

Occhio alle truffe

di **Romina Gobbo**

Sono costantemente in aumento, complici anche i nuovi mezzi di comunicazione, i social network o l'Intelligenza Artificiale che le rendono più semplici da ideare e realizzare. Stiamo parlando delle truffe online, le cui vittime sono prevalentemente adulti tra i 30 e i 65 anni.

Si chiama «romantic scam», è la truffa romantica. Abbiamo imparato a conoscerla recentemente perché è diventata virale la storia di Anne, 53 anni, interior designer francese, avvicinata sui social da un sedicente Brad Pitt. «Diceva le parole giuste, tanto che me ne sono innamorata», ha dichiarato. Ma, chiunque si celasse dietro al profilo del celebre attore, aveva ben altro in mente che le grazie della signora. «Ho bisogno di soldi per le cure di un tumore ai reni. La mia ex moglie, Angelina Jolie, mi ha congelato i conti». Così Anne ha inviato 850mila dollari all'uomo con cui era convinta di avere una relazione.

«Sono Riccardo, sono in viaggio in Cambogia, mi hanno rubato il portafogli. Mi serve del denaro». Facile che un parente o un amico di tal Ric-

cardo, preoccupato per lui, provveda al bonifico, e la cifra si volatilizza. «Sono Fabrizio, operatore della sua banca. Sembra sia in atto un tentativo di accesso abusivo al suo conto. Prema il link qui allegato per bloccarlo». In questo secondo caso, siamo di fronte a una truffa online chiamata *phishing*, cioè il link è malevolo e noi consegniamo così i nostri dati e le nostre credenziali a malintenzionati che, a quel punto, possono davvero avere accesso al nostro conto per fare bonifici o trasferimenti di denaro in maniera fraudolenta. Il termine *phishing* è una variante di *fishing*, che in lingua inglese significa «pescare», «prendere all'amo». E, in effetti, l'attività criminale è simile alla pesca: il truffatore cerca di catturare la preda attraverso una serie di email, sms (*smishing*)

o telefonate. C'è, poi, il *vishing*, o *voice phishing*, dove è la voce che conduce in errore, perché viene riprodotta quella di una persona conosciuta. Oppure c'è il caso di colui che si presenta come un finto impiegato, o un pubblico ufficiale, ed è particolarmente convincente.

Gli anziani, meno usi alla tecnologia, vengono per lo più raggiunti con la telefonata, con la quale vengono loro richieste informazioni personali, finanziarie o di sicurezza. «La qualità delle tecniche criminali si sta perfezionando – spiega il commissario capo Flavio D'Addario, responsabile della Prima Sezione Investigativa della Quarta Divisione (Financial Cybercrime) del Servizio Polizia postale e per la sicurezza cibernetica –. Gli algoritmi sono sempre più sofisticati. E con l'intelligenza artificiale i criminali riescono a riprodurre foto perfette, e a far utilizzare un italiano madrelingua anche a chi in realtà non lo padroneggia. Un esempio è il *deepfake* (in estrema sintesi, un falso che ti ruba la faccia, ndr), attraverso il quale si può riprodurre, a livello video e audio, l'immagine di una persona nota, il cui avatar va a promuovere dei prodotti finanziari, magari un *trading online* (la compravendita di strumenti finanziari tramite internet, ndr), o un investimento in criptovalute. Fanno dei tentativi a pioggia e, prima o poi, qualcuno, che magari ha un'alfabetizzazione digitale più bassa, ci casca. Con Meta, così come con Google, collaboriamo. Ma sono dei colossi e trattano una mole enorme di dati. E sulle inserzioni pubblicitarie, che sono milioni, non sempre è possibile un controllo del contenuto. Quando troviamo delle falle, le sottoponiamo, e loro procedono. Chiaro che la rimozione è quasi sempre un ex post, a seguito di segnalazione».

Casi in aumento

Nel 2024 la Polizia Postale ha investigato su 8.468 frodi informatiche, con 919 persone indagate e 48 milioni di euro di somme sottratte, con un incremento del 20% rispetto al 2023; 18.714 sono state le truffe online, con 3.581 persone indagate, e 181 milioni di euro di somme sottratte, con un incremento del 32% rispetto al 2023 (oltre 137 milioni di euro); 11.887 attacchi ad aziende, con 178 persone indagate.

Per *truffa online* si intende una tipologia di frode virtuale effettuata tramite internet, ma senza un accesso abusivo da parte del truffatore nel

MOORSTUDIO / GETTY IMAGES

ZOOM

Alcuni consigli

Diffidare di chi promette guadagni facili.

Controllare sempre la provenienza delle comunicazioni e l'attendibilità del mittente.

Non fornire mai dati personali (password, codici bancari, numeri di carte di credito).

Non cliccare su link o allegati inviati da mittenti sconosciuti o sospetti.

Fare attenzione a eventuali errori di sintassi o refusi, che potrebbero essere un campanello d'allarme.

Utilizzare metodi di pagamento sicuri (carte di credito, Paypal, ecc.).

Quando si compra online, utilizzare le piattaforme che hanno un sistema di protezione, evitando la trattativa privata.

Contattare la propria banca o il proprio gestore telefonico qualora si ricevesse una chiamata o un messaggio sospetto.

Tenere traccia di tutte le chat e dei pagamenti, che saranno utili nel caso di denuncia.

sistema informatico della vittima. Nella *frode informatica*, invece, il truffatore entra nel sistema informatico della vittima, sottraendo il Pin della carta di credito, inviando un virus e, nel peggiore dei casi, accedendo direttamente al suo conto bancario o alla sua posta elettronica. «Le frodi informatiche sono un reato ai sensi dell'articolo 640 ter del codice penale – afferma il commissario –. Se poi non si tratta di un singolo, ma di una moltitudine di persone, parliamo di associazione a delinquere, che può essere anche di stampo mafioso».

L'epoca dei social network rende tutti più vulnerabili, perché è diventato molto semplice reperire informazioni circa gli interessi, i luoghi che si frequentano, le amicizie, le abitudini e le preferenze di acquisto. «Nel periodo covid è cresciuto l'utilizzo dei mezzi informatici, e i criminali si sono buttati su questa frontiera. Anche per-

ché è un crimine "comodo", si commette restando seduti alla propria scrivania», continua il dottor D'Addario, che sottolinea l'importanza della cooperazione internazionale per poter recuperare le somme sottratte.

«Nelle nostre indagini sulle truffe online – riprende –, talvolta emerge il coinvolgimento di organizzazioni fraudolente ben strutturate, transnazionali, con base in determinati Stati. Con uno Stato europeo o con uno con il quale il nostro Paese ha rapporti stretti, è facile dialogare. Anche se le leggi non combaciano del tutto, si riesce sempre a trovare un punto in comune. Il problema sorge quando abbiamo a che fare con paradisi fiscali esotici o con alcuni Paesi extra UE, dove la legislazione è più permissiva. Fondamentale è la collaborazione con lo Stato italiano, con le banche, con i *provider*, con le *exchange di cripto valute* (piattaforme che facilitano l'acquisto

e la vendita di asset digitali in base ai prezzi di mercato giornalieri, ndr), con i grandi social network, con Poste Italiane, con le Authority e le associazioni dei consumatori».

Denunciare subito

La buona notizia è che il recupero delle somme sottratte è in crescita, ma serve tempestività nella denuncia, altrimenti il denaro scompare, anche immesso nel sistema del riciclaggio. «Capita, invece – riprende D'Addario –, che ci troviamo a lavorare su transazioni economiche fraudolente vecchie di mesi, se non di anni, perché la persona o non si è accorta, oppure si vergogna di essere caduta nella trappola. D'altra parte, il presunto broker di solito è galante, gentile, di bell'aspetto, e si conquista la fiducia dell'utente, chiedendo all'inizio somme basse per l'investimento, e magari per un po' rimborsa anche. L'utente, una volta fidelizzato, investe sempre di più, 100-200mila euro. Il risveglio avviene quando chiede di rientrare in possesso della cifra o di parte di essa. Dall'altra parte cominciano a prendere tempo, poi si rendono irreperibili. A quel punto la persona capisce di essere stata truffata».

I truffatori giocano sull'auto-revolezza, la fiducia, l'ignoranza, l'avidità e il senso di colpa. La fascia di età più interessata dalle truffe online è quella tra i 30 e i 65 anni, cioè la fascia adulta, che usa molto il telefonino per lavoro e per i pagamenti. Il target più giovane è più orientato all'e-commerce. Dalle varie piattaforme acquistano di tutto, dal telefono alle scarpe. «Anche se

sono nativi digitali, non sempre sono in grado di difendersi. Per questo, andiamo spesso nelle scuole. L'altro grande abbaglio per i giovani è quello degli *influencer* che promettono scorciatoie per ottenere soldi facili. Spesso dietro la facciata di legittimità si celano intenzioni truffaldine», conclude D'Addario.

A lavorare molto sul fenomeno delle truffe online è anche Confconsumatori. «Nel 2024, abbiamo ricevuto almeno 500 segnalazioni, di cui ci stiamo occupando – spiega il presidente Marco Festelli –. Le tecniche dei malviventi si affinano, e la moneta elettronica si presta maggiormente».

È andato in onda di recente a *Chi l'ha visto?* il caso del sui-

icidio di Alessandro Argentini. Alla trasmissione si era rivolta la sorella Antonella che, dall'analisi dello smartphone del fratello, aveva scoperto un fitto scambio di messaggi con broker che l'avrebbero convinto a investire progressivamente tutto il suo patrimonio.

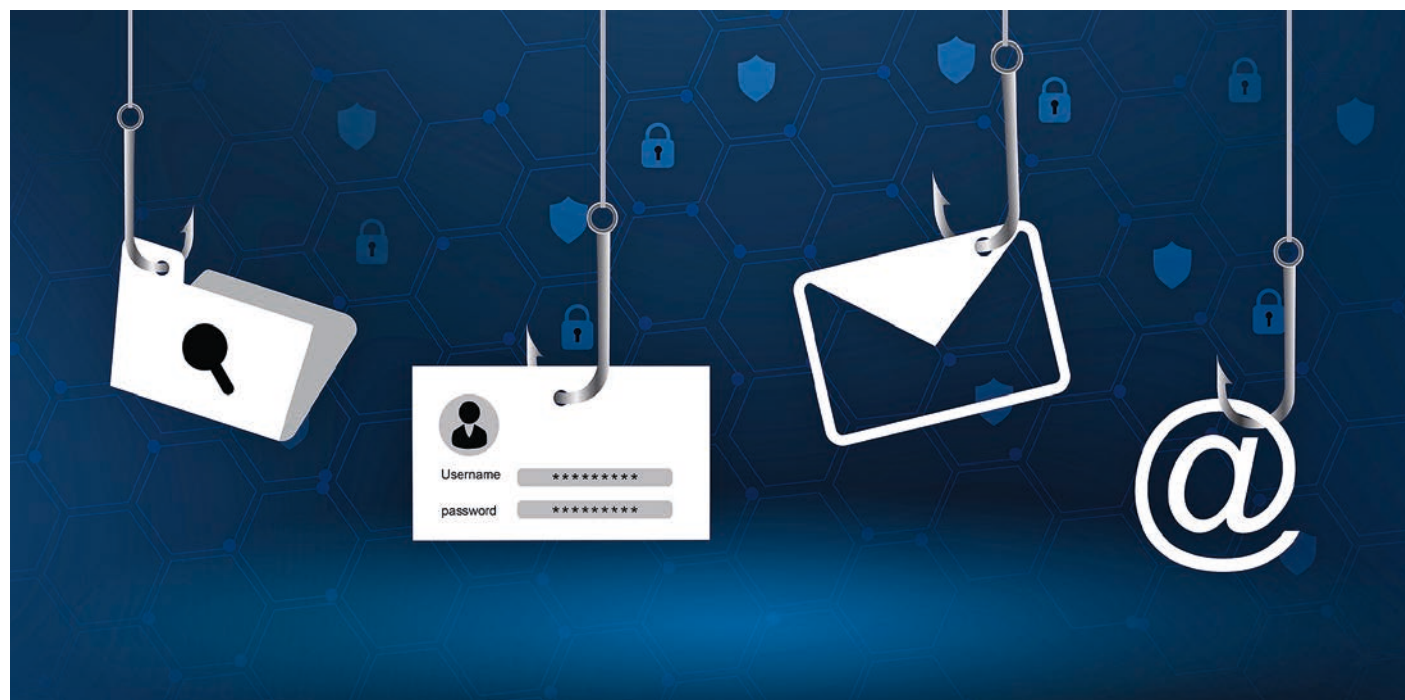
Confconsumatori assiste chi vi si rivolge tramite gli sportelli diffusi in sedici regioni, anche facendo pressione sugli istituti bancari che qualche volta cercano di evitare il rimborso ma, «nel 70% dei casi, riusciamo a recuperare i soldi», dice Festelli. L'associazione promuove, inoltre, anche tutta una serie di iniziative di formazione, rivolte sia ai propri dipendenti che all'utenza.

Per la sicurezza dei cittadini

Operatori della Polizia postale al lavoro. Nel 2024 questo ramo della Polizia ha investigato su 8.468 frodi informatiche, con 919 persone indagate e 48 milioni di euro di somme sottratte, con un incremento del 20% rispetto al 2023.



POLIZIA POSTALE



SARAYUT THANEERAT / GETTY IMAGES