La «truffa romantica», la clonazione della voce e le altre frodi telefoniche e online più diffuse: come difendersi

Dal wangiri, la truffa made in Giappone dello squillo senza risposta, passando per phishing e smishing fino al falso messaggio di un figlio ai genitori e al codice a sei cifre (da non condividere mai con terzi) (Fonte: https://www.corriere.it/ 13 marzo 2025)

Un danno da 10 miliardi di dollari

L'universo delle truffe online è **sempre più vasto e multiforme: wangiri, falsi messaggi, finti prelievi, lavori dal guadagno troppo facile**. **Nulla**, è però **come sembra**. Specie se ci sono di mezzo i soldi. E **nessuno**, mai o quasi mai, **ci viene casualmente a pescare tra miliardi di utenti** per farci **un favore**. Per inquadrare il fenomeno basta guardare i numeri. Secondo un dato diffuso dall'Fbi, il Federal Bureau of Investigation statunitense, nel 2023 le truffe online hanno causato **una perdita di oltre 10 miliardi di dollari**. In particolare, negli Stati Uniti sarebbero soprattutto le**persone di età superiore ai 60 anni**a cadere vittime delle truffe online, nonostante i cybercriminali prendano di mira utenti di tutte le età (e non soltanto negli Stati uniti). Ma non è solo l'e-commerce terra di conquista dei truffatori. Ci sono le e-mail di phishing e gli Sms, le finte notifiche giudiziarie e i falsi alert delle banche. Ogni fronte della nostra vita a contatto con la Rete ha la sua truffa. La parte spiacevole è che **siamo noi, il più delle volte, a fornire i dati segreti** con i quali ci «ripuliscono» i conti correnti e i crediti telefonici senza rendercene conto. Non dimentichiamocelo mai: alcuni dei dati dei nostri depositi di denaro sono **sconosciuti anche alla nostra banca**. Li sappiamo solo noi, e così deve restare. Di seguito potete trovare una guida con l'elenco delle truffe più comuni e su come fare per non farsi trovare impreparati.

Il money muling

La truffa del mulo del denaro è molto elaborata. Persino l'Fbi mette in guardia da questo inganno sul proprio sito. L'ingaggio delle vittime (Salve, posso parlarle un attimo?) avviene sulle principali app di messaggistica. Da WhatsApp a Instagram oppure via Sms. I truffatori, attraverso dei semplici compiti, inizialmente fanno pervenire dei pagamenti alle vittime contattate. Ingolositi dai (modici) pagamenti, vengono richiesti compiti più complessi, come versamenti più cospicui, con promesse di ritorno maggiore. Ma la verità è che non sono più risposti i pagamenti e dopo diversi bonifici, che si possono calcolare anche in svariate migliaia di euro, i truffatori spariscono. Ma non senza danni oltre la beffa: partecipare a queste attività rende inconsapevolmente complici del raggiro, con la possibilità concreta di vedere il proprio conto corrente sospeso e con la difficoltà di poter accedere a mutui o agevolazioni. Diversi nostri lettori sono stati colpiti da questo raggiro: alcuni sono arrivati a perdere anche fino a 125mila euro.

La clonazione vocale e i «rapimenti virtuali»

Per giorni non si è parlato d'altro. Il ministro Crosetto è stato vittima di clonazione della propria voce; insieme ad una storia montata ad arte, i malfattori dietro ad una elaborata truffa hanno poi contattato facoltosi imprenditori i quali sono stati informati di una fantomatica liberazione di giornalisti italiani arrestati all'estero, dietro il pagamento di una ragguardevole somma di denaro. **Difendersi da questa truffa può essere facile**, anche se gli strumenti utili a metterla in atto sono ampiamente diffusi **e anche economici**, grazie alla diffusione di strumenti di intelligenza artificiale. In passato, tecniche simili hanno dato inizio a quelli che vengono definiti «rapimenti virtuali» ovvero falsi rapimenti avvalorati dalla clonazione della voce di una persona cara alla potenziale vittima della truffa che, allarmata, procede a consegnare ai malviventi quanto richiesto.

Per proteggersi, prima di farsi prendere dal panico, in entrambi i casi, è bene contattare la persona «rapita» o che chiede del denaro **con un senso di urgenza**. Se sarà possibile mettersi in contatto con questa persona o con chi le è vicino e smentirà situazioni di pericolo, si potranno contattare le forze dell'ordine per segnalare la tentata truffa. Un altro modo è la possibilità di **istituire un codice segreto** che stabilisca che tutti sono al sicuro.

Il Pig butchering o«macellazione dei maiali»

Il pig butchering, o «macellazione del maiale», è una delle truffe informatiche più diffuse e devastanti che partono dal Sud-est asiatico. Il termine fa riferimento alla strategia adottata dai criminali: come un allevatore ingrassa un maiale prima di macellarlo, così i truffatori costruiscono con pazienza un rapporto di fiducia con la vittima, per poi svuotare i suoi conti nel momento più opportuno.

Questa truffa si sviluppa principalmente attraverso social network, app di messaggistica e piattaforme di incontri, dove i criminali si fingono investitori, esperti di finanza o, più spesso, potenziali partner romantici. La fase iniziale è caratterizzata da un lungo periodo di manipolazione psicologica, in cui il truffatore si mostra premuroso, disponibile e competente, costruendo una relazione solida con la vittima.

Una volta ottenuta la fiducia necessaria, l’inganno entra nella fase più pericolosa. I truffatori iniziano a consigliare “opportunità di investimento”, presentando piattaforme che sembrano professionali, spesso con app e siti web fasulli che simulano borse di criptovalute, trading forex o altri strumenti finanziari. All'inizio, gli investimenti sembrano funzionare: il sistema mostra profitti, la vittima viene invogliata a versare somme sempre più alte, convinta di aver trovato un’occasione irripetibile.

Quando il truffatore ritiene che la vittima abbia versato abbastanza denaro, arriva il momento della “macellazione”. I fondi scompaiono improvvisamente, l’accesso alla piattaforma viene negato, il finto consulente finanziario o partner romantico sparisce nel nulla. Se la vittima cerca di

ritirare il denaro, spesso le viene richiesto il pagamento di commissioni o tasse inesistenti, un ulteriore stratagemma per estorcere più denaro prima di chiudere il contatto definitivamente.

Man-in-the-middle

Di recente, un avvocato è stato vittima di una truffa che è stata resa possibile grazie ad una tecnica chiamata «man-in-the-middle». La tecnica è duttile, ma in questo caso **consente di intercettare la posta elettronica tra due realtà**. In questo caso un avvocato e un'impresa edile, ingaggiata per la ristrutturazione di un edificio. I malfattori sono riusciti ad intrufolarsi nelle caselle di posta elettronica dei due interlocutori **per modificare a proprio piacimento le fatture in Pdf da saldare**.

Proteggersi da questi attacchi è in realtà semplice. **Bastano una password solida e l'utilizzo dell'autenticazione a due fattori**, un procedimento che consente di accedere ad un determinato servizio solo dopo aver immesso una password e un codice a sei cifre che può essere recuperato via Sms, via e-mail oppure attraverso un'applicazione come **Authenticator**.

La truffa della pubblicità ingannevole

Sui social media e in particolare, di recente, anche su Facebook, sono sorte centinaia di pubblicità ingannevoli. I link, se cliccati, portano a siti malevoli che possono avere più scopi. Come la sottrazione dei dati personali, di denaro, o la diffusione di malware. Accorgersi degli annunci truffaldini tuttavia è semplice. Ormai il *modus operandi* è lo stesso da tempo: viene presa l'immagine di un volto noto della televisione e utilizzato un titolo sensazionale circa metodi di investimento, o riguardo la salute dello stesso. I messaggi sgrammaticati, le immagini di scarsa qualità e i siti clonati facilmente individuabili, **sono tutti segnali d'allarme che non vanno ignorati**.

La truffa romantica

Un'altra truffa tanto dannosa quanto odiosa è la truffa romantica, o romance scam. Il malfattore finge, anche con l'utilizzo di AI e tecniche di deepfake, di essere un attore, cantante o un personaggio noto e in grado di suscitare fiducia nella vittima. Una volta instaurata una relazione romantica, il malvivente convince la malcapitata o il malcapitato ad attingere dal proprio conto in banca per versare denaro sul conto del truffatore. I motivi possono essere di varia natura. Un prestito, un intervento urgente, non c'è limite alla fantasia. Di recente una donna è stata manipolata da un falso Brad Pitt, che l'ha convinta a lasciare il marito e darle i soldi recuperati dal divorzio. Anche il vero Brad Pitt si è poi espresso sulla vicenda: «Mai rispondere ai messaggi indesiderati»

Il wangiri «classico» e il wangiri 2.0

Di wangiri vi abbiamo parlato in due occasioni. Dal giapponese «squillo e giù» - si ritiene infatti che sia nata in Giappone - è nota in Italia come la truffa della chiamata senza risposta. Con questo stratagemma, i cybercriminali sfruttano l'ingenuità delle persone per **addebitare chiamate a servizi telefonici costosi o attivare abbonamenti a servizi premium con canoni elevati**.

Il wangiri «classico» consiste in **una chiamata senza risposta da un numero estero**. Se la vittima richiama, viene automaticamente indirizzata verso **un numero a pagamento in grado di addebitare uno o due euro in pochi secondi**. Ora si parla già di wangiri 2.0, ossia un'evoluzione per cui i truffatori hanno trovato lo **stratagemma giusto per tenere la chiamata aperta il più a lungo possibile** per fare lievitare la somma di denaro. Quando la vittima richiama, viene **riprodotto il suono di un numero che squilla** facendo sì che creda di essere in attesa quando invece è già connesso alla chiamata e gli stanno rubando credito.

Il codice a 6 cifre su WhatsApp

Molto simile al messaggio fittizio che invita i genitori a scrivere a un nuovo numero di un figlio, **la truffa del codice a 6 cifre** prevede che si riceva un testo di questo tenore: **«Ti ho inviato un codice per sbaglio, potresti rimandarmelo?»**, seguito per l'appunto da un codice a 6 cifre. E qui deve scattare nel destinatario la massima allerta. Infatti **il mittente del messaggio è apparentemente uno dei contatti che si hanno in rubrica**, trucco semplice per non destare sospetti. Sembra scontato, ma specifichiamo che **per inviare questo messaggio il cyber criminale deve essere in possesso del numero di telefono preso di mira** (può averlo trovato su internet

oppure potrebbe essere il risultato di un furto di dati). In questo modo, **prova ad autenticarsi su WhatsApp con il numero della vittima designata che a questo punto riceve il codice a 6 cifre** di cui si parla. La notifica di WhatsApp è piuttosto chiara: **prima del codice avvisa di «non condividerlo con nessuno»**. Se invece viene condiviso con il truffatore **gli si consente di prendere possesso del proprio account WhatsApp** (o di Instagram, Facebook e così via), dal quale si viene estromessi seduta stante, con l'eventuale **accesso a chat, foto e video** che sono stati ricevuti e condivisi con i propri contatti. Come difendersi? **Farsi sempre delle domande e magari provare a chiamare la persona che in teoria ci sta facendo una richiesta così insolita** (per scoprire facilmente che non ci ha mai inviato il messaggio dal quale parte la truffa). Detto ciò, se non si è mai fatta richiesta del codice è meglio ignorare la notifica, ma soprattutto non condividere mai dettagli dei propri account personali, **le scatole nere della nostra vita che fanno gola ai cyber criminali.**

Il phishing e lo smishing

Da diverso tempo le truffe via **Sms** imperversano sui numeri di telefono degli utenti di tutta Italia. Questo tipo di attacco ha un nome preciso: si chiama *smishing*, e prende il nome dalla tecnica del *phishing*. La modalità è sempre la stessa: **i malfattori inviano un messaggio di testo che replica in modo più o meno credibile le richieste di un'organizzazione.** Può essere ad esempio un corriere, un istituto bancario oppure un ecommerce. Lo scopo può essere duplice: **estorcere denaro o credenziali sensibili**, ma il fine ultimo è il medesimo, ovvero **attingere al patrimonio della vittima. Ma come non cadere in trappola, se non si ha dimestichezza con la tecnologia o non si riconosce un tentativo di truffa?** Semplicemente, **nessun ente o servizio chiederà dati sensibili per Sms, telefonate o email**, anche quando il mittente sembra autentico o attendibile. Inoltre, **se nel testo vi sono errori ortografici e il messaggio comunica un senso di urgenza, è sempre è una truffa**. Dunque, i consigli sono di non rispondere ed eliminare il messaggio, ovviamente **senza cliccare sul link contenuto nel messaggio**. Ma in aiuto accorrono anche le applicazioni e le soluzioni implementate dal sistema operativo, iOS e Android (ve ne parliamo **qui**).

Il finto prelievo su Paypal

Un altro grimaldello per invitarci a cliccare su un **link "svuota conto"** è quello dell'**Sms** che ci avvisa di un falso accesso abusivo dal nostro conto corrente. La formula del messaggio è sempre più o meno la stessa: messaggio che **allarma e invita al clic** e poi il **link** che porta direttamente nel **girone dei truffati**. Ciò che rende più insidiosi questi messaggi è che il **mittente** (una banca, PayPal, ecc.) **esce effettivamente con il nome corretto**, grazie ad una tecnica malevola chiamata «spoofing». Quando si riceve qualcosa del genere bisogna ricordare che **mai una banca chiede di compiere un'operazione** senza contatto a voce (al massimo chiede di essere richiamata) e (è il caso del nostro messaggio) se **pixela i numeri di una carta di credito** o di un conto **lascia sempre visibili alcuni numeri** che permettano di riconoscere la nostra carta o il nostro conto. Naturalmente **in caso di truffa** non accade perché **questi dati non sono noti**.

Le false multe

La tecnica viene da lontano ma si sta diffondendo anche in Italia, e in particolare a Milano. Raccontammo un po' di tempo fa (qui l'articolo) che a San Francisico in California **giravano falsi avvisi di contravvenzione** i quali rimandavano a un sito civetta, esattamente identico a quello della municipalità della città Californiana, in cui si effettuava il pagamento direttamente nelle mani dei truffatori online. Una cosa simile sta avvenendo anche a Milano, dove dei falsi avvisi di truffa contengono un Qr code che, inquadrato, rimanda a un sito «svuotaconto». Un esempio di falso avviso di contravvenzione lo avevamo intercettato anche a Verona.

«Papà, si è bagnato il telefono»

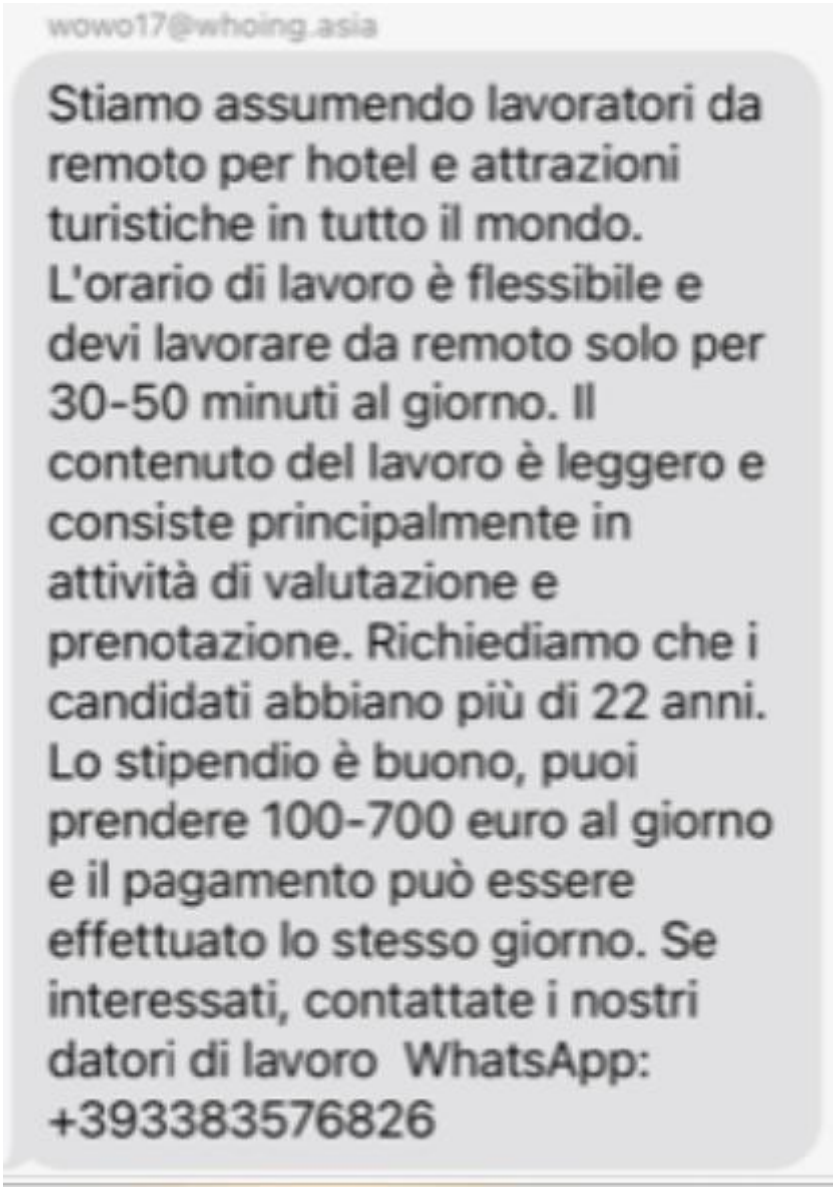
Un altro recente grande classico della truffa online è quello del **messaggio del figlio al genitore**. Da un numero sconosciuto a papà e mamma arriva un messaggio in cui il «sedicente» figlio dice di aver **rotto, perso, bagnato il telefono** e fornisce un nuovo numero cui contattarlo. Naturalmente, chattando con questo numero che ritiene quello del figlio, il genitore riceve la **richiesta di dati personali, bancari e simili**. Con i quali vieni, ovviamente, vuotato il conto corrente

Le carte bloccate

Una tipologia piuttosto frequente di truffa è quella che utilizza **gli sms per soffiarci dati sensibili** relativi al nostro conto corrente. Ovviamente le varie banche citate nei messaggi, così come Nexi, l'azienda che emette la stragrande maggioranza delle carte di credito in Italia, non ne sanno nulla. Ma il messaggio che ci viene recapitato è allarmante. ci dice o che **la carta è stata bloccata o che c'è stato un accesso fraudolento** e che bisogna **seguire il link** inserito nel messaggio **per arginare il problema**. Lo seguiamo, compiliamo i dati che ci sono richiesti, e il conto è violato.

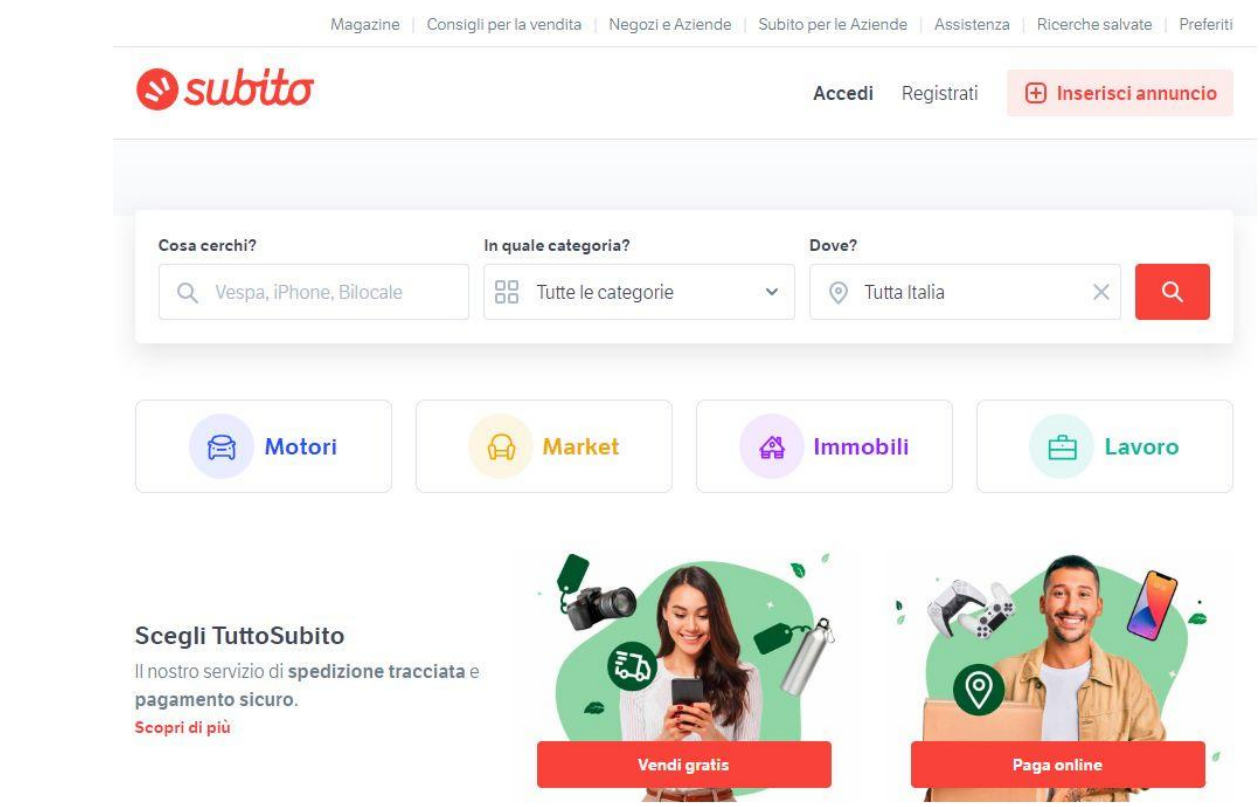
Come evitarlo: Una premessa che taglia la testa al toro. **Nessuna banca o istituzione simile ci contatta via messaggio allegando un link** da seguire. Seconda cosa: **la url**. Se guardiamo i link presenti nei messaggi il nome dell'istituzione finanziaria è citato ma non è mai il dominio del link, vale a dire il suffisso che identifica il mittente (xxx.nexi.it è un indirizzo del dominio nexi, nexi.xxx.it non lo è). Come evitare di cascarci? **Non cliccare niente e buttare tutto. Anche dalla memoria del telefono**.

Il lavoro facile e ben pagato



Tra le truffe che ultimamente, e comunque dopo il lockdown, hanno iniziato a circolare e hanno attirato l'attenzione degli investigatori c'è quella delle finte **offerte di lavoro allettanti**. Tecnicamente si chiama «Online Recruitment Scam» e funziona così. Arriva un messaggio, o una mail, in cui il fantomatico rappresentante di una **grossa organizzazione, di cui comunque è facile reperire informazioni online,** offre un lavoro. In alternativa viene proposto un **impiego molto leggero a stipendio molto alto**. È facile che chi lo riceva, specie se **affamato di lavoro ci casca**. Ovviamente il messaggio è dotato di un messaggio telefonico con cui, chattando, si viene spinti a **fornire informazioni personali e bancarie**, o il pagamento di somme di denaro adducendo diverse motivazioni. Se ci si casca, e si risponde, è già **troppo tardi per accorgersi della truffa.**

L'affare online



Attenti agli affari online: parliamo ad esempio di **Subito**, il portale per la compravendita dell'usato più usato e più famoso. Da quando ha attivato il servizio Tuttosubito, che gestisce in modo praticamente completo vendite e acquisti a distanza, ha messo in piedi molti sistemi anti-frode. Ma la fantasia degli imbroglioni (e l'ingenuità di molti) non è del tutto arginabile.
Quando vendiamo qualcosa online, la cosa migliore che ci possiamo aspettare è di **trovare qualcuno che sia disposto ad acquistare esattamente alla cifra che chiediamo**. Già questo ci **dovrebbe insospettire** (possibile che il potenziale acquirente non provi nemmeno a trattare?) ma ingolositi **dall'affare andiamo avanti**. Ci viene chiesto il **numero di telefono** per essere contattati, noi **ignoriamo l'allarme di Subito** che ci sconsiglia di fornire dati personali a sconosciuti, e diamo il numero. A questo punto l'acquirente **ci contatta e ci dice di recarci a uno sportello Postamat** dove, inserendo la **carta di credito e un codice** che ci fornirà l'acquirente richiamandolo di fronte allo sportello, ci verrà **accreditata la cifra**. In realtà il codice non è altro che un **codice di prelievo** e la cifra dalla nostra carta viene **tolta, invece che aggiunta**.
Del **truffatore**, a quel punto, più **nessuna traccia**, telefono spento e ricerche vane.
Come evitarlo: La risposta è semplice: se ricevete un'offerta di questo tipo **riattaccate**. Se siete caduti nella **trappola del truffatore**, è quasi superfluo dirlo, va precisato che **né Subito né le Poste hanno niente a che fare con questo meccanismo**. Anzi: **Subito** consiglia nelle sue policy di sicurezza di **non fornire dati personali ad estranei**, di mantenere la **discussione all'interno della «stanza»** creata al momento del contatto, di effettuare la compravendita con **mezzi di pagamento sicuri** (da quello interno a Paypal, dal bonifico al pagamento in contanti al momento

della consegna), di **consegnare il bene direttamente o di spedirlo** usando il sistema subito che garantisce la consegna solo ad avvenuto pagamento. Le Poste, invece, sono semplicemente un tramite usato senza nessun tipo di frode, specie visto che siamo noi, materialmente a digitare il codice che porta al prelievo dalla nostra carta. L'unica cosa che si può fare, in **sede di denuncia all'autorità**, è fornire il numero di cellulare chiamante, l'ora del prelievo, la cifra, e lo sportello Postamat interessato sperando che si possa così risalire al conto di accredito (sempre che sia intestato a qualche soggetto di interesse investigativo e non, come più probabile, a un prestanome).

«Due euro per pacchi Amazon non ritirati»

Sembra un'**offerta** super vantaggiosa, una sorta di **«fuori tutto»** da outlet, in realtà è una **truffa**. Di quelle che hanno tutti i requisiti per andare a buon fine: viene speso il nome di un'azienda arci nota (**Amazon**), si propone di fare una **cosa «innocua»** come dare il proprio numero di conto corrente, si chiede una **cifra irrisoria**, di quelle che «anche se non ci guadagno **non ci perdo un granché**». Invece la punizione per una leggerezza può essere di ben altra entità: **conto corrente svuotato**. La truffa è **nota come «brushing»**, che in inglese richiama appunto la spazzolatura. Di cosa? Del **conto corrente**. **Amazon ne è consapevole**, tanto che nelle sue pagine di assistenza al cliente dedica a questo tipo di truffe una pagina di «allarme». L'attenzione della vittima viene catturata attraverso **post sponsorizzati sui social**. Il «mittente» è apparentemente di Amazon, ma con **l'azienda americana non hanno nulla a che fare**. I post, spesso scritti in un italiano stentato (un punto essenziale che ci deve mettere in allerta), mostrano fantomatici **bancali di pacchi mai**

consegnati che si potrebbero riscattare **con una cifra irrisoria**. L'utente-vittima, «non deve fare altro» che seguire il link a un **sito clone di Amazon** per chiedergli di pagare l'intero bancale 2-3 euro inserendo i dati bancari. Così la vittima cade nella rete e il suo **conto viene «brushato»**, spazzolato, svuotato

Le associazioni dei consumatori

Come fare per evitarlo «Quando la nostra attenzione viene colta da offerte super vantaggiose – avverte l'associazione Consumatori attivi – è bene diffidare ed evitare di cliccare sui link del messaggio. Meglio reperire informazioni sull'offerta con una semplice indagine su un motore di ricerca nel web. Se si tratta di una truffa, nel 90% dei casi si troveranno informazioni in merito che porteranno a desistere dall'abboccare».

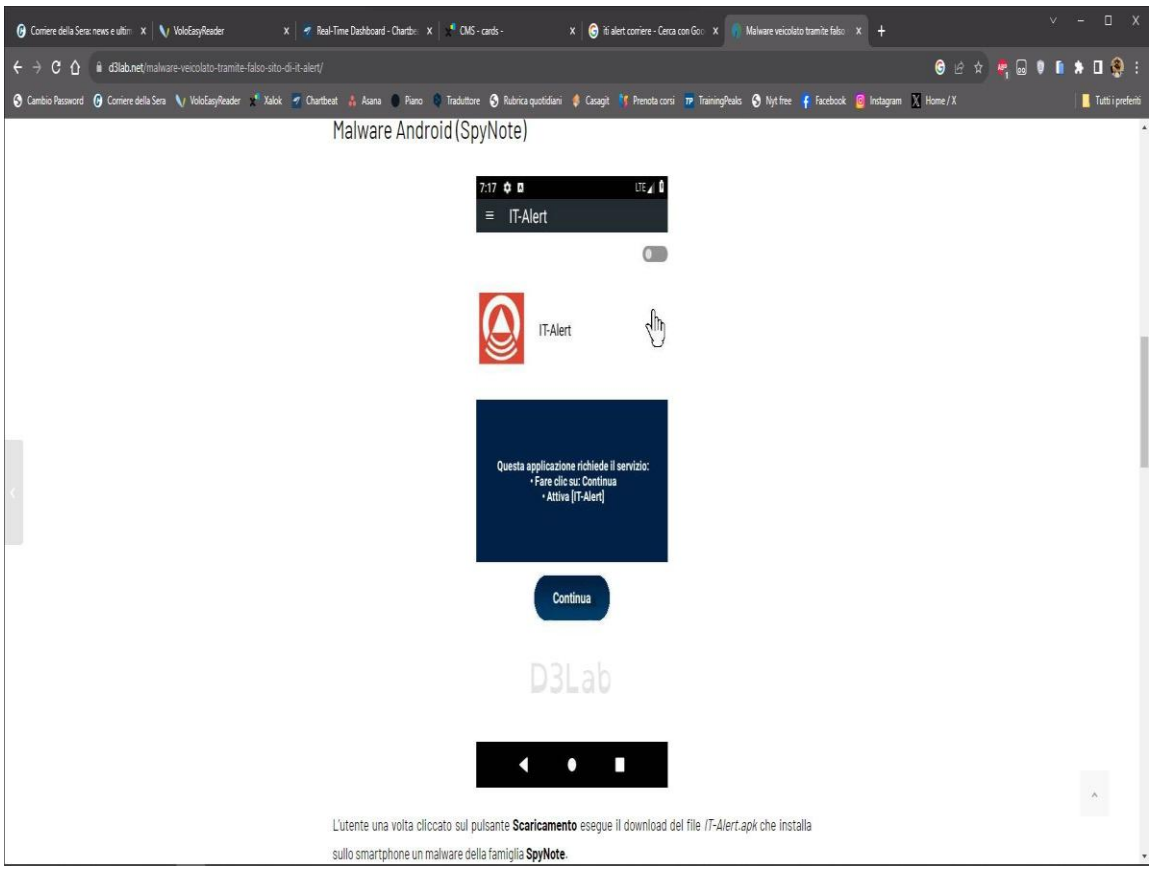
Investigazione criminale

La truffa **online stavolta mette la divisa**. A rendere questa mail piuttosto originale (e quindi potenzialmente pericolosa) è il riferimento alla **Polizia di Stato**, ai suoi vertici, all'**Europole** persino all'**Interpol**.

Innanzitutto a scrivere **è un non meglio precisato Dipartimento di investigazione criminale** che fa riferimento a un fascicolo di **inchiesta seguito da relativo numero di protocollo.** La mail recita testualmente: «Alla vostra attenzione. Io sottoscritto prefetto Vittorio Rizzi, vice direttore generale della pubblica sicurezza, **direttore centrale della polizia criminale** e il servizio per la cooperazione internazionale di polizia (Scip), in collaborazione con la sig. Catherine De Bolle, **direttore di Europole** capo della Brigata Protezione Minori (Bpm) visti**gli articoli 20 21-1 e da 75 a**

78 del codice di procedura penale.
Vi inviamo questo mandato poco dopo un sequestro di computer sotto copertura per informarvi che siete oggetto di diversi procedimenti legali in corso. Intraprendiamo azioni legali contro di voi...».
La mail continua elencando **i reati gravissimi** per i quali sarebbe stata **avviata l'azione penale**, ed essere associato a quell'**elenco invita il destinatario a rispondere** per chiarire che non c'entra: pornografia infantile, pedofilia, esibizionismo, cyberpornografia, offesa alla decenza».
Segue una sequela di oscuri riferimenti normativi e poi la minaccia: «Chiunque compia tali atti è passibile di procedimenti giudiziari e di una pena **da 5 a 35 anni**di reclusione e di una multa **da 78.000 a 535.000 euro**. Per motivi di riservatezza, vi inviamo questa e-mail. **Vi preghiamo di inviare le vostre giustificazioni via e-mail** in modo che possano essere esaminate e controllate per le sanzioni entro un periodo rigoroso di 72 ore». E qui potrebbe scattare la risposta da cui gli hacker possono trarre dati personali sensibili.
Come fare per evitarlo La mail che raccontiamo ha un contenuto molto allarmante, quindi innanzitutto occorre sangue freddo per distinguere le false minacce dalla realtà. Una premessa deve guidarci: nessun atto giudiziario ci verrebbe notificato usando una normale mail. Tutto il resto, è phishing. Veniamo al contenuto della mail, per capire da cosa possiamo capire che ci troviamo di fronte a un falso.
Innanzitutto: **non esiste nessun Dipartimento di investigazione criminale**, al massimo c'è una Direzione centrale della polizia criminale. Poi c'è il già citato problema del **dominio**: **quello della Polizia di stato non è composto così**. Le persone nominate esistono veramente (Vittorio Rizzi è capo della Criminalpol italiana e Catherine De Bolle guida l'Europol) ma la **Brigata protezione minori non esiste**. Infine gli articoli del codice di procedura penale riportati, che non hanno niente a che vedere con un'indagine penale. I primi due (20-21) riguardano il **difetto di giurisdizione e competenza**, gli altri due (75 e 78) i **rapporti con l'azione civile**. Esistono varie mail che circolano nel web con testi uguali o simili a questo. Per tutte, l'indicazione della Polizia postale (quella vera) è di ignorarle e di buttarle senza inviare nessun tipo di risposta. Anche in questo caso, viene ribadito che nessun atto giudiziario verrebbe inviato via mail ordinaria. Al massimo via Pec.

Il finto IT Alert



In **Campania** c'è chi sfrutta il timore legato a una eruzione vulcanica improvvisa per diffondere un **malware molto pericolosi per gli smartphone Android**. Lo specchietto delle allodole è il servizio IT Alert, il servizio di allerta nazionale che ha appena concluso la sua fase sperimentale. I ricercatori del **d3lab** hanno individuato una campagna **collegata ad un sito** che ricalca, nella grafica e nei contenuti, quello **ufficiale di IT Alert**. Sul sito si può leggere: «*A causa della possibile eruzione di un vulcano potrebbe verificarsi un terremoto nazionale. Scarica l'app per tenere d'occhio se la regione potrebbe essere colpita*». Chi visita questo sito con **iOS o con Safari** viene reindirizzato automaticamente al **sito ufficiale di IT-Alert**, chi lo visita invece con uno **smartphone Android viene portato allo scaricamento di una finta applicazione IT-Alert** che, se installata, carica all'interno del telefono della vittima un **malware della famiglia SpyNote**, decisamente pericoloso, perché sfrutta tutte le funzioni di accessibilità per leggere i contenuti presenti sullo **schermo del telefono e nei messaggi facilitando così il furto di credenziali**, sia di username e password sia di token di accesso per i sistemi protetti dall'autenticazione a due fattori.
I **destinatari principali dell'attacco**, quindi, sono gli **accessi ai siti delle banche.**