PROGETTO ANTIFRODE

ATTIVI DIGITALI

Per non cadere nella rete

Iniziativa promossa da
FONDAZIONE LONGEVITAS
FONDAZIONE LOTTOMATICA
In collaborazione con
MINISTERO DELL'INTERNO
anci

La Truffa: un inganno che fa leva sulla fiducia

Il truffatori non usano la forza, ma la psicologia, Studiano le loro vittime per manipolare le emozioni, creare un falso legame e sfruttare la loro sensibilità.

L'urgenza:

- spingono la vittima a muoversi in fretta per evitare di approfondire la situazione.
- La vincita scade fra pochi minuti!
- Suo nipote ha avuto un incidente!

Autorità:

- Si presentano come qualcuno di cui fidarsi.
- Polizia o carabinieri
- La propri banca

Affetto:

- Sfruttano la volontà di aiutare i propri cari.
- Papà ho perso il telefono, scrivimi su whatsapp...

Il danno di una truffa non è solo economico: Il danno più profondo èpsicologico, lasciando sentimenti di paura, vergogna e persino colpa per essere caduti nell'inganno.

Perché oggi il pericolo è digitale?

Una volta i truffatori bussavano alla porta. Oggi sono potenzialmente accanto a noi, 24 ore su 24, attraverso smartphone e computer. Internet ha dato loro strumenti potenti per raggiungerci ovunque, in ogni momento.

Sono strumenti immediati e globali, possono raggiungerci ovunque e in qualsiasi momento

Sfruttano la distrazione: a volte basta un click sbagliato per cadere nella trappola

Sono sofisticati: usano loghi e linguaggi identici a quelli delle vere istutuzioni (banche, le Poste, gli enti pubblici), rendendo più difficile riconoscere la truffa

Sempre più spesso sono potenziati dall'intelligenza artificiale, permettonod al truffatore di usare la voce o l'immagine di persone note (deepfake)

I veicoli del contagio sono gli strumenti che usiamo di più: **Telefono, messaggi, whatsapp**
E-mail
Social network (Facebook, Instagram...)

Le più diffuse truffe online

- truffa della email ingannevole (“*phishing*”)
- truffa sentimentale (“*love scam*”)
- truffa della compra-vendita online
- truffa dei finti operatori bancari o tecnici
- truffe su Subito.it e piattaforme online
- truffa alla nigeriana

1 – PHISING: L’amo digitale

Truffa online: qualcuno finge di essere una banca, INPS, Poste, Amazon o un familiare per rubare soldi o dati personali.

Arriva tramite: Email, SMS / WhatsApp, Telefonate

Attenzione se: “È urgente!”, Chiedono codici o password, Ti fanno cliccare un link

Cosa NON devi fare: Cliccare, Rispondere, Dare codici

Le banche e i servizi seri **NON chiedono** mai password o dati personali via email o SMS.
Se hai dubbi, chiedi sempre aiuto a un familiare o un esperto!

Cosa sto cliccando?

Come leggere la "targa" del sito prima di entrare:

1. **Su Computer: Passate il mouse sul link SENZA cliccare. Leggete l'indirizzo che appare.**

2. **Sul telefono: tenete il dito sul link per qualche secondo, vi apparirà il link vero.**

Regola: se leggete – ad esempio – "**Poste-italia**" invece di "**Poste.it**"
Non cliccate!

⚠ Truffa della compravendita online

Come funziona

Annunci con **prezzi troppo convenienti**
Chiedono **caparra o pagamento anticipato**
Dopo il pagamento **il venditore sparisce**

Attenzione quando

Ti mettono fretta
Chiedono pagamenti su **Postepay o ricariche**
Evitano telefonate o incontri

Come difendersi

Diffida delle offerte **troppo vantaggiose**
Chiedi **foto dettagliate** dell'oggetto
Conserva messaggi e ricevute
Usa solo **pagamenti tracciabili e sicuri**

Se hai un dubbio, fermati e chiedi aiuto

Truffa dei finti operatori bancari o tecnici

Come funziona

Si fingono: banca, Posta, INPS o assistenza tecnica computer
Ti dicono che c'è un **problema di sicurezza urgente**

Cosa vogliono

I **codici OTP** ricevuti sul telefono
Accedere al tuo **computer da remoto** o a un tuo **account**
Convincerti a fare un **bonifico**

Perché è pericolosa

Usano parole tecniche e tono professionale
Mettono **fretta e paura**
Ti fanno sentire "in errore"

Ricorda sempre

Banca e assistenza tecnica NON chiedono mai codici, accessi al computer, bonifici al telefono

Non comunicare mai dati via email, WhatsApp e chiedi aiuto a una persona di fiducia

Truffe su siti di annunci online

Finti venditori postano annunci di proprietà o veicoli a prezzi incredibilmente bassi.

Chiedono acconto per "bloccare" l'affare, poi scompaiono.

Truffe su **siti di usato** sono comuni e spesso colpiscono acquirenti inesperti con annunci troppo convenienti.


il Giornale

Sempre più numerose le vittime della "truffa alla nigeriana": ecco come funziona


TORINOTODAY

Torino, truffe su Subito.it e altre piattaforme online: chieste condanne fino a cinque anni di carcere e 8.000 euro di multa

Truffe su piattaforme online

Il Caso di Torino

Contesto: Decine di clienti truffati tramite annunci falsi su siti di compravendita dell'usato.

Modalità: I truffatori pubblicavano offerte ingannevoli, incassavano pagamenti e sparivano.

Conseguenze legali: Chieste condanne fino a 5 anni di carcere e 8.000 € di multa.

Impatto: Le vittime hanno perso denaro e fiducia nelle piattaforme digitali.

Attenzione alle compravendite online, verificare sempre identità e modalità di pagamento

Truffe su Annunci Immobiliari/Auto

Finti venditori postano annunci di proprietà o veicoli a prezzi incredibilmente bassi.

Chiedono acconto per "bloccare" l'affare, poi scompaiono.

TORINOTODAY

Torino, truffe su Subito.it e altre piattaforme online: chieste condanne fino a cinque anni di carcere e 8.000 euro di multa

Truffe relative ad auto usate sono comuni e spesso colpiscono acquirenti inesperti con annunci troppo convenienti.

Allarme truffa alla nigeriana - Come funziona e come difendersi

Meccanismo: Il truffatore risponde a un annuncio pubblicato dalla vittima.
Dopo aver instaurato fiducia, propone un pagamento tramite bonifico estero.
Chiede alla vittima di anticipare una "tassa nazionale" per completare la transazione.

il Giornale

Sempre più numerose le vittime della "truffa alla nigeriana": ecco come funziona

21 febbraio 2025 - 10:48

ASCOLTA ORA

C'è preoccupazione per l'impennata di casi di **truffa "alla nigeriana"**, un tipo di raggiro che sfrutta piattaforme di scambio come Subito.it o Vinted. Il metodo dei criminali, infatti, consiste nel rispondere agli annunci degli utenti per trascinarli nella loro trappola. I carabinieri hanno lanciato l'allarme, raccomandando ai cittadini di fare attenzione.

Questo genere di truffa prevede che il malvivente contatti la vittima, mostrandosi interessato a un suo particolare **annuncio**. Si predono due contatti, si crea un dialogo e solo dopo, una volta che si è instaurata una certa fiducia, il criminale passa all'azione. Il truffatore dice alla vittima che pagherà con **bonifico bancario dall'estero**, precisando che per completare la transazione sarà necessario il pagamento di una tassa nazionale che sarebbe una percentuale sul valore del bonifico. Tutta la questione pare convincente, e in molti cadono nel tranello. In questo modo i criminali ottengono denaro in maniera facile e veloce.

Compreso il pericolo, è più che mai necessario imparare a riconoscere la truffa e a sapere come intervenire. Sappiamo che i malviventi cercano le loro vittime sulle **piattaforme di scambio** beni come Subito.it, o Vinted, ma anche sui social network. Ogni spazio in cui troviamo annunci di vendita può diventare territorio di caccia. Ecco perché quando frequentiamo questi siti, che non hanno nulla a che fare con l'opera dei malviventi, è necessario prestare un po' di attenzione.

Obiettivo: Ottenere denaro facile sfruttando la buona fede e la scarsa familiarità con le procedure bancarie internazionali.

Consigli utili

Usare solo le chat integrate delle piattaforme.
Accettare esclusivamente i metodi di pagamento ufficiali.
Non fornire dati personali o bancari.
Segnalare comportamenti sospetti alle autorità o all'assistenza del sito.

⚠ Nuove minacce: L’intelligenza artificiale

Che cos’è:
L’intelligenza artificiale generativa è la nuova famiglia di sistemi che permette di «creare» contenuti: testi, immagini, audio e video, con qualità spesso indistinguibile da contenuti «reali»

Il «Deepfake»
Si tratta di contenuti generati dall’IA che usano l’aspetto e la voce di una persona reale per creare audio e video di queste in situazioni mai avvenute

Come difendersi
Come non ci fidiamo dei messaggi di sconosciuti, ora dovremo avere la prontezza di verificare anche messaggi vocali o video di persone a noi vicine. Cercate una verifica indipendente, fate domande sulla «storia di famiglia»

Difficile distinguere il vero dal falso