Valle Sabbia non solo News

QUI RURALE – "A BUON RENDERE" DOSSIER

Bestiario delle truffe finanziarie più comuni nel 2026

Di Redazione

Un viaggio tra le truffe finanziarie più diffuse nel 2026, raccontate come predatori digitali: dall'inganno su WhatsApp al vishing, dallo smishing al quishing, l'articolo spiega come riconoscerle e difendersi con semplici regole per evitare di cadere nelle loro trappole

Oggi passiamo gran parte della giornata al telefono tra notifiche, chat e chiamate. Rispondiamo a messaggi mentre lavoriamo, controlliamo le mail in fila al supermercato, gestiamo pagamenti direttamente dallo smartphone.
In questa giungla digitale però non circolano solo mail di lavoro o messaggi su WhatsApp.

Tra una notifica e l'altra si appostano dei predatori che sanno come muoversi senza dare nell'occhio, insinuandosi nella nostra quotidianità con fare losco e ingannevole.
Grazie anche all'intelligenza artificiale, hanno affinato tecniche sempre più sofisticate: possono clonare la voce di qualcuno che conosci, un parente o un amico, oppure possono far apparire sullo schermo del tuo smartphone il numero reale della tua filiale, fingendosi operatori bancari. Stiamo parlando, naturalmente, delle **truffe finanziarie**.

Molte delle tecniche descritte rientrano nel cosiddetto *social engineering*, ovvero strategie utilizzate dai truffatori per manipolare le persone e indurle a rivelare informazioni riservate o compiere azioni dannose.

In questo articolo, passeremo in rassegna le truffe finanziarie più comuni. Lo faremo come se fossimo in un documentario naturalistico o, se preferite, in un bestiario medievale. Ad ogni truffa, assoceremo un animale predatore e spiegheremo:

- Qual è il suo habitat;
- Come attacca le sue prede;
- Come riconoscerla;
- Come difendersi.

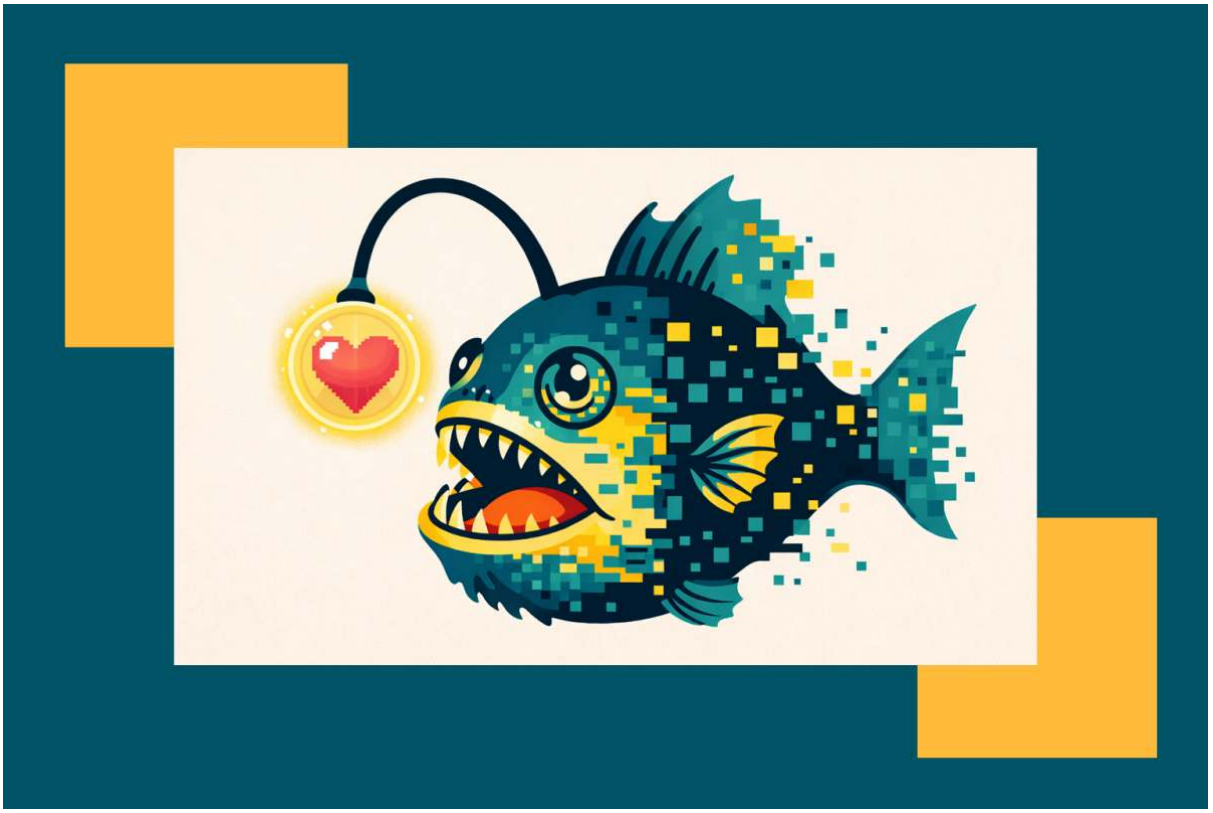
Truffe finanziarie: come attaccano e come difendersi.

1.Il Phishing su WhatsApp

Il **phishing** su WhatsApp è una truffa che attira la propria preda usando messaggi che sembrano credibili

e urgenti. Proprio come il pesce pescatore usa una piccola luce per attirare le sue prede, anche chi mette in atto un attacco phishing utilizza un'esca: un messaggio che arriva da qualcuno che sembra un conoscente e che chiede aiuto o supporto.

La richiesta può apparire plausibile, ma serve solo a convincere la vittima a compiere un'azione facendo leva sull'empatia, come condividere un codice, cliccare su un link o inviare denaro.



• **Habitat**: le chat WhatsApp

• **Modalità di attacco**: Il predatore agisce solitamente spacciandosi per un familiare in difficoltà e, facendo leva sul senso di urgenza, chiede un bonifico immediato. In altri casi si finge un conoscente e ti chiede di girargli un codice SMS che avresti ricevuto "per errore", una volta inviato, il truffatore lo utilizza per sottrarti l'account. Quel codice, infatti, serviva a trasferire il profilo WhatsApp della vittima su un nuovo dispositivo.

A quel punto, il predatore si finge la vittima e scrive ai tuoi contatti chiedendo loro di inviargli denaro. Una variante recente di questo schema, è la cosiddetta "truffa della ballerina": anche in questo caso tutto parte da un messaggio apparentemente inviato da un conoscente, che chiede di cliccare su un link per aiutare una ballerina a vincere un concorso di danza.

Una volta cliccato sul link, l'utente viene reindirizzato su una pagina web che imita una piattaforma ufficiale di votazioni, tuttavia, per "confermare il voto", il sito richiede prima di inserire il proprio numero di telefono e poi un codice ricevuto via SMS.
Anche in questo caso, inserendo il codice, si consegna ai predatori famelici il proprio account WhatsApp che verrà utilizzato per diffondere nuovamente il link fraudolento o per chiedere soldi ad amici e familiari.

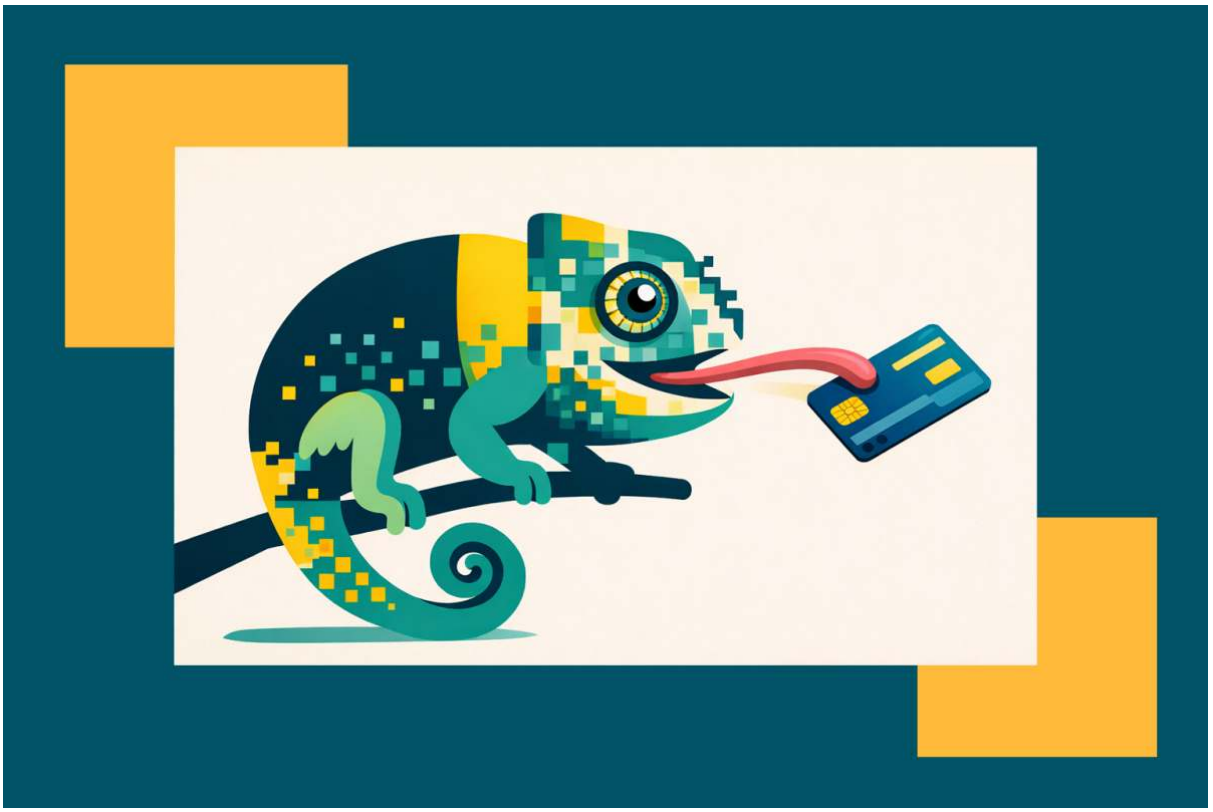
• **Segni di riconoscimento**: senso di urgenza, richieste insolite di denaro o di codici da parte di contatti che di solito non si comportano così, messaggi con link che portano a pagine dove viene richiesto di inserire dati personali o codici.

• **Come difendersi:** non condividere mai codici ricevuti via SMS. Se un parente o un amico ti chiede soldi su WhatsApp da un numero nuovo, fermati un attimo e chiama il suo numero salvato in rubrica: se risponde, hai appena evitato una trappola. Infine, non inserire mai dati personali o codici dopo aver cliccato su link relativi a concorsi e votazioni ricevute via chat.

2. Il Vishing (Voice Phishing)

Il **Vishing** è una truffa telefonica in cui chi chiama si finge una figura autorevole, come un operatore bancario o un agente delle forze dell'ordine, per indurre la vittima ad abbassare la guardia.

La richiesta è quasi sempre urgente: comunicare un codice, fornire i dati della carta, autorizzare un'operazione o spostare del denaro "per metterlo al sicuro".
Proprio come accade in natura, il mimetismo funziona perché la preda non percepisce il pericolo, e quando si rende conto che qualcosa non torna, l'operazione è già stata fatta e il truffatore è sparito con i soldi.



• **Habitat**: le chiamate telefoniche.

• **Modalità di attacco**: agisce usando lo **spoofing**, una tecnica fraudolenta mediante la quale i truffatori effettuano chiamate facendo apparire sullo schermo del tuo smartphone un numero diverso da quello reale, per mimetizzarsi, simulano così una chiamata proveniente dalla tua filiale o dalle forze dell'ordine.

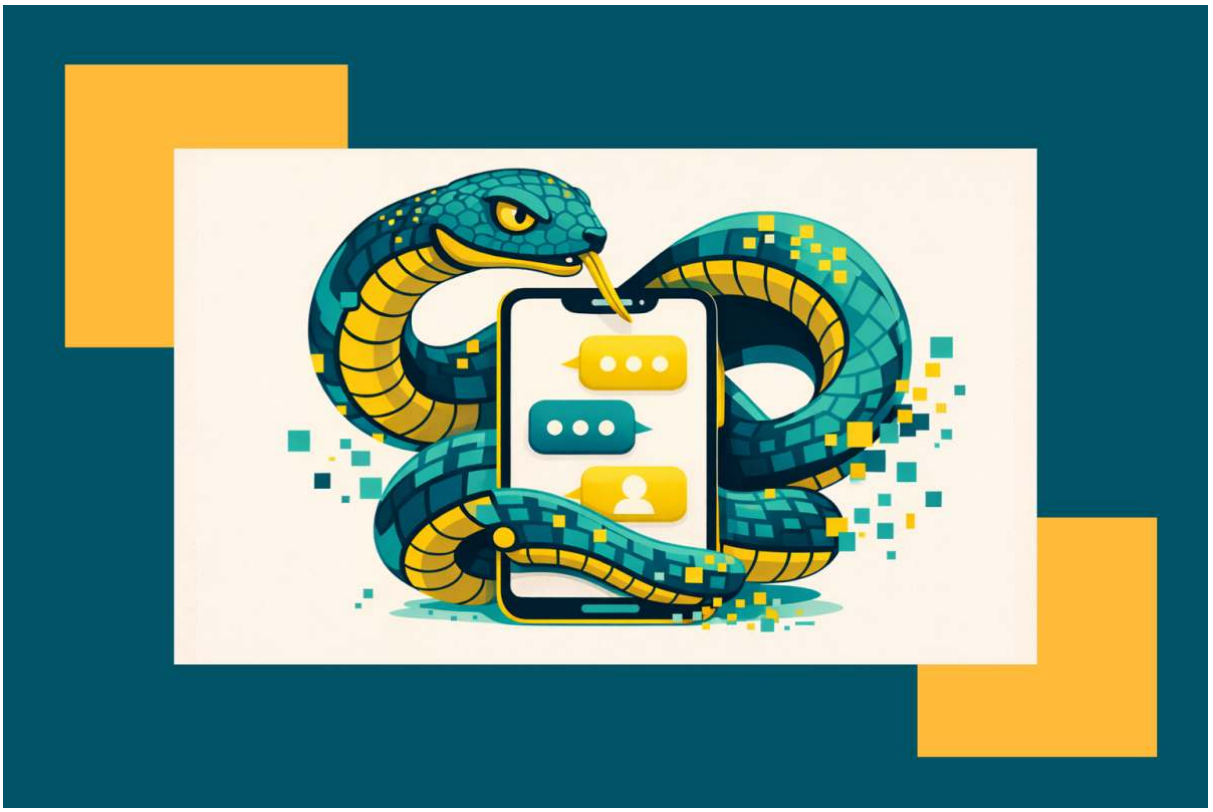
• **Segni di riconoscimento**: spesso ti contatta fingendosi un operatore bancario per un pagamento

sospetto sul conto o delle forze dell'ordine segnalando un pagamento illecito o dei problemi con gli operatori della banca.

• **Come difendersi:** non comunicare mai codici personali, password e credenziali via telefono. Se hai un dubbio, riaggancia e richiama tu il numero ufficiale.

3. Lo Smishing (SMS Phishing)

Dietro lo **Smishing** si nasconde un predatore insidioso e fulmineo.
Se ne sta lì tra le notifiche, mescolato a messaggi apparentemente normali, in attesa del momento giusto: quando la preda è di fretta, distratta o con la testa altrove. È proprio in quel momento che scatta, pronto a spingere la vittima a cliccare su un link fraudolento rubando informazioni personali, dati delle carte e soldi.



• **Habitat**: gli SMS.

• **Modalità di attacco**: invia un messaggio su un pagamento bloccato, un pacco fermo con una consegna da riprogrammare o un accesso sospetto al tuo conto corrente, con un link da cliccare "subito" o un numero da chiamare "al volo" per risolvere il problema.

• **Segni di riconoscimento**: il messaggio gioca quasi sempre sull'urgenza o sulla paura, con frasi tipo: "*Il tuo conto sarà bloccato*", con l'intento di spingerti a cliccare su un link che porta a un sito solo in apparenza autentico, dove ti viene chiesto di inserire dati personali. In alcuni casi, invece, il link fa partire direttamente il download di un malware, un virus che permette ai truffatori di controllare quello che fai sul telefono.

• **Come difendersi**: non cliccare mai sui link ricevuti via SMS, verifica prima il mittente e se il messaggio parla della tua banca, chiudi tutto e cerca un riscontro manualmente dall'app ufficiale.

4. Il Quishing (QR Code Phishing)

Nelle vastità oceaniche di bar, ristoranti e parcheggi, che usano il QR code per far consultare il menù o far pagare un servizio, si muove un predatore tanto silenzioso quanto rapido: il **Quishing**.
Si tratta di una truffa che sostituisce i QR code con versioni fasulle, applicandoli su tavoli, parchimetri o vetrine.

Basta una scansione per essere indirizzati verso pagine malevole che imitano quelle ufficiali per carpire dati riservati o installano malware sul dispositivo.

• **Habitat**: si nasconde sui tavoli di bar e ristoranti, nelle attività commerciali che utilizzano i QR code per comunicazioni o pagamenti. Ma anche in luoghi pubblici ad alto passaggio, sui parchimetri, sulle colonnine di ricarica elettrica e perfino su finte multe lasciate sul parabrezza delle auto.

• **Modalità di attacco**: il truffatore sostituisce il codice QR code originale con un adesivo identico creato apposta per ingannare le vittime. Quando lo si scansiona non si finisce sul sito ufficiale del ristorante, ma su una pagina falsa controllata dal truffatore, pronta a rubare dati e soldi o a installare virus sul telefono, mettendo a rischio anche informazioni di lavoro o dei clienti.

• **Segni di riconoscimento**: prima di scansionare un QR code, verifica che non si tratti di un adesivo applicato sopra un altro codice e osserva se è leggermente storto o realizzato con un materiale diverso rispetto al cartello su cui si trova.

• **Come difendersi**: controlla sempre l'indirizzo del sito che si apre quando scansioni un QR code. Se il link è strano, accorciato o pieno di numeri e sequenze casuali di lettere e numeri, è meglio chiuderlo subito. Diffida anche delle pagine che chiedono dati personali, credenziali o pagamenti. In caso di dubbio, interrompi l'operazione e verifica direttamente con il personale o tramite i canali ufficiali.

Le 5 regole d’oro per non abboccare alle truffe finanziarie

Le truffe finanziarie sono sempre più diffuse e cambiano continuamente forma.
Possono arrivare con una telefonata, con un messaggio su WhatsApp, con un SMS o semplicemente inquadrando un QR code con la fotocamera del tuo smartphone. Il meccanismo però è sempre lo stesso: spingere la vittima ad agire in fretta, senza darle il tempo di verificare cosa stia facendo davvero.

Anche grazie all’intelligenza artificiale le truffe sono diventate sempre più sofisticate: i siti clonati sono praticamente uguali agli originali, i messaggi rispettano la grammatica e la sintassi italiana, inoltre i truffatori sono in grado di imitare la voce di operatori bancari o di persone fidate.
Le minacce sono in continua evoluzione, cercare di catalogarle e conoscerle tutte nei minimi dettagli non è generalmente né possibile né sufficiente.

Per proteggersi non serve quindi una preparazione tecnica avanzata, bensì è importante adottare alcune semplici abitudini.
Ecco perché abbiamo raccolto cinque regole di sopravvivenza per orientarsi in questo territorio di caccia, cinque consigli sempre validi per ridurre al minimo il rischio di finire nella trappola - o tra le fauci - di una truffa finanziaria.

1. **Non agire mai di fretta**. Molti predatori puntano sull’urgenza per far reagire la preda d’istinto, quindi, se ti senti minacciato o sottopressione, fermati e verifica quello che sta succedendo.

2. **Non cliccare link sospetti.** Esche come i link possono sembrare invitanti, ma spesso nascondono una trappola. Se ricevi un messaggio o una mail con un link che ti porta su un sito dove ti viene chiesto di inserire credenziali di accesso o altri dati personali, è meglio non abboccare e chiudere subito la pagina.

3. **Verifica sempre il mittente di SMS e e-mail attraverso i canali ufficiali.** Controlla sempre l’interlocutore, anche se sembra “del branco”, visto che dietro un numero o una voce può nascondersi chiunque. Chiudi la conversazione o non rispondere al messaggio e, invece, contatta il mittente tramite canali già in tuo possesso.

4. **Non condividere mai informazioni riservate.** Evita di lasciare tracce che possano guidare i predatori verso la tua tana e svelargli l’ingresso. Codici di sicurezza, password, PIN o dati completi delle carte vanno custoditi con attenzione e mai condivisi, sono informazioni che le banche non ti chiederanno mai.

5. **Se riconosci i segnali di una trappola o se pensi di esserci già finito dentro, allora contatta immediatamente la tua banca** per bloccare operazioni o strumenti di pagamento.

Il video:

DATA DI PUBBLICAZIONE: 14/05/2026 - AGGIORNATO IL 12/06/2026 ALLE 02:00