dettagliato** e verificalo contattando direttamente l'impresa assicurativa.
- Non pagare mediante bonifici o ricariche di carte prepagate a favore di persone non iscritte nel RUI.
- Non pagare mai soggetti non iscritti nel RUI.
- Diffida dei venditori che comunicano solo via chat.

Entra nella famiglia de' I Navigati

Segui i consigli de' **I Navigati,**
una famiglia che di cybersecurity se ne intende!

inavigati.it

Insieme a voi per la sicurezza dei servizi finanziari

BANCA D'ITALIA
EUROSISTEMA

IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

ABI Associazione Bancaria Italiana

CERTFin

BNL
BNP PARIBAS

Con il patrocinio del

25 1997-2022 GPDP
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI