



scopriamo le **TRUFFE**

**UNA GUIDA UTILE
PER DIFENDERSI**

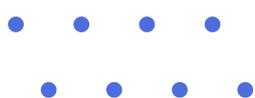


QUALI SONO LE PRINCIPALI

Phishing	03
Smishing	04
Vishing	05
Skimming	06
Quishing	07

e ancora...

Addebito fraudolento	08
E-commerce	09
Il lavoro facile	10
Il finto parente	11
La donazione	12





PHISHING

Il phishing è una delle truffe più comuni. I truffatori inviano messaggi (e-mail o SMS) apparentemente legittimi da banche, istituti finanziari o aziende conosciute, chiedendo alle vittime di fornire informazioni personali come username, password, numeri di carte di credito, e dati bancari. Questi messaggi spesso contengono link a siti web falsi che imitano quelli ufficiali, con l'obiettivo di rubare informazioni sensibili.

come difendersi

Non cliccare mai su link sospetti. Controlla sempre l'indirizzo dell'email o del sito web e verifica con la banca o l'ente tramite canali ufficiali se hai dubbi.



SMISHING

Simile al phishing, ma i messaggi vengono inviati via SMS. Questi messaggi spesso fingono di provenire da una banca o da un'azienda di fiducia e chiedono alle vittime di fare clic su un link per aggiornamenti o verifiche urgenti. Il link porta a siti falsi dove vengono richiesti i dati personali.

come difendersi

Non rispondere a SMS che richiedono informazioni sensibili e non cliccare su link che sembrano sospetti.



VISHING

Il vishing è una truffa telefonica in cui il truffatore si spaccia per un rappresentante di una banca, di un ente pubblico di una compagnia di servizi, e chiede informazioni personali o bancarie. Possono anche chiedere di trasferire soldi o di fare operazioni bancarie per "sbloccare" o "verificare" il proprio conto.

come difendersi

Non fornire mai dati sensibili per telefono, soprattutto se non hai richiesto il contatto. Chiama la tua banca o azienda direttamente usando il numero ufficiale.



SKIMMING

In queste truffe, i truffatori usano dispositivi chiamati skimmer per copiare le informazioni della carta di credito o debito, spesso nei bancomat o nei lettori di carte di negozi. Una volta che hanno i dati, li usano per effettuare acquisti o prelievi non autorizzati.

come difendersi

Controlla sempre i lettori di carte per eventuali dispositivi sospetti. Usa bancomat e lettori di carte in luoghi sicuri e ben illuminati. Monitora frequentemente i movimenti sul conto.

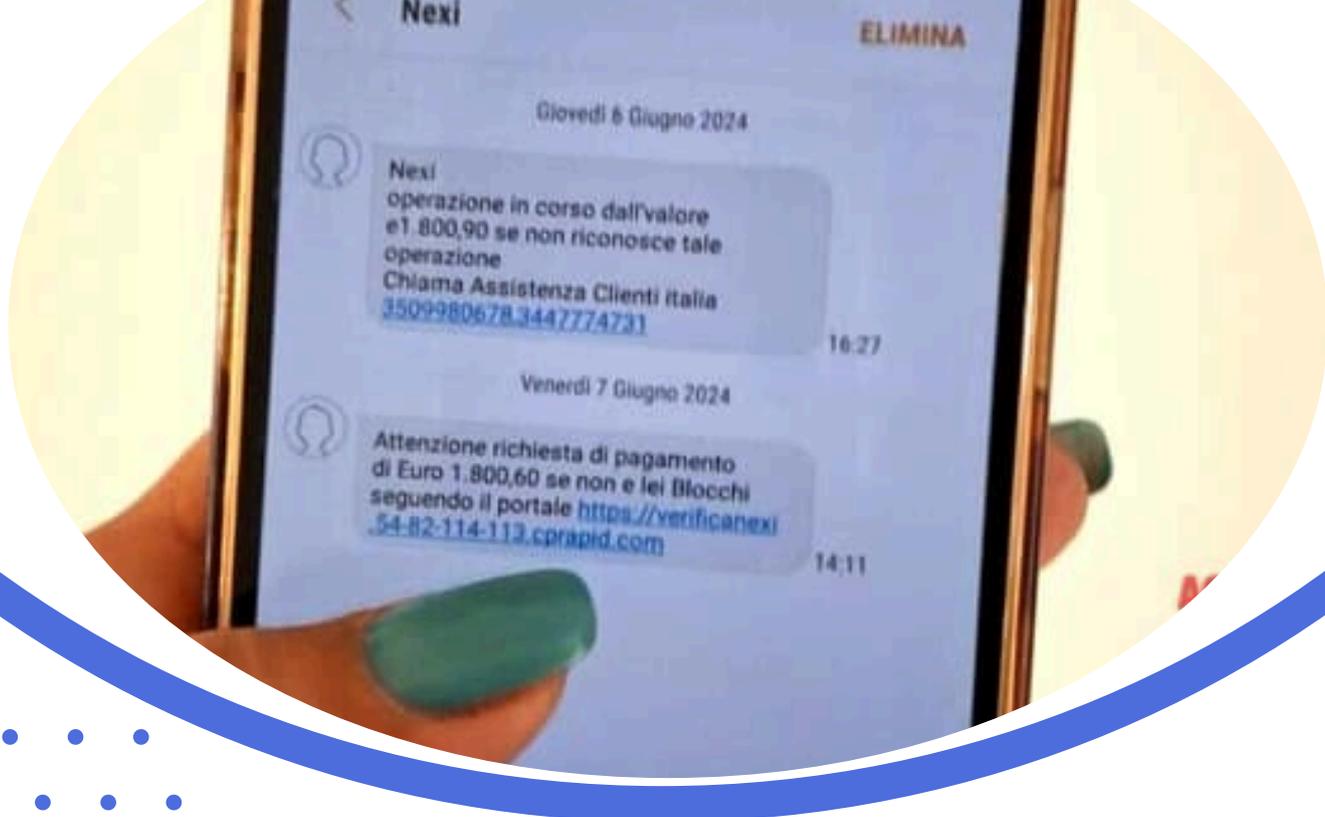


QUISHING

Questa è una truffa che usa codici QR (quei quadratini da inquadrare con la fotocamera) per rubare dati personali o soldi. Il truffatore mette il codice in volantini, email o cartelli, e quando lo si scansiona si viene indirizzati a un sito falso, che sembra vero, dove si chiede di inserire dati bancari o password.

come difendersi

Non inquadrare codici QR trovati per strada o in email sospette. Se ti serve un codice QR, usa solo quelli di siti ufficiali o chiedi aiuto a una persona di fiducia. In caso di dubbio, non cliccare e non inserire dati.



ADDEBITO FRAUDOLENTO

I truffatori inviano notifiche false, come se arrivassero dalla tua banca, avvisandoti di un tentativo di prelievo fraudolento. Per “risolvere” il problema, ti chiedono di fornire i tuoi dati bancari o i numeri della carta. Il messaggio sembra urgente per spaventarti e farti agire in fretta.

come difendersi

Non rispondere a email o messaggi di questo tipo e non cliccare su link sospetti. Verifica direttamente con la tua banca.



E-COMMERCE

I truffatori pubblicano articoli su siti di e-commerce, social media o marketplace (come eBay, Facebook Marketplace) a prezzi incredibilmente bassi. Dopo aver ricevuto il pagamento, non inviano mai i prodotti o inviano merce scadente o falsa.

come difendersi

Controlla sempre la reputazione del venditore, leggi le recensioni e non acquistare mai da venditori sconosciuti senza feedback verificabili. Usa metodi di pagamento sicuri come PayPal, che offre protezione sugli acquisti.



IL LAVORO FACILE

Truffe che promettono guadagni facili e veloci da casa, spesso con l'obbligo di pagare una somma iniziale per accedere a corsi o strumenti per "avviare l'attività". Alla fine, la vittima paga senza ottenere nulla. Spesso usano testimonianze false e siti ben fatti per sembrare seri. Diffida sempre da chi chiede soldi subito e promette risultati troppo belli per essere veri.

come difendersi

Diffida sempre da offerte di lavoro che sembrano troppo belle per essere vere. Le aziende legittime non chiedono mai pagamenti anticipati.



IL FINTO PARENTE

Un truffatore si finge un parente (ad esempio, il figlio, un nipote o un amico) e ti manda un messaggio urgente in cui ti chiede denaro per una situazione di emergenza, come un incidente o un arresto. Spesso ti chiederanno di trasferire il denaro in modo rapido. Giocano sulla paura e sull'affetto per spingerti ad agire senza riflettere. Prima di fare qualsiasi cosa, contatta direttamente la persona o chiedi consiglio a un familiare fidato.

come difendersi

Se ricevi un messaggio del genere, verifica sempre con il parente direttamente tramite una chiamata o un altro canale di comunicazione.



LA DONAZIONE

I truffatori si fingono organizzazioni benefiche o utilizzano storie false (ad esempio, malattia grave di un bambino o disastro naturale) per raccogliere soldi dalle persone. Approfittano della generosità e della sensibilità di chi vuole aiutare. Prima di donare, verifica sempre che l'associazione sia vera e riconosciuta. In caso di dubbio, meglio non inviare denaro e parlarne con qualcuno di fiducia.

come difendersi

Verifica sempre l'affidabilità delle organizzazioni tramite canali ufficiali e non inviare mai denaro senza prima fare delle ricerche.

IN GENERALE

CONSIGLI IN PILLOLE

- **Rimani scettico:** se una proposta sembra troppo bella per essere vera, probabilmente è una truffa.
- **Verifica sempre:** prima di fornire dati personali o fare pagamenti, controlla sui canali ufficiali.
- **Usa metodi di pagamento sicuri:** preferisci PayPal o carte di credito, che offrono maggiore protezione.
- **Segnala le truffe:** se pensi di essere stato truffato, avvisa subito la polizia postale o alle autorità competenti.
- **Non avere fretta:** i truffatori vogliono che tu decida in fretta. Prenditi sempre il tempo di riflettere.
- **Chiedi aiuto:** se hai dubbi, parlane con un familiare, un amico o con la nostra Associazione di consumatori.



Iniziativa finanziata con L.R. n. 4 /2017 - anno 2025 - Delibera
Giunta Regionale n. 917 del 27/05/2024

