7 novembre 2024 | Ufficio federale della cibersicurezza UFCS

Truffe telefoniche nel ciberspazio

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS
Ufficio federale della cibersicurezza UFCS

Indice

1 Introduzione

Gli utenti telefonici si trovano sempre più spesso confrontati con telefonate fraudolente. Il fenomeno della truffa telefonica, tuttavia, non è nuovo. Da sempre esistono criminali che cercano di manipolare le persone con telefonate nell'intento di appropriarsi del loro denaro. Nelle pagine che seguono, il rapporto spiega il modus operandi della truffa, la prevalenza del fenomeno nel contesto degli sviluppi tecnologici e gli elementi utili a identificare tali tentativi di frode. Vengono inoltre illustrate le misure messe in atto dagli operatori di telecomunicazioni e dal legislatore.

1.1 Imbroglio o truffa?

Nel linguaggio comune si parla spesso di «imbroglio telefonico» o persino di «terrorismo telefonico». Sono entrambe espressioni colloquiali, mentre il termine utilizzato nella legge, e quindi corretto, per indicare questo reato è «truffa».

> Art. 146 Codice penale svizzero (truffa)
>
> Chiunque, per procacciare a sé o ad altri un indebito profitto, inganna con astuzia una persona affermando cose false o dissimulando cose vere, oppure ne conferma subdolamente l'errore inducendola in tal modo ad atti pregiudizievoli al patrimonio proprio o altrui, è punito con una pena detentiva sino a cinque anni o con una pena pecuniaria.

1.2 Truffe telefoniche nel ciberspazio

La truffa telefonica (nel ciberspazio) è un fenomeno ampiamente diffuso a livello globale, vista la possibilità di instaurare durante la chiamata un rapporto di fiducia e manipolare l'interlocutore in modo mirato. I truffatori riescono a reagire prontamente e adeguatamente a un eventuale scetticismo delle vittime. Il fine ultimo è estorcere denaro, informazioni personali o altri dati sensibili fingendo di chiamare per conto di un'organizzazione affidabile – ad es. una banca, un ufficio governativo o un'altra azienda. Come pretesto per i loro tentativi di frode, i truffatori utilizzano anche persone note alla vittima, ad es. un cliente, un collaboratore dell'helpdesk o addirittura una figura interna all'azienda, come un superiore o un collega del reparto di informatica. Il «trucco del nipote» è un classico esempio che fa leva sulla vita privata della vittima: un truffatore chiama una persona anziana fingendo di essere la nipote o il nipote che ha bisogno di denaro.

Il progresso tecnologico consente agli attori criminali di abbinare telefonate e mondo ciber: attraverso procedimenti informatici possono affinare la loro tecnica e utilizzare i dati sottratti a loro vantaggio, servendosi delle nuove tecnologie sia prima che durante e/o dopo un tentativo di truffa.

La combinazione tra truffa telefonica e impiego di nuove tecnologie ha preso piede a partire dai primi anni 2000, quando i cybercriminali hanno iniziato a utilizzare la tecnologia Voice-over-IP (*VoIP*), applicazioni Voicemail e sistemi di chiamata automatizzati per il phishing telefonico. Con la tecnologia VoIP è possibile generare numeri di telefono fasulli e mascherare l'identità del chiamante, facendo credere che le telefonate provengano da imprese o istituzioni legittime. Il Voice-over-IP consente inoltre ai truffatori di effettuare centinaia di telefonate fraudolente automatizzate via Internet, il che complica la possibilità di tracciare i numeri utilizzati.

Col passare del tempo è stata messa a punto una molteplicità di tecniche criminali differenti, che sfruttano il binomio tra telefonate fraudolente e mondo ciber. Si può decidere, ad esempio, di chiamare un numero a caso oppure di raccogliere a monte i dati personali da fonti pubbliche, social network o precedenti fughe di dati, per poi personalizzare gli attacchi e guadagnarsi la fiducia delle vittime. Le truffe telefoniche nello spazio digitale sono spesso integrate da altre forme

di ingegneria sociale[1], così come dall'invio di e-mail di phishing o dalla creazione di siti web fasulli con cui incrementare la credibilità dell'attacco. Alcuni criminali, ad esempio, inducono le loro vittime a chiamarli inviando loro prima un'e-mail.

Non appena una vittima fornisce i propri dati, i criminali possono utilizzarli per arricchirsi mediante frodi, commettere altri reati o rivenderli ad altri criminali. In alcuni casi possono fungere da procacciatori di primi accessi (i cosiddetti Initial Access Broker). Questi attori sono specializzati nel compromettere sistemi e reti informatiche per poi vendere l'accesso non autorizzato ad altri hacker.

2 Tecniche utilizzate

Le truffe telefoniche nello spazio digitale si fondano su due aspetti – il progresso tecnologico nel settore delle telecomunicazioni e la pura manipolazione psicologica.

2.1 Sviluppi tecnologici

Tra i parametri tecnologici si annoverano, ad esempio:

- Chiamate automatizzate (cosiddette robocall o chiamate robotizzate):
  sono chiamate effettuate a tappeto, generalmente in lingua inglese. L'intento è instaurare un clima di intimità e fiducia facendo credere che la telefonata provenga da un'organizzazione nota. Grazie a questa tecnica i criminali riescono a contattare un gran numero di potenziali vittime con risorse di personale ridotte, concentrandosi su coloro che, dopo aver ascoltato la chiamata automatizzata, decidono di rimanere in linea.
- Falsificazione dei numeri di telefono (cosiddetto spoofing[2]):
  i cibercriminali falsificano l'ID del chiamante in maniera tale che la vittima veda un numero affidabile e sia indotta a rispondere. L'Ufficio federale della cibersicurezza (UFCS) ha osservato casi di spoofing in cui sono stati falsificati non solo numeri di telefono di banche, ma anche di autorità di polizia.
- Incitazione a richiamare:
  i criminali inviano contemporaneamente a più dipendenti di un'azienda un messaggio audio registrato. L'ID del chiamante è probabilmente modificato in maniera digitale così da assomigliare a quello di un collega interno all'organizzazione. L'audio contiene un messaggio della massima urgenza. Spesso la persona di cui si sente la voce finge di essere qualcuno di fidato e invita la vittima a richiamarla a un determinato numero per avere informazioni più dettagliate. Il numero da richiamare è però un numero che i criminali hanno scelto a monte appositamente per la truffa.

2.2 Inganno e manipolazione

I cibercriminali sono abili nel manipolare le loro vittime. L'uso di tecniche psicologiche, come la manipolazione, da parte di cibercriminali con l'intento di estorcere informazioni riservate o denaro è detto ingegneria sociale. Questa tecnica sfrutta la natura e i comportamenti basilari dell'essere

[1] Cfr. cap. 2.2. per la definizione

[2] In generale lo spoofing consiste nel camuffare una comunicazione da fonte ignota in una comunicazione proveniente da una fonte nota e affidabile (simile al furto d'identità).

umano per ingannare le vittime. Attraverso fonti pubbliche, ad esempio, i cibercriminali si informano a priori in merito alle loro vittime e utilizzano quei dati personali per apparire seri, guadagnarsi la fiducia della controparte e carpire ulteriori informazioni. Un elemento chiave dell'ingegneria sociale è l'uso di scenari d'emergenza. Il criminale inscena una situazione critica, come l'imminente chiusura di un conto o un incidente, per indurre la vittima a rivelare senza indugio informazioni sensibili. Sotto stress, infatti, non si ha tempo di riflettere in modo logico e razionale su quanto si è sentito. Anche altre emozioni possono essere sfruttate per scopi criminali, ad esempio la curiosità, il senso di colpa, l'empatia, la paura o il rispetto per le autorità. Queste manipolazioni emotive inducono la vittima ad agire in modo avventato senza riflettere.

3 I criminali e il progresso tecnologico

Dalla comparsa delle prime truffe telefoniche negli anni 2000, il fenomeno associato al mondo ciber si è costantemente evoluto – e non si intravede ancora una fine. Grazie al progresso tecnologico i criminali hanno a disposizione strumenti sempre più potenti e sofisticati. All'inizio le chiamate provenivano soprattutto da numeri internazionali o da Internet. Oggi, invece, i criminali possono fare ricorso allo spoofing di numeri telefonici locali e nascondere alla vittima l'identità del chiamante, visualizzando come numero di chiamata un numero di telefono locale.

3.1 Esempi: SIM-Box, malware e abuso di SIM

Uno degli sviluppi tecnologici che ha facilitato ai criminali la messa in atto di truffe telefoniche è la SIM-Box.[3] Si tratta di un dispositivo che, utilizzando più carte SIM prepagate – spesso acquistate con identità fasulle – devia le telefonate su una rete desiderata, facendole diventare locali. Questo tipo di truffa fa leva sulla differenza tra la tariffa locale e quella internazionale, consentendo ai criminali di pagare solo la tariffa locale. Oggi sono sempre più i criminali che possono ricorrere a questo metodo, essendo diventato molto più economico.

Per mettere a segno le truffe, tuttavia, ora si utilizzano anche software dannosi (malware)[4]. Esistono malware che manipolano i dispositivi, installano messaggi vocali preregistrati e reindirizzano le chiamate a call center fraudolenti. Una volta scaricati e installati, questi malware richiedono il consenso della vittima per accedere a contatti, microfono, videocamera, servizio di localizzazione ecc. Con un trojan, ad esempio, è possibile ingannare la vittima nel momento in cui compone il numero di telefono della propria banca, facendole credere che stia comunicando con il servizio clienti.

Recentemente la comparsa delle eSIM ha permesso ai criminali di sviluppare un'altra variante di truffa telefonica nel ciberspazio. Con la tecnologia eSIM, la carta SIM digitale è integrata nel dispositivo, il che offre agli utenti flessibilità e comodità, ma comporta anche nuovi rischi di frode. Nelle truffe eSIM i criminali utilizzano tecniche come il SIM swapping o l'ingegneria sociale per impossessarsi del numero di cellulare della vittima e accedere quindi a vari servizi, come l'online banking e i social network, che usano quel numero come sistema di autenticazione. Visto che molti servizi online utilizzano l'autenticazione a due fattori (2FA) via SMS, appropriandosi del numero di cellulare i criminali possono intercettare i codici di sicurezza e accedere indebitamente ad account e conti bancari, il che può comportare sia perdite finanziarie che violazioni della privacy. Per tutelarsi, gli utenti dovrebbero utilizzare password forti e metodi di autenticazione alternativi, come app di autenticazione o token di sicurezza. Gli operatori di telefonia mobile, inoltre, possono offrire un'ulteriore sicurezza applicando un processo di verifica più rigoroso in caso di cambio dei profili eSIM.

---

[3] https://www.infosysbpm.com/blogs/bpm-analytics/what-is-sim-box-fraud.html

[4] Per esempio applicazione di vishing, trojan

3.2 Avvento dell'intelligenza artificiale (IA)

Dall'avvento dei metodi di intelligenza artificiale (IA), come l'apprendimento automatico (machine learning), queste nuove tecnologie vengono sempre più spesso utilizzate per automatizzare le chiamate ed eludere i sistemi di riconoscimento. Un ostacolo per i criminali è rappresentato dalla lingua. Mentre per le e-mail e gli SMS vengono ormai utilizzati strumenti di traduzione affidabili, nel caso delle telefonate non è sempre così. Generalmente, quindi, le chiamate vengono effettuate in inglese, la lingua più parlata al mondo. Anche in questo caso l'IA potrebbe tornare utile ai criminali in futuro. Oggi è normale condividere contenuti vocali via Internet. Grazie allo sviluppo e alla commercializzazione di applicazioni software per l'intelligenza artificiale generativa (GenAI), che forniscono all'istante risultati relativamente attendibili, bastano pochi clic per gettare le basi di una truffa. Questa evoluzione ha un impatto significativo sul modus operandi dei criminali e quindi sulla strategia di difesa dalle minacce di natura vocale. Tutto ciò di cui hanno bisogno i criminali per imitare una voce, infatti, è un frammento audio che riproduca, ad esempio, una telefonata registrata o un video pubblicato sui social network.

Il fatto è che più informazioni vengono condivise via Internet o nei social network, più si è esposti ai rischi legati all'usurpazione d'identità e ad altre attività cibercriminali. È importante agire in modo proattivo, riducendo i dati personali disponibili online o quanto meno accettando consapevolmente le possibili conseguenze derivanti dalla loro pubblicazione.

In Svizzera, tra gli schemi di frode basati sull'IA si annoverano soprattutto la truffa telefonica, la truffa degli investimenti a nome di personaggi famosi e la fake sextortion con immagini generate dall'IA. Visto il numero di segnalazioni relativamente ridotto in questo ambito, l'UFCS ritiene che probabilmente si tratti ancora di primi tentativi da parte dei cibercriminali per sondare le possibilità future di utilizzare l'IA con profitto nei ciberattacchi. In molti casi di truffa è difficile stabilire in che misura sia stata utilizzata l'intelligenza artificiale, per cui si può ad esempio solo supporre se si sia fatto ricorso o meno a un tool di traduzione. Sono pochi i casi in cui l'utilizzo dell'IA è evidente.

4 Truffe telefoniche nel ciberspazio in Svizzera

Le truffe telefoniche nel ciberspazio sono un fenomeno ormai consolidato in Svizzera. Se ne segnalano casi sin dalla nascita della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) nel 2004, successivamente trasformata in Centro nazionale per la cibersicurezza (NCSC) e infine nell'UFCS.

4.1 Fake support e fake support pop-up

I primi casi di truffa telefonica nel ciberspazio registrati in Svizzera consistevano, ad esempio, in una chiamata da parte di presunti operatori del servizio di assistenza Microsoft con cui si veniva informati che il proprio computer era stato hackerato e che occorreva intervenire all'istante. Le vittime venivano indotte a installare sul loro computer un software di accesso remoto, ad esempio AnyDesk, dopodiché i criminali cercavano di connettersi all'online banking del malcapitato per effettuare bonifici.

Da qualche tempo l'UFCS sta osservando una variante simile, in cui compaiono finestre pop-up mentre si naviga su siti pubblicitari. La configurazione del pop-up è tale da indurre l'utente a credere al suo contenuto. In esso viene comunicato che il computer è stato infettato da un virus e che, per risolvere il problema, è necessario chiamare un determinato numero di telefono. Da quel momento in poi la truffa procede secondo lo schema sopra descritto.

4.2 Telefonate fraudolente da parte di presunti impiegati di banca

L'UFCS riceve regolarmente anche segnalazioni di chiamate da parte di presunti impiegati di banca che chiedono se la persona in questione abbia effettuato un determinato pagamento.[5] In molti casi il chiamante sostiene, ad esempio, che sia stato registrato un addebito per l'acquisto di uno schermo piatto presso un negozio di elettronica e consiglia di telefonare immediatamente alla divisione antifrode della Polizia cantonale. Alla vittima viene subito fornito il presunto numero della polizia, dopodiché la si convince a effettuare una serie di operazioni e a controllare i movimenti sul suo online banking, confermando vari dati così da poter stornare il pagamento. L'UFCS presume che in questi casi l'intento sia di indurre la vittima ad accedere a un sito creato dai criminali, dal quale sarebbe possibile annullare i pagamenti fittizi, presumibilmente fraudolenti. A tal fine vengono chieste le credenziali d'accesso e le password temporanee. Allo stesso tempo, con i dati ottenuti i criminali si collegano al portale e-banking della vittima ed effettuano personalmente pagamenti a loro favore. Nel frattempo, alla vittima viene fatto credere che lo storno sia andato a buon fine. Anche in questo caso esistono diverse varianti con cui i cibercriminali cercano di insinuarsi nel computer della vittima attraverso un software di accesso remoto per poi compiere azioni fraudolente.

4.3 Robocall – chiamate automatizzate da parte di presunte autorità

Da luglio 2023 si susseguono in Svizzera ondate di truffe telefoniche su larga scala. Ogni giorno i criminali, spacciandosi per la polizia, effettuano migliaia di chiamate automatizzate a cittadini svizzeri, accusando le potenziali vittime di un reato. La truffa in questi casi consiste nel chiamare contemporaneamente una grande quantità di numeri. Se la persona risponde, parte un messaggio registrato che la informa di un'indagine in corso da parte della polizia e la invita a premere il tasto «1» per ricevere ulteriori informazioni. Se lo fa, la persona viene messa in contatto con un operatore di un call center. Questi fa credere alla vittima di essere coinvolta in un caso di riciclaggio di denaro o in un altro reato e la informa che il suo conto corrente verrà bloccato. Anche in questo tipo di frode i criminali accedono al conto bancario della vittima attraverso AnyDesk o un software di accesso remoto analogo.

I criminali sono organizzati in call center e si esprimono perlopiù in inglese con un accento straniero, anche se non è raro ormai – come riscontrato dall'UFCS – sentirli parlare con un buon livello di tedesco o francese.

Falsificano il loro ID del chiamante attraverso il cosiddetto spoofing. Spesso scelgono numeri di cellulare casuali, che nelle truffe telefoniche vengono visualizzati alla vittima come numero da cui proviene la chiamata. I veri proprietari dei numeri vengono poi presumibilmente richiamati da sconosciuti, ignari del fatto che la chiamata originaria non era partita dal numero rubato visualizzato sul display.

Grazie al trucco del messaggio registrato, i criminali possono effettuare più chiamate contemporaneamente e selezionare le vittime adatte. A quel punto possono concentrarsi unicamente sulle chiamate a cui si è risposto e nelle quali le persone rimangono in linea e seguono, ad esempio, le istruzioni della voce registrata.

L'UFCS ha riscontrato che alcune persone che, durante la telefonata, avevano espresso dubbi sull'autenticità della chiamata sono state successivamente richiamate con un numero pubblico

[5] Cfr. «In primo piano»: https://www.ncsc.admin.ch/ncsc/it/home/aktuell/im-fokus/2023/wochenrueckblick_44.html

dell'Interpol ed esortate a controllare il numero su Internet. Con questa tattica i criminali sperano di guadagnare credibilità.

Sebbene vi siano alcune differenze, le similitudini tra le classiche telefonate di fake support e le telefonate minatorie automatizzate sono evidenti:

- i truffatori operano da call center;
- i truffatori utilizzano numeri di telefono rubati, spesso con lo stesso prefisso del numero della vittima;
- le vittime vengono spesso indotte a installare un software di accesso remoto e quindi a consentire l'accesso all'online banking.

4.3.1 Differenze tra telefonate di fake support e robocall

Le figure 1 e 2 illustrano l'impatto delle telefonate minatorie automatizzate da parte di presunti funzionari di polizia sulle segnalazioni ricevute dall'UFCS negli ultimi 12 mesi. A seguire si confrontano i fenomeni fake support e telefonate minatorie apparentemente effettuate dalla polizia, evidenziando le differenze più rilevanti.

In entrambi i casi l'obiettivo finale è convincere le potenziali vittime a scaricare un software di accesso remoto e concedere successivamente ai criminali l'accesso al computer. Nel caso del fake support si tratta di un approccio individuale, come descritto in precedenza: i criminali contattano ogni potenziale vittima singolarmente. Da un anno e mezzo, infatti, le segnalazioni trasmesse all'UFCS si mantengono stabili a un livello modesto, per una media di circa 60 segnalazioni al mese. Il modus operandi dei criminali pare essere dispendioso in termini di risorse e non molto produttivo.

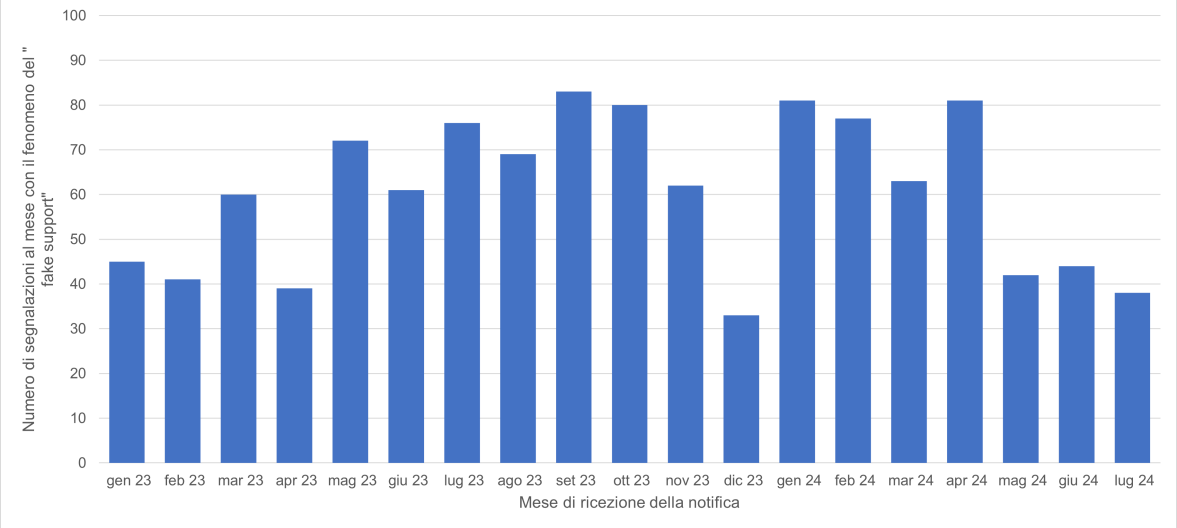

***Figura 1**. Segnalazioni relative a telefonate di fake support al mese. Il numero di segnalazioni si distribuisce in modo regolare sull'arco dell'anno e si mantiene a un livello basso.*

Non sorprende dunque che i criminali abbiano cercato delle modalità con cui rendere questa variante di truffa più efficace. Nel caso delle telefonate minatorie da parte di presunte autorità, non sono i criminali stessi a chiamare, bensì vengono selezionati in maniera casuale e automatizzata molteplici numeri diversi nell'arco di breve tempo. Soltanto coloro che rimangono in linea e premono il tasto citato nel messaggio automatico vengono inoltrati a un truffatore. I criminali si occupano pertanto solo delle chiamate che si presume possano andare a buon fine. In tal caso, quindi, la situazione sul fronte delle segnalazioni pervenute è totalmente differente. Fino a giugno 2023 questo tipo di truffa era praticamente sconosciuta in Svizzera. A partire da luglio dello stesso

anno, invece, il numero di segnalazioni è costantemente aumentato, raggiungendo il mese successivo la soglia di 1000 al mese. Si è trattato probabilmente di un primo test da parte dei criminali. A ottobre dello stesso anno i numeri sono letteralmente esplosi. Soltanto per questo tipo di truffa, in alcuni momenti l'UFCS ha ricevuto fino a 1000 segnalazioni alla settimana. Dopo una breve pausa all'inizio del 2024, nel mese di febbraio del 2024 il numero di segnalazioni ha ripreso a salire vertiginosamente, raggiungendo ancora una volta valori record di oltre 1500 a settimana. Le statistiche del 31 luglio 2024 mostrano che l'UFCS riceveva solo ancora un centinaio di segnalazioni alla settimana relative a questo fenomeno.

Si evince pertanto che il numero di chiamate fraudolente, e quindi di segnalazioni all'UFCS, non dipende tanto dalle risorse di personale messe in campo dai criminali, quanto dalle capacità tecniche e dall'efficienza dei bot che effettuano le chiamate automatizzate.

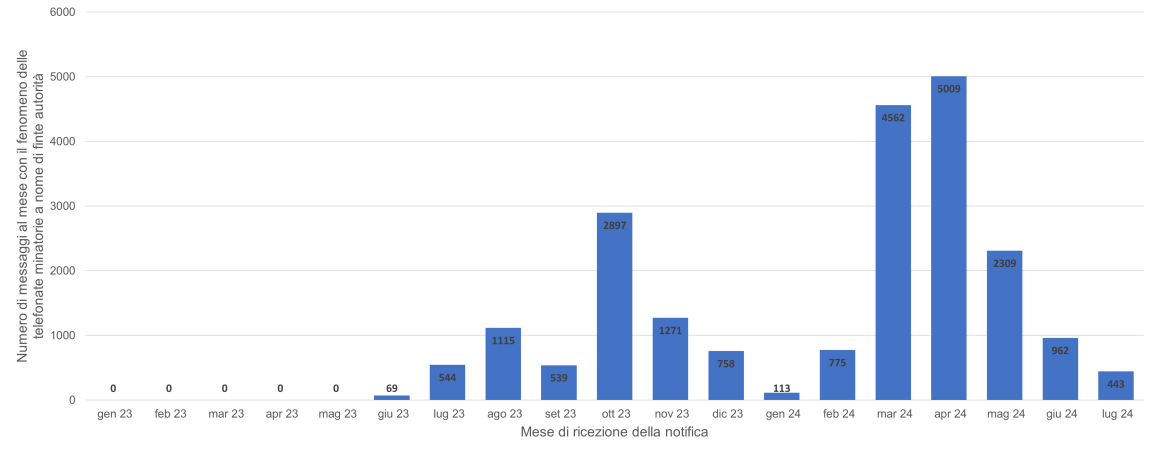

***Figura 2**. Segnalazioni di telefonate fraudolente effettuate a nome di presunte autorità. Spicca in maniera evidente l'alto numero di segnalazioni a marzo e aprile 2024. Nell'estate del 2024 il trend ha iniziato nuovamente a calare.*

4.3.2 Gli orari di lavoro dei criminali

La figura 3 mostra la distribuzione media delle segnalazioni ricevute nell'arco di una giornata tipo, tenendo conto soltanto delle segnalazioni di telefonate fraudolente da parte di presunte autorità. L'UFCS parte dal presupposto che la maggior parte dei casi di truffa telefonica legata al mondo ciber venga segnalata subito dopo la chiamata. Di conseguenza, l'ora della telefonata fraudolenta e l'ora di ricezione della segnalazione praticamente coincidono. Gli orari di lavoro dei criminali vengono pertanto stimati sulla base delle segnalazioni ricevute.

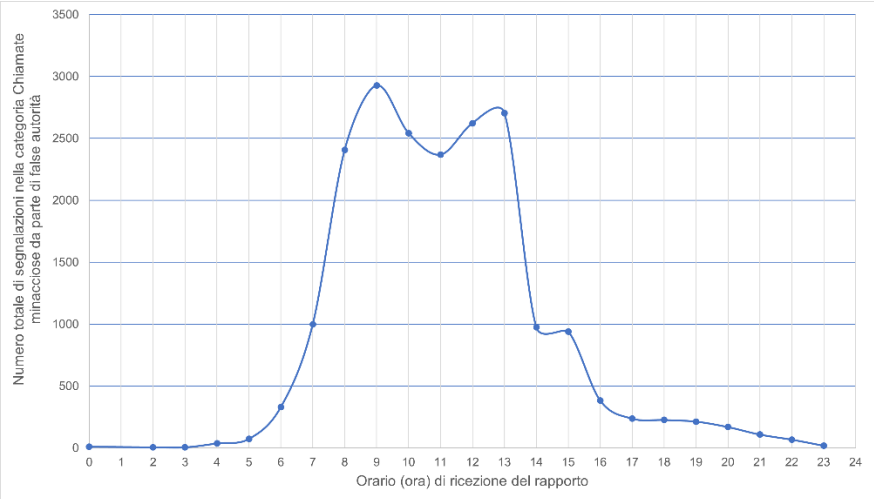

***Figura 3.** Distribuzione temporale media delle telefonate da parte di presunte autorità. Le segnalazioni iniziano alle 5.00 e raggiungono un primo picco alle 9.00. C'è un secondo picco alle 13.00, mentre dalle 16.00 diminuiscono nuovamente.*

La distribuzione ricorda una tipica giornata di lavoro, che inizia alle 6.00 e termina alle 16.00. I criminali sembrano però fare una pausa intorno a mezzogiorno. Visto il numero relativamente ridotto di segnalazioni pervenute nella fascia oraria delle 11.00 si suppone che vi sia una pausa pranzo – anche se a quell'ora è troppo presto per mangiare in Svizzera – il che lascia supporre che i criminali si trovino in un Paese più a est.

5 Il punto di vista di un operatore di telecomunicazioni

Dopo l'analisi delle segnalazioni trasmesse all'UFCS, di seguito viene presentato il punto di vista di un operatore di telecomunicazioni svizzero.

5.1 Gioco del gatto e del topo

I criminali sviluppano sempre nuovi metodi per truffare i clienti telefonici. Combinando diverse tecniche massimizzano le loro possibilità di successo. Una di queste tecniche è l'usurpazione d'identità, che consiste nel nascondere la vera identità della persona che effettua la chiamata. I truffatori sanno che si tende a rispondere più facilmente al telefono se si ritiene che il chiamante sia affidabile. Il metodo sembra essere efficace, tanto che negli ultimi due anni il numero di chiamate con falsa identità è aumentato del 50 per cento – una tendenza destinata a continuare.

Anche l'uso dell'IA a fini di truffa telefonica gode di estrema popolarità tra i criminali. Sebbene i metodi sinora utilizzati per effettuare le chiamate automatizzate siano ancora relativamente rudimentali, è solo una questione di tempo prima che i criminali sviluppino tecniche più sofisticate per ottimizzare i loro tentativi di truffa. A prescindere dal fatto che i chiamanti utilizzino o meno un'identità fasulla, attualmente agli operatori di telecomunicazioni (*Voice Service Provider*) non è né consentito né tecnicamente possibile riconoscere in base a contenuti, lingua o voce i robocall che impiegano metodi di IA. Questo limite rappresenta un notevole svantaggio, considerato che i cibercriminali sfruttano l'IA per scopi malevoli. Gli operatori di telecomunicazioni potrebbero utilizzare gli stessi accorgimenti tecnici basati sull'IA non solo per monitorare modelli di chiamata, ma anche per identificare i robocall analizzando il contenuto delle telefonate. Mediante avvisi automatizzati e rispettosi della privacy, potrebbero reagire di conseguenza e adottare le contromisure opportune. Lo svantaggio attuale deve essere colmato affinché gli operatori di telecomunicazioni non continuino a rimanere indietro rispetto ai criminali.

5.2 Misure adottate dagli operatori di telecomunicazioni

Nella lotta alla criminalità sono varie le misure di natura tecnico-legale che vengono adottate ormai da anni. Attraverso opportuni interventi tecnici gli operatori di telecomunicazioni possono bloccare gli attacchi telefonici e limitare il numero dei tentativi:

- con il filtraggio delle chiamate si possono analizzare le chiamate in arrivo e bloccare i numeri sospetti associati a frodi telefoniche;
- con il riconoscimento vocale si possono identificare i chiamanti, in particolare in caso di operazioni rischiose o interazioni sensibili;
- con gli algoritmi gli operatori possono individuare modelli di chiamata o comportamenti insoliti che potrebbero indicare un tentativo di attacco, come ad es. un elevato volume di chiamate a determinati numeri in un breve lasso di tempo.

In Svizzera gli operatori si concentrano sull'analisi dei modelli di chiamata per individuare eventuali anomalie. Si sta inoltre lavorando per limitare lo spoofing di numeri svizzeri dall'estero. Un'altra criticità è il fatto che i truffatori modificano costantemente le loro modalità d'azione. È dunque fondamentale sensibilizzare la popolazione in merito ai rischi. Alcuni operatori di telecomunicazioni, ad esempio, informano regolarmente i loro clienti su questo tema attraverso diversi canali e raccomandano un'adeguata dose di scetticismo. Dati personali come password e codici PIN non vanno rivelati in nessun caso al chiamante. Gli operatori consigliano inoltre ai loro clienti di attivare il filtro delle chiamate, disponibile sia per la rete fissa che per i cellulari, così da essere tutelati anche contro le chiamate pubblicitarie indesiderate.

5.3 Il ruolo di supporto dell'Ufficio federale delle comunicazioni (UFCOM)

Secondo gli operatori di telecomunicazioni, le basi legali di riferimento esistono già. Attualmente, gli operatori e l'Ufficio federale delle comunicazioni (UFCOM) stanno lavorando a un'iniziativa congiunta per trovare una soluzione settoriale al problema. Non appena l'industria delle telecomunicazioni svizzera avrà individuato una soluzione adeguata, l'UFCOM potrà supportarne l'implementazione, la regolamentazione ed eventualmente la supervisione.

Nel complesso la lotta alle truffe telefoniche rimane un'impresa ardua, che richiede una stretta collaborazione tra gli operatori, le autorità di regolamentazione e la popolazione. Soltanto così si potranno sviluppare soluzioni tecniche che siano conformi alla legge, efficaci e rispettose della privacy dei clienti. È chiaro che, anche in futuro, non ci sarà una protezione efficace al 100 per cento contro le truffe telefoniche, ma con le giuste contromisure è possibile ridurre il rischio.

6 Protezione dell'individuo: un compito giuridicamente complesso

Oltre all'articolo 146 del Codice penale svizzero, vi sono altre leggi che compongono il quadro giuridico:

- la legge federale contro la concorrenza sleale (LCSI) vieta le pratiche d'affari sleali, tra cui anche prassi fraudolente come la truffa telefonica;
- la legge federale sulla protezione dei dati (LPD) disciplina il trattamento dei dati personali e può essere applicata nei casi in cui la truffa telefonica comporti la raccolta indebita o l'uso improprio di dati personali;
- la legge sulle telecomunicazioni (LTC) regolamenta i servizi e le reti di telecomunicazione e può essere applicata nei casi in cui la truffa telefonica comporti un uso improprio delle infrastrutture di telecomunicazione;
- l'Autorità federale di vigilanza sui mercati finanziari (FINMA) vigila sugli istituti finanziari e sulle assicurazioni e può quindi imporre sanzioni alle entità coinvolte in truffe telefoniche mirate contro il settore finanziario.

6.1 Aspetti legali dal punto di vista dell'UFCOM

Il diritto delle telecomunicazioni obbliga gli operatori a tutelare i loro clienti dalle chiamate pubblicitarie sleali (art. 3 cpv. 1 lett. u, v e w LCSI), fornendo loro uno strumento adeguato per respingere tali chiamate. In pratica si tratta di offrire loro una soluzione di filtro (cfr. cap. 5.2), con cui contrastare questo tipo di telefonate nella misura in cui lo stato della tecnica lo consenta (art. 45*a* LTC). Ciò significa che gli operatori devono reagire a nuove tecnologie e procedure e adattare di

conseguenza la funzionalità dei filtri. Essendo le chiamate pubblicitarie sleali generalmente abbinate allo spoofing del numero visualizzato, i filtri messi a disposizione dagli operatori sono anche idonei a combattere l'usurpazione d'identità (art. 179^{decies} CP) nell'ambito delle truffe telefoniche. Questi strumenti possono contribuire a proteggere gli utenti dai tentativi di frode telefonica.

Dal punto di vista del diritto delle telecomunicazioni, una vittima di truffa può rifarsi all'articolo 146 del Codice penale svizzero ed esercitare il proprio diritto di informazione (art. 45 LTC). Quest'ultimo mira a far sì che gli operatori su cui poggia il collegamento possano risalire all'origine, ovvero all'utenza, da cui provengono le chiamate fraudolente. Le chiamate con numeri oggetto di spoofing possono essere considerate abusive, in particolare se effettuate nell'ambito di un atto presumibilmente fraudolento. Ovviamente spetta a un tribunale penale decidere se tale condizione sia soddisfatta o meno, tuttavia è sufficiente dimostrare la credibilità della fattispecie. A prescindere da ciò, il vero problema è che le chiamate solitamente provengono dall'estero e l'operatore straniero, anche se rintracciato, non è soggetto al diritto delle telecomunicazioni svizzero.

6.2 Limiti imposti dalle leggi internazionali

Un problema legato al filtraggio delle telefonate è che questa prassi non deve causare il blocco delle chiamate legittime, in quanto ciò violerebbe l'obbligo di interoperabilità che, per principio, impone agli operatori di dover inoltrare le chiamate ai destinatari. Occorre altresì considerare che, in virtù del segreto delle telecomunicazioni, gli operatori non possono conoscere il contenuto delle chiamate. I filtri devono pertanto essere impostati in base a vari indicatori e devono funzionare in maniera dinamica, visto che i criminali cambiano anche continuamente i numeri adibiti alle truffe. Se ad esempio utilizzano numeri di cellulare, diventa ancora più difficile per gli operatori valutare se la chiamata sia legittima o meno, poiché potrebbe provenire da una persona in vacanza e non da un truffatore.

Nel mese di maggio del 2024 gli Stati Uniti hanno scoperto un gruppo criminale chiamato «Royal Tiger», il cui obiettivo è di agevolare le chiamate fraudolente attraverso le reti internazionali. Secondo un comunicato stampa[6] il gruppo cerca di spacciarsi per autorità governative, banche e imprese del settore pubblico. Scopo delle telefonate è ingannare i consumatori a livello mondiale, offrendo presunti tassi di interesse ridotti sulle loro carte di credito o chiedendo loro di approvare richieste d'acquisto per ordini che non hanno mai effettuato. Attualmente Royal Tiger opera dall'India, dal Regno Unito, dagli Emirati Arabi Uniti e dagli Stati Uniti. Negli USA il legislatore ha deciso di creare una nuova classificazione per questo tipo di robocall, denominata Consumer Communications Information Services Threat (C-CIST)[7].

In Austria, il 21 dicembre 2023 (con termine di attuazione al 1° settembre 2024) è entrata in vigore una modifica del regolamento[8] che obbliga gli operatori nazionali a verificare i numeri di telefono delle chiamate effettuate dall'estero con numeri austriaci. Se tale verifica non è possibile, il numero non deve essere visualizzato. Ciò non impedisce tuttavia eventuali chiamate fraudolente da numeri provenienti da altri Paesi, in particolare di lingua tedesca, come ad es. lo spoofing telefonico con numeri germanici.

---

[6] https://www.documentcloud.org/documents/24661582-doc-402506a1

[7] https://www.documentcloud.org/documents/24661584-da-24-388a1

[8] https://www.rtr.at/9_novelle_kem-v

6.3 Intelligenza artificiale e futuro

Alla complessità tecnica si aggiunge ora anche il problema della manipolazione delle persone attraverso l'uso dell'IA. In data 12 dicembre 2023 l'UFCS ha pubblicato un articolo[9] sull'uso dell'IA nei tentativi di truffa. La combinazione tra spoofing e modifica della voce tramite IA offre ai criminali grandi opportunità. Man mano che la tecnologia migliora, diventa più difficile riconoscere i tentativi di truffa.

Una soluzione per arginare lo spoofing sarebbe quella di introdurre un processo di verifica (simile a quello utilizzato per le e-mail) con cui controllare l'origine e l'autenticità del numero. Soluzioni di questo tipo sono attualmente oggetto di discussione in seno a vari organismi internazionali, ad esempio in seno Conferenza europea delle amministrazioni delle poste e delle telecomunicazioni (CEPT), al Comitato per le comunicazioni elettroniche (ECC) e all'Unione internazionale delle telecomunicazioni (UIT), a cui l'UFCOM prende parte regolarmente. Dall'ultima revisione, il diritto delle telecomunicazioni contiene le basi legali di riferimento per l'introduzione di tali processi. Affinché portino a un effettivo miglioramento della situazione, tuttavia, dovrebbero essere implementati, oltre che in Svizzera, nel maggior numero possibile di Paesi.

7 Misure di prevenzione raccomandate dall'UFCS

Per proteggersi dalle truffe telefoniche, i cittadini possono adottare le seguenti misure:

1. Non fidatevi di chiunque: interrompete immediatamente le telefonate non plausibili.
2. Non lasciatevi intimidire o mettere sotto pressione.
3. Non comunicate mai password o codici PIN al telefono.
4. Non rivelate informazioni aziendali a sconosciuti.
5. Non concedete mai l'accesso al vostro computer a sconosciuti, anche se danno l'impressione di essere affidabili.

8 Conclusione

In molti tentativi di truffa telefonica nello spazio digitale, l'elemento più vulnerabile è la persona all'altro capo della linea. Se messa sotto pressione, a livello privato o professionale, può agire in modo avventato anziché prudente, soprattutto quando si tratta di risolvere presunte emergenze. In questi casi, sono spesso le vittime stesse ad aprire la porta ai criminali opportunisti. Al giorno d'oggi la sicurezza non può e non deve dipendere soltanto dalla capacità degli utenti di identificare correttamente il pericolo e adottare le misure di protezione adeguate. I criminali operano a livello globale e all'interno di reti internazionali. I metodi di identificazione tradizionali, come la famosa «Calling Line Identification», sono ormai superati per effetto del progresso tecnologico. A differenza del settore delle e-mail, dove grazie all'autenticazione DMARC[10] è possibile riconoscere e

[9] https://www.ncsc.admin.ch/ncsc/it/home/aktuell/im-fokus/2023/wochenrueckblick_49.html

[10] Domain-based DMARC (Message Authentication Reporting and Conformance) è un protocollo di sicurezza e-mail. DMARC verifica i mittenti delle e-mail sulla base dei protocolli Domain Name System (DNS), DomainKeys Identified Mail (DKIM) e Sender Policy Framework (SPF).

limitare le tecniche di spoofing, nella telefonia non esistono ancora nuovi metodi di autenticazione. Secondo l'UFCOM i tentativi effettuati con i protocolli STIR/SHAKEN[11] nell'America del Nord non hanno avuto particolare successo. Numerose organizzazioni del settore hanno abbandonato questo standard[12], il che sottolinea quanto sia difficile introdurre nuovi metodi di autenticazione a livello mondiale.

[11] Serie di protocolli per l'autenticazione dei chiamanti e dei loro dati in caso di chiamate sulla rete VoIP (https://www.fcc.gov/call-authentication)

[12] https://commsrisk.com/global-stir-shaken-is-dead-what-comes-next/