



Protezione Anti-Truffa

Riconoscere messaggi falsi, link pericolosi
e richieste sospette.

Digital Senior Routine™

Guida pratica stampabile

Cosa imparerai in questa guida

- ✓ Perché le truffe colpiscono tutti e come difendersi.
- ✓ Come riconoscere i finti messaggi su WhatsApp e via SMS.
- ✓ Cosa sono i link pericolosi e perché non vanno toccati.
- ✓ La regola d'oro per non farsi rubare dati o soldi.
- ✓ Cosa fare subito se pensi di aver sbagliato.



NOTA IMPORTANTE

Questa guida fa parte del tuo kit digitale stampabile. Leggila con calma. Nessuno può rubarti nulla dal telefono se tu non gli dai il permesso. Imparare a riconoscere l'inganno è il tuo scudo migliore.

Perché le truffe funzionano

Molte persone pensano che i truffatori siano dei geni del computer capaci di entrare magicamente nei telefoni. La verità è molto diversa e molto più semplice.

I truffatori non "hackerano" il tuo telefono. Ingannano la tua mente. Per farlo, usano tre armi molto potenti:

la fretta, la paura e la confusione.

Ti fanno credere che ci sia un'emergenza: un conto bloccato, un pacco in giacenza, un figlio nei guai. Quando sei spaventato o hai fretta, smetti di pensare lucidamente e fai esattamente quello che vogliono loro.

● RICORDA: IL METODO FERMATI, CONTROLLA, CHIEDI

Ogni volta che ricevi un messaggio urgente che ti chiede di fare qualcosa subito, la prima cosa da fare è **fermarti**. La fretta è il nemico. Respira e non fare nulla d'impulso.

Messaggi falsi su WhatsApp

Una delle truffe più comuni arriva direttamente su WhatsApp, da un numero sconosciuto. Il messaggio di solito dice una cosa del genere:

"Ciao mamma/papà, ho perso il telefono e sto usando quello di un amico. Questo è il mio nuovo numero, salvalo. Ho bisogno di un favore urgente, mi devi pagare una bolletta perché non ho accesso alla banca."

Il tuo istinto di genitore o nonno ti spinge ad aiutare subito. Ma è una trappola. Il truffatore cerca di isolarti facendoti credere che tuo figlio sia irraggiungibile sul vecchio numero.

● PASSO PRATICO

Se ricevi un messaggio del genere, usa il metodo **fermati, controlla, chiedi**. Chiama tuo figlio sul suo "vecchio" numero (quello vero che hai in rubrica). Il 99% delle volte ti risponderà tranquillamente e scoprirai che sta benissimo e ha ancora il suo telefono.

SMS sospetti e finti pacchi

Ricevere un messaggio normale (SMS) sul telefono è ormai raro, per questo quando ne arriva uno ci facciamo subito caso. I truffatori lo sanno e inviano SMS fasulli che sembrano provenire dai corrieri (BRT, Poste, GLS).

Il testo tipico è:

"Il tuo pacco è bloccato in dogana. Paga 2 euro per lo sblocco cliccando su questo link."

Spesso clicchiamo per curiosità, anche se non aspettiamo nessun pacco. Oppure, per pura coincidenza, stiamo davvero aspettando un ordine e pensiamo sia quello.

● ATTENZIONE: NON CLICCARE MAI I LINK NEGLI SMS

Applica il metodo **Leggi — Controlla — Fai™**. Leggi il messaggio. Controlla: stai aspettando un pacco? Se sì, vai sul sito ufficiale del negozio dove hai comprato, non cliccare la scritta blu nell'SMS. Nessun corriere ti chiede 2 euro per sbloccare un pacco tramite SMS.

Email phishing (la pesca dei dati)

La parola "Phishing" (si legge *fishing*) viene dall'inglese e significa "pescare". Il truffatore lancia una rete con migliaia di email false, sperando che qualcuno "abbocchi" all'amo.

Queste email sembrano inviate da aziende vere: usano il logo dell'INPS, dell'Agenzia delle Entrate, o della tua banca. Spesso dicono che c'è un rimborso a tuo favore, oppure che devi rinnovare i tuoi dati, altrimenti il servizio verrà sospeso.

Il trucco sta nel farti cliccare su un pulsante dentro l'email che ti porterà su una pagina falsa, creata apposta per rubare le informazioni che scriverai.

● RICORDA

Loghi e colori si possono copiare in due minuti. Non fidarti mai dell'aspetto di un'email. Nessun ente ufficiale ti promette soldi facili via email chiedendoti di inserire le coordinate bancarie cliccando su un bottone.

Finte banche, Poste, INPS

I truffatori sono diventati molto abili. A volte riescono a far arrivare i loro finti SMS esattamente nello stesso punto in cui ricevi i veri messaggi della tua banca o delle Poste. Questo fa sembrare il messaggio autentico.

Potrebbero scriverti:

"Accesso anomalo al tuo conto. Clicca qui per bloccarlo."

La reazione immediata è lo spavento. Si ha paura di perdere i propri risparmi. Ma è proprio quella paura che ti fa commettere l'errore.

SE TI BLOCCHI O HAI PAURA

Chiudi il messaggio. Apri tu, manualmente, l'applicazione ufficiale della tua banca o delle Poste, come fai tutti i giorni. Se c'è un vero problema, troverai un avviso direttamente dentro l'applicazione ufficiale, non tramite un SMS o un link.

Richieste di password, PIN e codici

Il PIN del bancomat, la password dell'applicazione e i codici di conferma (OTP) che arrivano via SMS sono le chiavi della tua casa digitale.

Regola assoluta e universale: **nessun operatore vero ti chiederà mai questi codici**. Nemmeno se ti telefona dicendo di essere il direttore della banca, nemmeno se sembra gentilissimo e ti chiama per nome.

Se qualcuno ti telefona dicendo:

"C'è un bonifico in partenza, per bloccarlo mi legga il codice di 6 cifre che le è appena arrivato per SMS"

sta cercando di rubarti i soldi. Quel codice serve per AUTORIZZARE, non per bloccare.

● ATTENZIONE

Non inviare mai codici, non leggere mai a voce numeri arrivati per SMS, non mandare mai soldi a sconosciuti. Se ti chiedono un PIN o un codice OTP, riattacca immediatamente il telefono.

Link sospetti e urgenza artificiale

Un "link" è quella scritta azzurra (o sottolineata) che, se toccata, ti porta su un sito web. Nelle truffe, il link è la botola sotto i tuoi piedi. Finché non la calpesti, sei al sicuro.

Per farti cliccare, il truffatore crea una "urgenza artificiale". Ti dice che hai tempo solo 12 ore, oppure che il conto verrà chiuso entro oggi, o che la multa raddoppierà domattina.

● PASSO PRATICO

Usa il metodo **Leggi — Controlla — Fai™** per togliere potere al truffatore: fermati e aspetta un'ora. Fatti un caffè. L'urgenza è sempre finta. Se aspetti un'ora, la mente torna lucida e capirai subito che si trattava di un inganno.

Checklist finale anti-truffa

Tieni a mente queste semplici regole e la tecnologia sarà solo uno strumento utile, mai un pericolo.

✓ CHECKLIST FINALE

Non mi faccio mettere fretta da messaggi o telefonate (l'urgenza è quasi sempre finta).

Se mio figlio/nipote mi scrive da un "nuovo numero", lo chiamo al suo vecchio numero per verificare.

Non clicco mai sui link (le scritte blu) arrivati via SMS.

Se ricevo un'email preoccupante da banca o Poste, non clicco, ma apro l'app ufficiale per controllare.

Non do MAI il mio PIN o i codici OTP arrivati per SMS, a nessuno.

Se ho un dubbio, mi applico la regola: **Fermati, controlla, chiedi** a un familiare.

⚠ SE HAI INSERITO I DATI PER ERRORE

Non provare vergogna. Succede a migliaia di persone ogni giorno. Chiedi subito aiuto a un familiare, oppure chiama il numero verde della tua banca (cercalo su un foglio ufficiale, non sul messaggio falso) e chiedi di bloccare la carta o l'accesso.