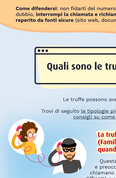
Dalla telefonata sospetta all'email ingannevole:

scopri come difenderti

In un'epoca in cui fuse dei canali digitali e della interazioni a distanza è sempre più difficoltoso, adottare misure adeguate per navigare online in sicurezza è fondamentale. Proteggere i propri dati, riconoscere le minacce e adottare comportamenti prudenti è essenziale per evitare rischi. Ad esempio, ricevere una chiamata o un messaggio da parte di sedicenti amici/conoscenti che paiono in tono di urgenza può essere utilizzato per manipolarte, ottenere la loro fiducia e indurre a effettuare pagamenti per tramite un guadagno facile o cedere informazioni personali.

In questa guida esplorano come possono avvenire, fornendo consigli chiari e pratici per navigare online in sicurezza.

Come si può manifestare una truffa al telefono o on-line?



Ad esempio, potrebbe proporti un investimento, anche piccolo, o l'acquisto, o comunicarti informazioni sensibili. Il tutto, con la scusa di aiutare amici/conoscenti o richiedere consigli molto diversi da quanto pubblicizzato. Questo può accadere perché sotto la pressione di una notizia non verificata, non spinta a eseguire un pagamento ad un soggetto sconosciuto, fidandosi sempre, il truffatore cerca di strumentalizzarti e manipolarti, sfruttando la tua buona fede nei confronti di persone a cui hai normalmente non faresti, agendo sul tuo punti deboli per avvantaggiarsene.

Cli Spoofing: attenzione al numero falsificato

Il "Caller ID Spoofing" o **cli spoofing** è una tecnica utilizzata dai truffatori per **falsificare il numero di una chiamata in entrata che appare sul display del telefono**. Questo serve a rendere più credibile una forte affiliabile, come una banca, un ente pubblico o un familiare. In questo modo la vittima è portata a fidarsi e a condividere dati personali, codici di sicurezza o autorizzare transazioni. Il numero che appare sul display del telefono, in realtà, è falsato fare credendo di interagire con un soggetto legittimo, con conseguenza economiche e di sicurezza grave. Inoltre, **identificare il truffatore è difficile**, poiché il numero è camuffato.

Come difendersi: non fidarti del numero visualizzato sul display e in caso di dubbio, **intervengi la chiamata e richiama tramite un numero ufficiale reperito da fonti sicure** (sito web, documenti ufficiali).

Quali sono le truffe più comuni?

Le truffe possono avere diverse forme.

Trovi di seguito la tipologie più comuni di truffa e alcuni consigli su come può evitarle:

La truffa dell'urgenza familiare (family Emergency Scam): quando la paura prende il sopravvento

Questa truffa sfrutta il senso di responsabilità e preoccupazione verso i propri cari. I truffatori chiamano la vittima e si fingono un familiare in difficoltà e si spacciano per figure autorevoli, come avvocati o poliziotti, sostenendo di voler aiutare un tuo parente nel guai, ad esempio un figlio coinvolto in un grave incidente. Utilizzano il tono di panico del momento, i truffatori ti chiedono di inviare urgentemente del denaro tramite bonifico, ricarica prepagata o app di pagamento istantanea, tendono a negare ogni sfiducia, trattenendo denaro o condividendo informazioni sensibili. **Per evitare** di cadere in questa trappola, è fondamentale **cercare una calma e mantenere una lucidità e non razionalità**, analizzando la verisimiglianza dei contenuti riportati dal manipolatore. **Prima di agire**, contatta direttamente il tuo parente tramite numeri noti per verificare la situazione. **Diffidare** di richieste improvvise di denaro, specialmente se arrivano da numeri sconosciuti. Evitare di essere "di pancia" è la scelta migliore per tutelarti.

La truffa del blocco del pagamento (Blocking Payment Scam)

Un'altra truffa molto diffusa consiste nel segnalare alla vittima un presunto blocco su un pagamento o su un conto bancario. I truffatori, fingendosi operatori del servizio clienti o un operatore di banca, ti chiedono di molto spesso proprio della tua cui - di un fornitore di servizi finanziari o di un ente istituzionale. Inviano messaggi sms - o email o chiamano la vittime per chiedere dati/ricevere dati. Il tono usato è spesso di "emergenza" la situazione è significata o corrette funzionamento. Il mancato di conseguenze immediate, come penali o la sospensione del conto, ha l'obiettivo di spingere ad agire in fretta.

Le difese migliore è ignorare questi messaggi e **non fornire mai** informazioni personali tramite canali non verificati. **Se hai dubbi**, contattare direttamente la tua banca attraverso i numeri ufficiali, **ma non cliccare mai** su link e non aprire allegati sospetti. **Ricorda** infatti che la banca non ti chiederà mai in questo modo nella relazione con la sua clientela.

La truffa del falso investimento (Fake Investment Scam): il miraggio dei guadagni facili

Questa truffa consiste nel promettere investimenti molto vantaggiosi, con rendimenti straordinari e senza rischi, attirando le persone con l'ingenuità. I truffatori inviano e-mail o messaggi sui social media, o tramite chiamate telefoniche, promettendo offerte apparentemente legittime. Tuttavia, una volta che la vittima versa i soldi, il denaro scompare e i responsabili diventano irraggiungibili.

Per evitare di questo tipo, fai attenzione agli investimenti sicuri e realistici non arrivano mai attraverso messaggi non richiesti. **Prima di agire, verifica** sempre l'**affidabilità** della controparte e **rivolgiti** a un consulente finanziario o di fiducia.

Un'altra minaccia è il **SIM swap**, in cui i truffatori trasferiscono il tuo numero di telefono su una SIM controllata da loro, permettendo così accessi ai tuoi account bancari e sociali. Questo avviene convincendo il tuo operatore telefonico a emettere una nuova SIM con il tuo numero, bloccando la tua e prendendo il controllo dei codici di sicurezza inviati via SMS.

Infine, non mancano i **falsi siti di e-commerce**, che attirano i consumatori con prezzi stracciati per problemi che non verranno mai consegnati.

Allo stesso modo, i **social media** possono rappresentare un terreno fertile per i malintenzionati, che usano le informazioni condivise sui profili personalizzate i loro attacchi.

Vediamo qualche **esempio**:

Le **smishing** è un tipo di phishing che utilizza messaggi di testo e servizi di messaggistica per appropriarsi di dati personali. In pratica, ricevi un SMS che sembra provenire da una fonte affidabile, come la tua banca, e che ti invita a cliccare su un link per risolvere un problema.

Vishing è una forma di truffa telefonica che combina la parola "voice" e "phishing". Consiste in una tecnica usata dai truffatori per ottenere informazioni sensibili, come dati bancari, codici di accesso o credenziali personali. Attraverso una chiamata vocale, spesso falsificando operatori di banca, enti pubblici o aziende affidabili, cercano di indurre la vittima a compiere azioni contro il loro interesse.

Anche le app di **messaggistica istantanea**, come **WhatsApp, telegram o Instagram**, possono talvolta essere usate per truffe. I truffatori possono inviare messaggi di phishing, messaggi che riproducono schemi di truffa già citati in precedenza come il family emergency scam o il falso blocco di pagamento offerta (avvisi fasulli per ottenere dati personali o denari).

* Il phishing è una tecnica con cui si tenta di ottenere informazioni sensibili, come password, informazioni bancarie, l'originale un'entità affidabile tramite e-mail, messaggi o siti web fraudolenti.

Messaggi, email e chiamate sospette: riconoscere phishing, smishing e vishing su ogni canale

- **Mittenti sconosciuti**: i truffatori spesso utilizzano numeri di telefono non salvati in rubrica o con prefissi internazionali inusiti
- **Messaggi allarmistici**: questi messaggi sostengono minacciano la chiusura di un account o richiedono azioni immediate per risolvere un problema falso
- **Errori ortografici e grammaticali**: i messaggi di phishing possono contenere errori di scrittura o traduzioni approssimative
- **Richieste di informazioni personali**: i truffatori chiedono spesso di condividere dati sensibili come password, OTP o informazioni finanziarie
- **Link sospetti**: i link forniti possono sembrare legittimi ma sono in realtà falsi e progettati per rubare dati sensibili. Whatsapp può contrassegnare alcuni link come sospetti
- **Attenzione**: controlla scrupolosamente l'URL per individuare eventuali errori o piccole modifiche che potrebbero essere apparentemente simili ai siti web ufficiali. Ricorda che se la URL inizia con https non significa che il sito sia legittimo, significa solo che è una connessione sicura. In caso di dubbi, evita di cliccare sul link e digita l'indirizzo direttamente nel tuo specifico browser. Gmail e Whatsapp possono segnalare alcuni automaticamente i link sospetti. **Meglio evitare di cliccare se non sei sicuro**
- **Tono urgente**: i messaggi cercano di creare un senso di urgenza per spingere a rispondere senza riflettere
- **Richiesta di pagamenti su canali non convenzionali**: i truffatori, al fine di rendere più difficile la loro identificazione, spesso richiedono pagamenti tramite canali non convenzionali, anche anche tramite mezzi tracciabili come bonifici bancari o carte di credito. Tra i metodi preferiti figurano il prelievo di contanti, l'effettuazione di acquisti che non lasciano tracce evidenti, trasferimenti di denaro o bonifici verso conti terzi, dai quali è difficile recuperare i fondi. Questi metodi rendono le transazioni difficili da tracciare. Gli acquisti "non tracciabili" includono, ad esempio, l'acquisto di criptovalute, crediti per il gioco d'azzardo online o beni facilmente monetizzabili su internet. Tra questi beni figurano spesso biglietti aerei, buoni acquisto o carte regalo di vario tipo.

Cosa fare in caso di messaggi sospetti

1

- **Ignora e blocca: non rispondere** ai messaggi sospetti e **blocca immediatamente** i contatti sconosciuti
- **Non cliccare link non verificati: verifica sempre l'autenticità** di un link prima di aprirlo

- **Mantieni l'App aggiornata**: gli **aggiornamenti** spesso **correzioni** per vulnerabilità note
- **Proteggi i tuoi dati: evita di condividere** documenti sensibili o informazioni bancarie tramite WhatsApp

Come fare per proteggersi?

Per proteggerti dalla truffe e anche dalle frodi online ci sono alcune semplici regole da seguire:

- **non condividere mai** informazioni personali o finanziarie tramite SMS, e-mail o chiamate non richieste
- **evita di** cliccare su link o aprire allegati in messaggi sospetti
- **mantieni** i tuoi dispositivi aggiornati e **utilizza** software antivirus affidabili, **custodisci con cura** le credenziali di accesso ai conti online e i codici delle carte di pagamento
- **usa** password forti e uniche per ciascun account, attivando l'autenticazione a due fattori, dove possibile
- **monitora** regolarmente i movimenti bancari e segnala immediatamente qualsiasi attività sospetta alla tua banca
- **fai attenzione** a messaggi che sollecitano ad azioni immediate che comportano esborsi di denaro o governo sensazioni di panico crescente, **diffida** di presunti operatori bancari che ai telefono chiedono informazioni personali o codici di sicurezza. Non fare operazioni fondi, offrendoti di farlo direttamente
- **diffida** di persone che si presentano come "amici" e segnalano situazioni di pericolo di familiari o conoscenti. **Verifica** sempre personalmente la situazione senza dar corso a richieste di invio di denaro

- **quadra il tuo cellulare non sia più in grado di effettuare/ricevere chiamate, verifica** i motivi contattando il tuo operatore telefonico.

Cosa fare se sei vittima di truffa o frode

Se sei stato vittima di un tentativo di phishing o rilevi attività sospette sul tuo conto, **agisci subito**. **Contatta** la tua banca, **blocca** le carte e/o l'operatività sul tuo conto bancaria **o** denunciare l'accaduto alla Polizia postale e delle comunicazioni. Inoltre, **controlla** attentamente i movimenti sulla tua banca/carti per assicurarti che non ci siano ulteriori operazioni sospette. Nel caso un addebito che non hai autorizzato comunica alla banca il disconoscimento dell'operazione di pagamento e chiedi il rimborso della somma addebitata.

Se l'interlocuzione con l'istituto finanziario non ti soddisfa, puoi inoltrare un reclamo alla banca che deve rispondere nel termine di 15 giorni lavorativi.

Se il reclamo non è stato accolto o la risposta non ti convince puoi presentare un esposto alla Banca d'Italia. Inoltre, puoi presentare un ricorso all'Arbitro Bancario Finanziario (ABF) per contestare il comportamento ritenuto irregolare o scorretto.

Ricorda: la tua banca non ti chiederà mai dati sensibili via SMS, e-mail o telefono. Se ricevi una richiesta sospetta, verifica sempre prima di agire.

Vuoi saperne di più?
Scopri di più sulla sicurezza online visitando il sito https://navigaci.certfin.it/. Troverai video, guide pratiche, documenti pensati per aiutarti a riconoscere e prevenire le truffe digitali.

Navigaci è una campagna di cybersecurity awareness realizzata dal CERTFin in collaborazione con Banca d'Italia, ABI, IVASS, Polizia di Stato e il settore Bancario Italiano. L'obiettivo è fornire strumenti e informazioni utili per affrontare le minacce informatiche in modo consapevole, proteggendo i tuoi dati e le tue transazioni.

OSSIF CERTFin
ASSOCIAZIONE BANCARIA ITALIANA · ACU · CONFCOMMERCIO · ALTROCONSUMO · ADOCONSUMO · CONFIMPRESE · CONSUMERS FORUM · CODACONS · CITTADINANZATTIVA · MOVIMENTO CONSUMATORI · U.N.C.Tem.
Realizzato da ABI Servizi S.p.A. - Luglio 2026