

BONUS 2

Checklist Anti-Truffa

Le 15 cose da controllare prima di cliccare su un link o rispondere a un messaggio.

La tua difesa più potente

I truffatori sfruttano la tua buona fede, la fretta o la paura. Questa checklist è il tuo scudo: 15 domande semplici ma potentissime per proteggerti ogni giorno.

NOTA IMPORTANTE

Le truffe funzionano perché non ci diamo il tempo di pensare. Un minuto di controllo salva i tuoi risparmi.

Come usare questo bonus

Questa non è una guida da studiare a memoria.
È uno strumento pratico che diventa un'abitudine.

Il metodo: Fermati, Controlla, Chiedi

LEGGI

Leggi il messaggio senza toccare nessun link. Non avere fretta.

CONTROLLA

Usa le 15 domande di questa checklist per analizzare il messaggio.

FAI

Decidi se ignorare, cancellare o chiedere aiuto a un familiare.

PASSO PRATICO

Vai all'ultima pagina (Pagina 8). Troverai le 15 domande pronte da stampare. Stampale e tienile sul frigorifero o vicino alla scrivania.

SE TI BLOCCHI O HAI DUBBI

Se una domanda ti fa accendere un allarme, fermati. Chiudi il messaggio. Non succede nulla di grave se aspetti un giorno per verificare.

Chi mi scrive e cosa vuole?

Inizia sempre controllando il mittente e la natura della sua richiesta.

1

Conosco chi mi ha scritto?

Se ricevi un SMS o email da un numero sconosciuto o indirizzo strano, la prudenza deve essere massima.

2

Mi stanno mettendo fretta?

"Scade tra 24 ore", "Il tuo conto verrà chiuso oggi". Se ti mettono fretta, è quasi certamente una truffa.

3

Mi chiedono password o codici?

Nessun operatore o banca ti chiederà MAI il tuo PIN, password o codice OTP via SMS.

4

Mi chiedono soldi?

Richieste di pagare piccole somme o messaggi da finti parenti. Fermati sempre davanti a una richiesta di denaro.

Link, errori e allarmi finti

I truffatori usano pretesti specifici per farti cliccare su indirizzi pericolosi.

5

Il link sembra strano?

Un link vero è poste.it. Uno finto sarà poste-aggiornamento-sicurezza.com. Se è lungo o strano, non cliccarlo.

6

Ci sono errori nel testo?

Errori di grammatica, parole sbagliate o italiano poco chiaro? Spesso i truffatori usano traduttori automatici.

7

Parlano di conto bloccato?

"Conto bloccato" o "carta sospesa" è l'esca più comune. Serve a spaventarti per farti inserire i dati della carta.

8

Parlano di pacco bloccato?

Ti dicono che manca 1,50€ per lo sdoganamento? Non cliccare e non pagare. È una truffa diffusissima.

Promesse e richieste anomale

Fai molta attenzione se ti offrono qualcosa di troppo bello o se vogliono i tuoi dati.

9

Promettono premi o soldi?

"Hai vinto uno smartphone!", "Buono spesa da 500€". Nessuno regala niente su Internet. Sono tentativi di rubare i tuoi dati.

10

Mi chiedono di installare qualcosa?

Se un finto avviso ti dice di scaricare un'App urgente, fermati. Le banche non ti costringono a scaricare nulla tramite SMS.

11

Mi chiedono dati personali?

Le aziende serie hanno già i tuoi dati. Se ti chiedono di reinserirli, stai per regalarli a un truffatore.

12

Il mittente sembra falso?

Controlla l'indirizzo email reale, non solo il nome. "Poste Italiane" potrebbe venire da info@xyz123.com.

Urgenza e verifica sicura

Gli ultimi controlli prima di prendere qualsiasi decisione.

13

Mi chiedono di agire subito?

Qualsiasi comunicazione che richiede un'azione immediata è pensata per non farti ragionare. Ignora l'urgenza.

14

Posso verificare da un sito ufficiale?

NON cliccare il link nel messaggio. Apri l'App ufficiale della banca o chiama il numero verde. Scoprirai che era tutto falso.

15

Posso chiedere a qualcuno prima di cliccare?

Nel dubbio, l'unica azione corretta è non agire. Chiama un figlio, un nipote o un amico esperto prima di fare qualsiasi mossa.

ATTENZIONE

Non provare vergogna se hai quasi creduto a un messaggio falso. I truffatori ingannano persone di ogni età. Il traguardo è sapersi fermare prima di cliccare.

Esempi di messaggi sospetti

Ecco come si presentano nella realtà. Memorizza queste tipologie.

La truffa del pacco in giacenza (SMS)

"PosteInfo: Il tuo pacco IT48392 è fermo. Manca il pagamento di 1,90€. Paga entro 24h o tornerà indietro. Clicca qui: <http://poste-sbloccopacco.com>"

Perché è finto: Ti mette fretta, ti chiede soldi, il link non è quello vero delle Poste.

La truffa del conto bloccato (Email)

"Gentile Cliente, abbiamo notato un accesso anomalo. Per sicurezza la sua carta è bloccata. Per riattivarla verifichi i suoi dati cliccando sul bottone. Accesso Sicuro."

Perché è finto: La banca non blocca le carte chiedendoti di sbloccarle da un link.

La truffa del "finto figlio" (WhatsApp)

"Ciao mamma, mi è caduto il telefono. Questo è il mio nuovo numero. Mi serve un favore urgente, devo pagare una bolletta. Mi fai un bonifico?"

Perché è finto: Chiama il vecchio numero di tuo figlio. Non inviare mai soldi a numeri sconosciuti.

La tua Checklist Stampabile

Se rispondi SÌ anche a una sola domanda, fermati: è probabilmente una truffa.

Posso chiedere a un familiare prima di fare qualsiasi cosa?

- ☐ Il mittente è un numero sconosciuto o strano?
- ☐ Mi stanno mettendo fretta per decidere?
- ☐ Mi stanno chiedendo di inserire il PIN o la password?
- ☐ Mi stanno chiedendo soldi o di fare un bonifico urgente?
- ☐ Il link contiene parole strane o errori?
- ☐ Il testo del messaggio ha errori di grammatica?
- ☐ Mi dicono che il mio conto bancario è stato bloccato?
- ☐ Mi dicono che c'è un pacco fermo in dogana?
- ☐ Mi promettono in regalo uno smartphone o dei buoni spesa?
- ☐ Mi chiedono di scaricare e installare un programma?
- ☐ Mi chiedono di inserire i miei dati personali da zero?
- ☐ L'indirizzo email del mittente non corrisponde al nome?
- ☐ Mi dicono che se non clicco perderò qualcosa?
- ☐ Ho cliccato ma la pagina non mi sembra quella ufficiale?
- ☐ Mi chiedono di agire subito senza pensare?

RICORDA: Se una comunicazione è inattesa o crea urgenza, considerala falsa fino a prova contraria.