# Dalla telefonata sospetta all'email ingannevole: scopri come difenderti

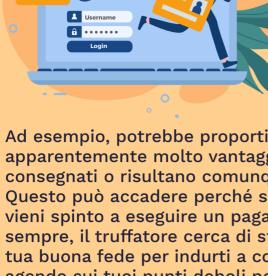
In un'epoca in cui l'uso dei canali digitali e delle interazioni a distanza è

sempre più diffuso, 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 attuare i tentativi di truffe sono persone molto esperte che sfruttano emozioni come la paura e il senso di urgenza delle potenziali vittime per manipolarle, ottenere la loro fiducia e indurle a effettuare pagamenti per trarne un guadagno illecito o cedere informazioni personali. In questa guida esploriamo come possono avvenire, fornendo consigli chiari e pratici per navigare online in sicurezza.

Come si può manifestare una truffa

## Si tratta sostanzialmente di un inganno con cui il truffatore, mediante trucchi o trappole opportunamente predisposte, ti



apparentemente molto vantaggioso, di beni o servizi che poi non vengono consegnati o risultano comunque molto diversi da quanto pubblicizzato. Questo può accadere perché sotto la pressione di una notizia non verificata, vieni spinto a eseguire un pagamento ad un soggetto sconosciuto. Quasi sempre, il truffatore cerca di strumentalizzarti e manipolarti, sfruttando la tua buona fede per indurti a compiere azioni che normalmente non faresti,

agendo sui tuoi punti deboli per avvantaggiarsene. CLI Spoofing: attenzione al numero falsificato +0938281003 Il CLI Spoofing è una tecnica utilizzata dai truffatori per falsificare il numero di una chiamata in entrata che appare sul display del telefono, facendolo sembrare quello di una RISPONDI... fonte affidabile, 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

# buona fede credendo di interagire con un soggetto legittimo, con conseguenze economiche e di sicurezza gravi. 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, interrompi 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 <u>le tipologie più comuni di truffa e alcuni</u>

La truffa dell'urgenza familiare

chiamano la vittima e si fingono un familiare in

(Family Emergency Scam):

quando la paura prende il sopravvento Questa truffa sfrutta il senso di responsabilità e preoccupazione verso i propri cari. I truffatori

panico del momento, i truffatori ti chiedono di inviare urgentemente del denaro per risolvere la presunta emergenza. Le vittime, colte alla sprovvista, tendono a reagire senza riflettere, trasferendo denaro o condividendo informazioni sensibili. Per evitare di cadere in questa trappola, è fondamentale non cedere alla pressione emotiva e valutare con razionalità, analizzando la veridicità dei contenuti riportati dal manipolatore. Prima di

migliore per tutelarsi. 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 comunque un operatore di banca molto spesso proprio della tua! – di un fornitore di servizi finanziari o di un ente istituzionale, inviano messaggi sms - o email o chiamano le vittime per chiedere dati

## La difesa migliore è ignorare questi messaggi e non fornire mai informazioni personali tramite canali non verificati. Se hai dubbi, contatta direttamente la tua banca attraverso i numeri ufficiali, ma non cliccare mai su link e non

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'inganno. I truffatori inviano e-mail o messaggi sui social media, oppure effettuano chiamate, presentando offerte apparentemente legittime. Tuttavia,

sospensione del conto, ha l'obiettivo di spingerti ad agire



che sembra provenire da una fonte affidabile, come la

tua banca, e che ti invita a cliccare su un link per

Anche le app di messaggistica istantanea, come Whatsapp, Telegram o Instagram, possono talvolta essere utilizzate dai criminali per veicolare messaggi di phishing, messaggi che riproducono via chat schemi

finanziario di fiducia. -

Un'altra minaccia è il SIM SWap, in cui i truffatori trasferiscono il tuo numero telefonico su una SIM controllata da loro, ottenendo cosi accesso ai tuoi account bancari e social. Questo avviene convincendo il tuo operatore telefonico a emettere una nuova SIM a loro favore, bloccando la tua e prendendo il controllo

una volta che la vittima versa i soldi, il denaro

Se ricevi offerte di questo tipo, fai attenzione. Gli investimenti sicuri e redditizi non arrivano mai attraverso messaggi non richiesti. Prima di agire, verifica sempre l'affidabilità della controparte e rivolgiti a un consulente

scompare e i responsabili diventano

irraggiungibili.

denaro attraverso i canali bancari a fini fraudolenti (ad es. furto di credenziali o dati personali che vengono successivamente usati per accedere ai tuoi conti bancari o social, senza che tu ne sia consapevole). Vediamo qualche esempio:

Le minacce possono determinare sia reati di truffa (per es. inganno diretto per convincerti a cliccare su un link o a fornire informazioni)

risolvere un problema.

Il **vishing** è una forma di truffa telefonica che combina le parole "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 fingendosi operatori di banca, enti pubblici o aziende affidabili, cercano di indurre le vittime a compiere azioni contro il



loro interesse.

di truffa già citati in precedenza come il family emergency scam o il job scam (proporti offerte di lavoro fasulle per ottenere dati personali o denaro). 'Il phishing è una truffa informatica che mira a ottenere dati sensibili, come password o informazioni bancarie, fingendosi 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

Attenzione: controlla scrupolosamente l'URL per individuare se l'indirizzo del sito web online presenta caratteri 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,

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

Cosa fare in caso di messaggi sospetti

verifica l'affidabilità del sito tramite recensioni online o app specifiche. Anche app come WhatsApp possono segnalare 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 il pagamento attraverso canali non convenzionali,

trasferimenti. Gli acquisti "non tracciabili" possono includere,

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

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

Ignora e blocca: non rispondere ai messaggi

sospetti e blocca immediatamente i

verifica sempre l'autenticità di un link

Non cliccare link non verificati:

WhatsApp

Come fare per

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

> non condividere mai informazioni personali o

o chiamate non richieste

mantieni i tuoi dispositivi

richieste di invio di denaro

finanziarie tramite SMS, e-mail

evita di cliccare su link o aprire allegati in messaggi sospetti

proteggersi?

contatti sconosciuti

prima di aprirlo

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 monitora regolarmente i ciascun account, attivando movimenti bancari e segnala l'autenticazione a due fattori, immediatamente qualsiasi

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 allo stesso che deve rispondere nel termine di 15 giorni

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?** 

I Navigati 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



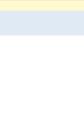




CODACONS

迄 U.Di.Con,







ABISERVIZI S.p.A.- Settembre 2025



operazioni finanziarie. Il **rischio principale** è quello di agire in

consigli su come puoi evitarle:

difficoltà o si spacciano per figure autorevoli, come avvocati o poliziotti, sostenendo di voler aiutare un tuo parente nei guai, ad esempio un figlio o un nipote coinvolto in un grave incidente. Sfruttando il

agire, interrompi la conversazione e contatta direttamente il familiare per verificare la situazione. Diffida di richieste improvvise di denaro, specialmente se arrivano da numeri sconosciuti. Evitare di agire "di pancia" è il modo

personali o finanziari con l'obiettivo di "sbloccare" la situazione e ripristinare il corretto funzionamento. La minaccia di conseguenze immediate, come penali o la

aprire allegati sospetti. Ricorda infatti che la banca non agisce mai in

in fretta.

come di frode digitale, cioè tentativi diretti ad accedere al tuo Lo **smishing** è un tipo di phishing<sup>1</sup> che utilizza messaggi di testo e servizi di messaggistica per appropriarsi di dati personali. In pratica, ricevi un SMS

insoliti Messaggi allarmistici: questi messaggi solitamente 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

anziché 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 poi possibile prelevare fondi, effettuare ulteriori acquisti o

carte regalo di vario tipo

dove possibile

direttamente

fai attenzione a messaggi che

crescente, diffida di presunti

che segnalano la necessità di

chiedono informazioni personali o

spostare fondi, offrendosi di farlo

qualora il tuo cellulare non sia più in grado di effettuare/ricevere chiamate, verifica i motivi contattando il tuo

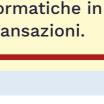
••• Cosa fare se sei vittima di truffa o frode Se sei stato vittima di un tentativo di phishing o rilevi attività sospette sul tuo conto, agisci subito. Contatta la tua banca, blocca le carte e/o l'operatività sul tuo internet banking e denuncia l'accaduto alla Polizia

lavorativi.

operatore telefonico.

attività sospetta alla tua banca diffida di persone che si sollecitano ad azioni immediate presentano come "amici" e che comportano esborso di denaro segnalano situazioni di pericolo e generano sensazioni di pericolo di familiari o conoscenti. Verifica sempre personalmente operatori bancari che al telefono la situazione senza dar corso a

postale e delle comunicazioni. Inoltre, controlla attentamente i movimenti sui tuoi conti bancari per assicurarti che non ci siano ulteriori operazioni sospette. Nel caso un addebito che non hai autorizzato





CONFCONSÛMATORI APS

CONSUMATORI ACP consumo lavoro cittadinanza Casa del onsumatore

🔊 ASSOCIAZIONE

LEGA CONSUMATOR

pensati per aiutarti a riconoscere e prevenire le truffe digitali.





MOVIMENTO

**CONSUMATORI**