

Scopri come riconoscere i tentativi di frode e furto d'identità.

Esistono varie tipologie di truffe elaborate per carpire notizie e dati personali allo scopo di realizzare frodi e furto d'identità. Conoscerle ti permette di evitare di diventarne vittima. Ecco alcuni consigli pratici da seguire per difenderti da possibili attacchi.

Ricorda, la banca non ti contatterà mai via e-mail, SMS o telefono per chiedere i tuoi dati personali, le credenziali di accesso, i tuoi codici segreti o i dettagli dei tuoi rapporti bancari.



Frode tramite telefono

- Diffida di coloro che si definiscono operatori di banca e chiedono informazioni personali o di effettuare operazioni non chiare
- Verifica l'attendibilità delle segnalazioni
- Non cedere alle pressioni o a ipotetiche urgenze
- Non comunicare i tuoi dati al telefono, in particolare codici o credenziali.



Frode tramite sms

- Non cliccare in nessun caso sui link presenti in un SMS
- Verifica il mittente dell'SMS e presta attenzione ai numeri anche se sembrano reali o noti
- Diffida degli SMS con avvisi urgenti sulla sicurezza o di riscatto di somme in denaro
- Verifica con la tua banca o con il servizio clienti in caso di SMS sospetti



Frode tramite e-mail

- Verifica il mittente dell'e-mail anche se sembra corretto e la presenza di errori di grammatica e ortografia
- Controlla che i toni non siano intimidatori e che non comunichino urgenza
- Non cliccare mai sui link presenti in e-mail sospette o inaspettate
- Non fornire in nessun caso le tue credenziali bancarie o altri codici riservati.



Frode tramite sito clone o applicativi

- Non cliccare su link ma digita direttamente tu l'indirizzo
- Controlla la presenza dell'icona "lucchetto" vicino all'indirizzo URL del sito e cliccaci sopra per verificare i dettagli sull'intestatario del certificato
- Fai attenzione agli allegati e-mail che potrebbero installare un virus per reindirizzare la tua navigazione web su un sito fittizio o cambiare il beneficiario del pagamento.