UN CALCIO ALLE FRODI.

Vademecum per i Cittadini contro le frodi informatiche.

UN **PROGETTO SOCIALE** A CURA DI:

Posteitaliane

Polizia di Stato

CAGLIARI CALCIO

IN COLLABORAZIONE CON sosor

Un Calcio Alle Frodi vuole rendere omaggio alla figura di **Gigi Riva**. Grande uomo e campione sia dentro che fuori dal campo, ha lasciato una significativa eredità a tutte le generazioni, **trasmettendo valori** universali come **l'onestà, l'integrità morale e la dedizione alla trasparenza e correttezza**.

Così come Rombo di Tuono, che con il suo sinistro infallibile bucava le reti avversarie sui campi da calcio, i lettori di questo vademecum avranno uno strumento in più per segnare un gol decisivo contro la criminalità informatica.

PREFAZIONE

Polizia di Stato

Recentemente si sta assistendo a un costante aumento dei reati finanziari commessi online. Le tecniche ideate dai truffatori sono sempre più sofisticate e variegate: si fingono operatori di banca, familiari in difficoltà, agenti di polizia, al fine di trarre in inganno gli utenti, carpire i loro dati personali ed effettuare operazioni bancarie a loro insaputa. In molti casi sono così convincenti da indurre la vittima a eseguire personalmente le operazioni finanziarie in frode.

La prevenzione e il contrasto di tale fenomeno criminoso passano innanzitutto dalle attività di monitoraggio della rete e investigative svolte dalla Polizia Postale e altrettanto importante è una costante e dedicata opera di sensibilizzazione degli utenti ed è in tale direzione che si muove il progetto sociale "Un Calcio alle Frodi".

La Polizia Postale, infatti, pone massima attenzione all'informazione del cittadino sui rischi presenti nella rete, fornendogli idonei strumenti necessari per riconoscere le frodi informatiche ed evitarne le conseguenze.

Luigi Rinella - Direttore Centrale per la Polizia Scientifica e la Sicurezza Cibernetica

Posteitaliane

Il contrasto delle frodi informatiche rappresenta una priorità per Poste Italiane, per questo l'Azienda, in funzione dell'evoluzione nel tempo delle modalità e dei sistemi di pagamento, ha adeguato i suoi sistemi di difesa a tutela dei Cittadini e dei propri servizi finanziari, fino a dotarsi, dall'inizio del 2023, di un Centro Prevenzioni Frodi, uno tra più avanzati in Europa.

La consapevolezza, però, da parte dei Cittadini che ogni giorno eseguono operazioni finanziarie attraverso i dispositivi elettronici, di quali aspetti debbano essere oggetto di particolare attenzione per evitare di essere frodati, rappresenta un elemento altrettanto fondamentale per limitarne l'impatto sulla società.

Questa iniziativa si inquadra in un più ampio progetto da parte di Poste Italiane caratterizzato da continue azioni di sensibilizzazione, della propria clientela e non, circa i principali crimini informatici e le modalità di attacco dei cybercriminali che coinvolge da diversi anni anche tutti i canali proprietari.

Raffaele Panico - Responsabile Risk e Compliance di Gruppo

CAGLIARI

Essere la prima Società sportiva a sposare un progetto di questo tipo rappresenta un orgoglio e una doverosa assunzione di responsabilità. Il Cagliari Calcio vuole fare la sua parte insieme agli altri attori coinvolti in una campagna di sensibilizzazione e lotta contro criticità che riguardano la vita di tutti i cittadini.

Tommaso Edoardo Giulini - Presidente

UN CALCIO ALLE FRODI.

È un progetto sociale nato dalla collaborazione tra la Polizia di Stato, attraverso la Polizia Postale e per la Sicurezza Cibernetica, Poste Italiane S.p.A., il Cagliari Calcio volto a sensibilizzare i cittadini in materia di crimini informatici, spiegando le attuali e più diffuse tipologie di truffe e frodi informatiche e le modalità di attacco dei cybercriminali.

Prima di iniziare ad affrontare passaggio dopo passaggio le fenomenologie fraudolente, aiutandovi così a dribblarle, è necessario fare un piccolo passo indietro, conoscere l'avversario e comprendere quali sono le sue tecniche di attacco.

D'altra parte, lo stesso avversario/cybercriminale studia le proprie vittime sulla base di tutte le informazioni esposte agli occhi di tutti e non solo.

Al riguardo, si parla di cybercriminale come ingegnere sociale.

Che cosa si intende esattamente per ingegneria sociale, il cosidetto social engineering?

L'ingegneria sociale è la capacità di persuadere le persone affinché compiano azioni o rivelino informazioni utili all'ingegnere sociale.
La manipolazione, basata da un precedente studio del comportamento e profilo della vittima, avviene tramite l'inganno, facendo leva sui sentimenti della **paura**, **ansia**, **fretta**, **ingenuità**, **avidità**, **curiosità**, **rabbia** etc.. L'attaccante riesce così a carpire informazioni personali dalla vittima, la quale normalmente non rivelerebbe ad un estraneo, ottenendo ad esempio l'accesso non autorizzato a sistemi informatici (come l'home banking) o riuscendo ad estorcere denaro o ancora a rubarne l'identità.

Il social engineering viene attuato secondo uno schema circolare:

1. RICERCA DI INFORMAZIONI

su fonti aperte, specialmente sulle piattaforme social;

2. SVILUPPO DI UN RAPPORTO DI FIDUCIA

fingendosi un'altra persona (ad esempio attraverso la compromissione dell'account social o di messaggistica di un amico o familiare della vittima) o citando persone conosciute alla vittima;

3. SFRUTTAMENTO DEL RAPPORTO DI FIDUCIA

domandando informazioni o azioni alla vittima oppure convincendo la vittima a chiedere aiuto all'attaccante/interlocutore;

4. UTILIZZO DELLE INFORMAZIONI/ATTACCO

Se l'informazione ottenuta è solo un passo verso la meta finale, l'attaccante ritorna all'inizio del ciclo fino a quando non ha ottenuto quel che cerca.

Giova sottolineare come le piattaforme social offrano ai cybercriminali un vasto bacino di dati personali. Gli utenti condividono spesso dettagli intimi della loro vita, come interessi, relazioni, luoghi visitati, eventi importanti e altro ancora: informazioni che costituiscono un tesoro per gli attaccanti (frodatori) in quanto gli permettono di personalizzare e rendere più convincenti i loro attacchi, aumentando la probabilità che la vittima cada nella trappola.

"Le piattaforme social non sono di per sé pericolose ma possono diventarlo se l'utente rivela troppo di sé"

Tecniche di attacco del social engineering: Phishing, Smishing e Vishing

Pensiamo al cybercriminale come un avversario di calcio, il social engineering (ingegneria sociale) è lo schema di gioco adottato che prevede le modalità di azione, quali il **Phishing**, **Smishing** e **Vishing**.

1. Che cos'è il Phishing?

Il phishing consiste in una falsa comunicazione trasmessa mediante posta elettronica a una moltitudine di persone, alcune delle quali diventeranno delle vere e proprie vittime in quanto verranno indotte a scaricare un allegato che potrebbe contenere un malware o a cliccare un link che reindirizza ad un sito clone della propria home banking o di una piattaforma social, al fine di carpirne le credenziali di accesso.
Questi siti clone riproducono fedelmente l'architettura del sito originale. In realtà, se si controlla bene, il dominio risulterà difforme da quello originale presentando una piccola modifica; al riguardo, si parla di typosquatting, tecnica basata sull'errore comune di battitura.

QUANDO DIVENTA SPEAR PHISHING?

Quando le false e-mail non sono più rivolte ad una moltitudine di persone ma sono messaggi mirati ingannevoli indirizzati ad un individuo o organizzazione specifica. Sono, quindi, appositamente forgiate in base alle caratteristiche della vittima, dopo aver raccolto informazioni specifiche su di lei (vedi la fase 1 del social engineering: Ricerca di Informazioni), inserendo così nel corpo del testo dell'e-mail riferimenti correlati a quella persona relativi alla vita privata o alla sua professione per rendere il messaggio meno asettico e formale e, quindi, più credibile.

"La personalizzazione del messaggio aumenta sensibilmente il tasso di successo degli attacchi"

2. Che cos'è lo Smishing?

Variante del phishing, in cui il falso messaggio "trappola" viene trasmesso non più tramite e-mail ma tramite sms (ordinario o su app di messaggistica). Al fine di rendere credibile il messaggio, l'avversario fa apparire come mittente un numero a piacimento o un nome preciso (es. di un istituto di credito o ente pubblico) per trarre in inganno la vittima. Ad esempio, i messaggi provenienti dalle nostre banche presentano come mittente il nome dell'istituto di credito. In questo caso, il messaggio trappola, presentando come mittente il nome dell'istituto di credito, andrà a confondersi con i reali messaggi ricevuti dalla vittima, in quanto quello falso verrà inserito automaticamente dal dispositivo all'interno dello stesso archivio che riporta il nome della nostra banca.

3. Che cos'è il Vishing?

Anch'esso è una variante del phishing e consiste in una chiamata di un soggetto che finge di essere un'altra persona al fine di ottenere informazioni personali ovvero estorcere denaro. Il numero chiamante o il nome che compare sullo smartphone è scelto ad hoc dal cybercriminale, il quale sfrutta la tecnologia VoIP (voce tramite protocollo Internet) e altri servizi internet, che permettono di cambiare a piacimento il mittente. Ad esempio, si può far comparire il numero o il nome del proprio istituto di credito o addirittura di un ufficio di polizia o ancora di un familiare o persona conosciuta.
Come abbiamo visto, i numeri e i nomi del mittente delle chiamate e dei messaggi vengono camuffati, o per meglio dire falsificati, mediante la tecnica fraudolenta SPOOFING, che costituisce la base di tanti attacchi informatici.

Tale tecnica, permettendo all'avversario di impersonare nelle comunicazioni online un'altra persona a suo piacimento, aumenta sensibilmente la potenzialità di convincimento della vittima (vedi la fase 2 del social engineering: Sviluppo del rapporto di fiducia).

3 - 0 per i cybercriminali. Come ribaltare la partita?

Conoscere le tipologie di truffe e frodi informatiche, riconoscere i segnali di allarme, seguire i consigli forniti e diffonderli con il passa parola.

Si inizia!

FAMILY EMERGENCY SCAM

Si tratta della truffa del familiare in difficoltà che ha lo scopo di estorcere del denaro alle vittime facendo leva sui sentimenti della **paura**, **ansia** e **preoccupazione**.
Il cybercriminale è un vero ingegnere sociale: chi non aiuterebbe suo figlio o suo nipote qualora si trovasse in difficoltà?
Attualmente, la truffa più diffusa è quella del **cellulare rotto**: *"mamma/papà ho rotto il cellulare"*

Come Funziona

Sms: Tutto parte con un SMS o messaggio WhatsApp apparentemente proveniente da un familiare in difficoltà, di solito il figlio/a, il quale rappresenta di aver cambiato numero perché gli si è rotto il cellulare. Spesso il messaggio viene inoltrato in orari in cui la vittima potrebbe essere ancora assonnata o stanca.
L'apertura può avere varie forme e punta direttamente sull'indurre il destinatario a dare per scontato chi sia il mittente, solitamente figli:

- *"Mamma questo è il mio nuovo numero salvalo e scrivimi su WhatsApp +39***"*
- *"Papà ho perso il telefono, questo è il mio nuovo numero, puoi salvarlo e scrivermi al più presto su whatsaap? https://wa.me/39***"*
- *"Ciao mamma, il mio cellulare è rotto. Puoi scrivermi su WhatsApp al numero +39***"*
- *"Papà…ho lasciato cadere il telefono in acqua e ora non funziona. Ho un nuovo numero. Potete mandarmi un messaggio su whatssapp? 39*** questo numero."*

L'apparente figlio comunica l'impossibilità di un contatto a voce tramite chiamata per una ragione più o meno definita, ad esempio una limitazione delle funzionalità dello stesso o perché impegnato o ancora perché sotto stress per aver perso tutti i numeri. In questo modo, si spinge la vittima a non chiamare il nuovo numero appena indicato o il vecchio (in realtà unico ed esistente) numero del reale figlio per evitare che scopra l'inganno.

Richiesta di denaro: Dopo un primo e breve scambio di messaggi su WhatsApp con l'apparente figlio, quest'ultimo richiede urgentemente e nel tempo più breve possibile l'invio di denaro su un mezzo di pagamento indicato, di solito bonifico istantaneo o ricarica presso una tabaccheria, ovvero la dazione di credenziali di accesso al conto corrente della vittima. Il motivo è l'acquisto di un nuovo telefono per ristabilire le comunicazioni o anche per rimuovere un determinato pericolo incombente, ad esempio pagare una multa, fattura od altro pagamento a scadenza, adducendo l'impossibilità di utilizzo del proprio conto per via di un blocco temporaneo o per aver speso tutti i soldi nell'acquisto di un nuovo telefonino.
Si nota come la richiesta di denaro sia accompagnata da un aumento del senso di urgenza in cui si comunica un'esigenza ulteriore che, se ignorata, potrebbe comportare dei disagi sempre più gravi e irreparabili per il familiare che richiede aiuto.
Lo schema di attacco, impostato sull'urgenza e la fretta, induce così la vittima a pagare sull'onda della preoccupazione, **ansia** e **paura** per il proprio familiare, ancor più se vive all'estero o in viaggio.

Come difendersi

- Cercare immediatamente di contattare con ogni altro canale il proprio familiare o, qualora non risponda, una persona a lui vicina. Non fermarsi alla sola chiamata in quanto, nelle ipotesi più sofisticate, ci potrebbe essere l'uso della deepfake audio*, ossia l'utilizzo della voce del familiare riprodotta fedelmente mediante l'utilizzo dell'intelligenza artificiale.
- Non rispondere al messaggio, cancella la conversazione e, se lo hai salvato, elimina il numero dalla rubrica.

* Sono audio che riproducono la voce (inclusa la cadenza, timbro e tono) di una determinata persona, grazie ad un campione audio reale della sua voce anche di pochi secondi.

Ricorda di prestare attenzione sulle informazioni che vengono pubblicate online in quanto potrebbero essere usate per aumentare l'efficacia di questa tipologia di attacco, ad esempio l'indicazione che il proprio figlio/a sia all'estero per ragioni di lavoro o viaggio ed ancora dati personali della propria vita privata che, se sfruttati, renderebbero ancora più credibile il fatto che si stia parlando realmente con il proprio familiare.

FAKE TRADING ONLINE

Si tratta della truffa del finto broker, il quale spacciandosi per un intermediario finanziario accreditato presso le più importanti agenzie di trading, telefonicamente o on-line, convince le vittime a investire ingenti somme di denaro promettendo rendite elevate. Dopo aver ricevuto il denaro, il criminale, per convincere la vittima a investire sempre di più, di solito permette il ritiro di piccole somme. Nel momento in cui la vittima decide di monetizzare i guadagni derivanti dall'investimento, i falsi intermediari fanno perdere le loro tracce impossessandosi dell'intero capitale investito, prosciugando i risparmi di una vita delle vittime.

Come Funziona

Primo contatto con la vittima: Sul web e soprattutto sui social medi avengono pubblicate dai cybercriminali false pagine di trading e pubblicati falsi annunci pubblicitari su come guadagnare facilmente tanti soldi mediante degli investimenti. Per rendere il messaggio più convincente vengono utilizzate anche immagini o video di personaggi famosi (ignari della truffa) che sponsorizzano l'investimento mediante dei deepfake video** creati con l'intelligenza artificiale. La vittima così viene spinta a chiedere maggiori informazioni compilando un form*** in cui fornisce il suo numero di telefono o mettendo il "mi piace" nel post. Da qui, le vittime vengono contattate da un sedicente esperto di trading (uomo o donna) da un numero, di solito con prefisso estero +44. A partire da questo momento le conversazioni avvengono telefonicamente e su WhatsApp.

Primo investimento: Il finto broker propone inizialmente di investire una piccola somma, usualmente 200/250 €, di solito da versare mediante bonifico a favore di Iban esteri. Successivamente, la vittima viene convinta ad iscriversi ad una

** Sono video falsi ma altamente realistici che hanno lo scopo di far credere agli utenti che le parole dette o le immagini siano reali.

*** Modulo online da compilare con i propri dati personali.

falsa piattaforma di trading per seguire i suoi investimenti. Oltre a questa, molto spesso vengono convinti ad aprire uno o più conti su reali piattaforme di trading e scaricare l'applicativo AnyDesk o TeamViewer che permette un controllo da remoto del dispositivo sul quale viene installato, permettendo al broker di effettuare le operazioni indipendentemente dall'ausilio della vittima. Vengono, inoltre, convinte ad inviare i propri documenti d'identità.

Richieste ulteriori di denaro: La vittima vede sulla falsa piattaforma di trading (siti fake creati per simulare i guadagni degli investimenti) gli eccellenti risultati dell'investimento. Viene, quindi, indotta ad investire sempre più somme di denaro per aumentare i profitti. In alcuni casi, la fiducia viene carpita a seguito di piccoli prelievi di denaro che vengono fatti eseguire dalla vittima, la quale si convince della genuinità dell'investimento. Quando però viene richiesto di prelevare l'intero o gran parte del capitale investito maggiorato dai guadagni, il finto trader (non è quasi mai uno ma si succedono nel tempo) adduce le più svariate argomentazioni, ad esempio la necessità di pagare una tassa per sbloccare i soldi, cercando di ottenere il massimo possibile dalla vittima.

Acquisizione e fuga: I truffatori dopo aver ottenuto quanta più liquidità dal malcapitato, portandolo anche ad indebitarsi con amici/parenti o società di finanziamento, si dileguano, così come sparisce la finta piattaforma di trading alla quale la vittima accedeva per verificare i fantomatici guadagni. La vittima capisce così di essere cascata nella truffa.

Doppia truffa: Molto spesso la vittima di trading online viene successivamente contattata, anche dopo anni, da fittizie società di recupero crediti che la convince a pagare il servizio offerto al fine di recuperare l'intero capitale perso in precedenza.

"Pacco, doppio pacco e contropaccotto": Quando la vittima si accorge che anche questa è una truffa in quanto non recupera alcunché ma perde altre somme di denaro, viene contattata da un sedicente avvocato che promette di occuparsi legalmente delle truffe subite. Non c'è nemmeno bisogno di ripeterlo ma si tratta anche in questo caso di una truffa.

Combo (la truffa a incastro): In alcuni casi le vittime di trading online non vengono agganciate con le pubblicità di investimento, come abbiamo visto prima, ma da una "nuova conoscenza" avvenuta sui social, con la quale crede di aver iniziato una relazione sentimentale. La persona, ormai diventata di fiducia, tende a chiedere per diversi motivi delle somme di denaro, fino poi a proporgli anche degli investimenti di criptovalute. In questo caso, abbiamo la truffa romantica (cd. Romance Scam) e la truffa del falso trading online.

Come difendersi

- Verificare che il soggetto che propone il trading online sia autorizzato ad operare come intermediario finanziario consultando i siti della Consob e della Banca d'Italia.
- Consultare le sezioni "Occhio alle truffe" della Consob e "Warning and publications for investors" dell'ESMA (la CONSOB europea) sul sito www.esma.europa.eu al fine di verificare se, nei confronti del trader o della piattaforma di trading sponsorizzata, siano presenti degli avvisi di truffa (warning).
- Controllare, attraverso i motori di ricerca sul web, le recensioni riferite alle società di trading sponsorizzata dal broker.
- Non investire ulteriori somme di denaro per sbloccare i rimborsi di quanto già investito.
- Non fidarsi di fantomatiche società di recupero crediti o avvocati che telefonicamente o per e-mail promettono di risolvere il problema.

Ricorda di diffidare dei broker che offrono un rendimento fuori mercato prospettando un ritorno economico in percentuali di elevata entità. Inoltre, non inviare i propri documenti d'identità in quanto vengono utilizzati per aprire nuovi conti bancari o sulle piattaforme di trading per effettuare il riciclaggio di denaro.

E-COMMERCE SCAM

Si tratta della truffa del commercio elettronico che si attua mediante siti fasulli di negozi online oppure annunci di vendita trappola pubblicati sulle più note piattaforme di e-commerce, quali Subito, eBay, o sui social media, come la pagina Marketplace di Facebook. Tali truffe si concretizzano nel danno patrimoniale subito dall'acquirente o dal venditore.

Come Funziona

Vittima l'acquirente: L'utente interessato al bene messo in vendita effettua il pagamento o direttamente sul sito ovvero mediante ricarica o bonifico. Capisce di essere caduta in una vera e propria truffa quando il bene acquistato non arriva o viene consegnato un prodotto difforme da quello acquistato. Questo avviene perché il sito sul quale si è effettuato l'acquisto è fasullo oppure perché la contrattazione e il pagamento è avvenuto fuori dalle piattaforme e-commerce che prevedono un'alta protezione negli acquisti.

Ad esempio, Subito (con l'opzione "TuttoSubito"), eBay e Vinted prevedono che la contrattazione avvenga mediante la messagistica interna della piattaforma (in cui si può non rendere visibile il numero di telefono e l'indirizzo e-mail). Il pagamento avviene sulla piattaforma, associando il proprio rapporto bancario.

Nello specifico, la piattaforma avvisa il venditore che il pagamento è stato effettuato e invia l'etichetta di spedizione. Se non arriva il pacco o arriva un oggetto difforme alla descrizione si segnala alla piattaforma che restituisce i soldi all'acquirente, non trasferendoli al venditore.

Dal momento che i cybercriminali hanno ben capito che gli utenti preferiscono salvaguardare le proprie tasche adottando la procedura appena descritta, aggirano questa protezione.

Come è possibile? Dopo che viene effettuato il pagamento con la procedura interna della piattaforma, i cybercriminali inviano un messaggio di prenotazione della consegna del pacco con all'interno un link. Cliccando il link si apre una finta pagina di login (accesso) che produce fedelmente quella della piattaforma utilizzata per la vendita. L'ignaro acquirente inserisce le credenziali di accesso alla piattaforma, venendo così carpite e utilizzate dal cybercriminale per accedere sull'account personale della vittima e confermare la ricezione del pacco.

Vittima il venditore: In questo caso, la truffa si concretizza nel far credere al venditore di ricevere il pagamento del bene messo in vendita con un vaglia postale o mediante accreditamento del denaro sulla sua carta. In quest'ultimo caso ci sono due modalità utilizzate dal cybercriminale.

Modalità A: Il venditore viene indotto a presentarsi presso uno sportello ATM al fine di ricevere il denaro pattuito. In tale frangente, la vittima, seguendo le indicazioni dettate per telefono dal finto acquirente, effettua inconsapevolmente delle ricariche alle carte in uso ai criminali. Il numero delle carte da ricaricare viene anch'esso indicato telefonicamente al fine di evitare che la vittima se lo annoti. Il denaro inviato viene immediatamente prelevato. **Truffa dell'ATM**.

Modalità B: Il venditore riceve sulla propria utenza telefonica, comunicata in precedenza, dal finto acquirente un QR Code che, a suo dire, permette di ricevere nell'immediato l'accredito sul su conto della somma di denaro pattuita. In realtà, la vittima, scannerizzando il codice a barre con il suo dispositivo, viene rimandata ad una pagina di pagamento nella quale inseriti i propri dati della carta, anziché ricevere il denaro, effettua lei stessa il bonifico a favore del finto acquirente. **Truffa del QR Code**.

Come difendersi

In caso di acquisti su siti diversi dalle piattaforme e-commerce:

- Verificare se il sito è sicuro controllando l'URL completo in alto nella barra degli indirizzi del browser. Se è un sito noto controllare che sia scritto bene, in quanto molto spesso vengono creati domini molto simili per far cadere in errore il potenziale acquirente (ricorda la tecnica del typosquatting).
- Accertarsi che il sito presenti il protocollo https che indica una connessione sicura, in quanto i dati in transito da e verso l'e-commerce sono protetti in quanto criptati e non condivisi.
- Leggere i "feedback" (recensioni) pubblicati dagli altri utenti sul sito che lo mette in vendita o con una ricerca sul web.
- Scegliere sempre metodi di pagamento tracciabili. Preferibilmente, utilizzare carte ricaricabili utilizzate solo per acquisti online e che vengono caricate in occasione di un acquisto; diffidare da metodi di pagamento non tracciabili, quali trasferimenti tramite Western Union.

In caso di acquisti sulle piattaforme e-commerce:

- Effettuare la contrattazione e il pagamento all'interno della piattaforma.
- Dubitare di chi chiede di esser contattato al di fuori della piattaforma mediante e-mail e/o sms, con la scusa di far risparmiare sulle commissioni, e di chi ha troppa fretta di concludere l'affare.
- Non cliccare su link o non scannerizzare QR Code inviati tramite messaggio perché potrebbero rimandare a delle pagine fake per carpire i propri dati personali e/o denaro.
- Non recarsi negli sportelli ATM per ricevere il pagamento perché in realtà si viene indotti ad effettuare delle transazioni in uscita di denaro.

Ricorda di diffidare dalle offerte che si presentano troppo conveniente rispetto all'effettivo prezzo di mercato del prodotto.

BANK SCAM

Questo fenomeno criminale consiste in un messaggio apparentemente proveniente dal proprio istituto di credito (Smishing) seguito da una chiamata (Vishing) di un sedicente operatore di quell'istituto, il quale convince la vittima, dietro la scusa di accessi abusivi sul suo conto, a fornire i codici che gli arrivano sul dispositivo (OTP) o a spostare il denaro dal suo conto ad un altro per evitare la perdita dello stesso. Per rendere ancora più credibile quanto raccontato, i cybercriminali effettuano in aggiunta una chiamata da parte di un finto operatore della polizia facendo comparire sul dispositivo della vittima il reale numero in uso agli Uffici di Polizia.

Come Funziona

Smishing dell'istituto di credito: Sull'utenza della vittima arriva un sms apparentemente proveniente dal proprio istituto di credito che viene inserito all'interno della box di messaggi reali ricevuti dalla propria banca. Nel messaggio viene comunicato il tentativo di accesso abusivo sul conto della vittima e/o pagamenti effettuati da dover disconoscere cliccando un link.

Ecco alcuni esempi di messaggi:

- *"Avviso la sua app *** risulta associata ad un nuovo dispositivo da Lugano se non sei tu bloccalo al link……."*
- *"ATTENZIONE! Un dispositivo non autorizzato risulta connesso al suo conto online se disconosce tale accesso clicca il modulo correllato https://***"*
- *"Gentile cliente la sua carta e in fase di blocco per evitare la sospensione aggiorna i dati al link https://***"*

La vittima è già in un forte stato di **agitazione** e **paura** ma non basta: si aggiungono una o più chiamate da diversi interlocutori per rendere il tutto più credibile e dare indicazioni alla vittima su cosa fare. Vediamo insieme chi affermano di essere.

Vishing del finto operatore: Subito dopo la ricezione del messaggio, la vittima riceve una chiamata da un numero apparentemente in uso al proprio istituto di credito. L'interlocutore si presenta come operatore finanziario e gli conferma quanto comunicato per messaggio. Il cybercriminale, quindi, può agire in due modi.

Modalità A: L'interlocutore convince la vittima ad accedere al link inviato per messaggio che rimanda ad una pagina fake di login del suo conto, al fine di carpirne le credenziali di accesso. Una volta ottenuto l'accesso alla sua home banking, il cybercriminale effettua delle disposizioni di pagamento per le quali, oltre

una certa soglia, gli servirà il codice che viene inviato sul dispositivo della vittima (codice OTP). Così convince la vittima a fornirgli uno o più codici a seconda di quante disposizioni di pagamento vengono effettuate. Il conto viene prosciugato.

Modalità B: L'interlocutore convince la vittima a recarsi in filiale, non parlare con nessuno di tale pericolo sul suo conto in quanto altre persone potrebbero essere coinvolte e spostare tutto il denaro presente sul suo conto su un altro intestato ad altra persona.

Doppio Vishing del finto operatore di polizia: Di solito, viene ricevuta un'ulteriore chiamata da un numero realmente esistente e assegnato agli Uffici di Polizia. L'interlocutore si finge un poliziotto e conferma quanto detto dal finto operatore dell'istituto di credito, avvisandolo di non dire nulla a nessuno in quanto c'è un'attività d'indagine in corso.

L'arrivo presso l'istituto di credito: La vittima viene, quindi, richiamata dal finto operatore che lo segue passo per passo telefonicamente al fine di essere certo che non riveli nulla al reale personale dell'istituto di credito. Inoltre, le detta il numero della carta sulla quale effettuare il bonifico dell'intero capitale presente sul suo conto.

Come è possibile che vengano utilizzati i numeri assegnati agli istituti di credito e agli Uffici di Polizia? L'abbiamo visto nelle pagine iniziali: il cybercriminale adotta la tecnica dello spoofing che permette di manipolare il nominativo o il numero del mittente sia di messaggi che di chiamate utilizzando dei servizi offerti in rete. Oltretutto, sfrutta il sentimento di **paura** e **stato di agitazione** della vittima come ben sa fare un ingegnere sociale.

Come difendersi

- Non fornire mai i propri dati personali e bancari (numero di carta, pin, CVV e codici OTP).
- Chiamare subito il proprio istituto di credito o chiamare l'ufficio di polizia da cui si riceve la chiamata.
- Non accedere sulla propria home banking mediante link, QR Code inviati tramite SMS o e-mail ma solo dal sito o app ufficiale.

Ricorda nessun istituto di credito e nessuna forza di polizia chiede dati bancari né chiede di spostare il denaro su un altro conto.

MAN IN THE MAIL

Si tratta di una frode informatica in cui il cybercriminale accede alle comunicazioni di posta elettronica tra due persone, grazie alla compromissione della casella e-mail di una delle due parti. Ciò viene fatto allo scopo di individuare eventuali messaggi che contengono richieste di pagamento e modificare le coordinate bancarie sul quale effettuare il bonifico.

Come Funziona

Compromissione della casella e-mail: Il cybercriminale accede abusivamente sulla casella e-mail della vittima al fine di monitorare l'arrivo o l'invio di messaggi relativi a richieste di pagamento. Dunque, verifica la presenza di comunicazioni tra creditore e debitore.

Sostituzione delle coordinate bancarie: Una volta trovata l'e-mail in cui vengono indicate le coordinate bancarie sulla quale effettuare il bonifico, il cybercriminale le cambia con altre al fine di dirottare il denaro su conti di cui ha la disponibilità. Può farlo in due modi.

Modalità A: Modifica l'e-mail originaria, ad esempio scollegando l'allegato in cui sono inserite le coordinate bancarie per inserire un nuovo allegato creato alla stregua di quello originale, inserendo un diverso Iban.

Modalità B (più diffuso): Cancella l'e-mail originale e ne invia una nuova con diverso Iban da un altro indirizzo e-mail molto simile a quello del mittente/creditore al fine di trarre in inganno il destinatario. Viene utilizzata la tecnica del typosquatting, ossia la creazione di un dominio e-mail molto simile a quello originale che presenta dei piccoli errori di battitura, tanto da sembrare a prima vista uguale rispetto al dominio originale (ad esempio viene tolta o aggiunta una lettera).

Pagamento: Il debitore effettua il bonifico a favore delle nuove coordinate bancarie indicate e capirà di essere caduta vittima della frode solo quando il creditore solleciterà il pagamento a lui dovuto.

Come difendersi

- Cambiare sovente le password della casella e-mail e verificare se le regole predefinite di ricezione delle mail sono state cambiate;
- Controllare con attenzione il mittente del messaggio verificando se vi siano piccoli errori di battitura rispetto all'indirizzo originale, con cui si ha avuto contatti fin dall'inizio.
- Proteggere la rete WIFI utilizzando password efficaci.
- Aggiornare sempre il sistema operativo ed installare un anti-malware;
- Sensibilizzare ed aggiornare il personale preposto al pagamento delle transazioni commerciali informandolo riguardo tali fenomeni di "hacking".

Ricorda prima di effettuare un pagamento è sempre bene chiamare il soggetto a favore del quale deve essere effettuato, sui contatti già in proprio possesso, per verificare se le coordinate bancarie siano corrette, soprattutto se si notano delle discrepanze relative alle modalità di pagamento, ad esempio il cambio dell'Iban.

JOB SCAM

Si tratta di false offerte di lavoro veicolate mediante sms, e-mail, canali Telegram o ancora pubblicizzate sui social media. Tali offerte consistono in attività part-time da svolgere comodamente da casa; ad esempio, nella pubblicazione di recensioni di prodotti in vendita, in offerte di impieghi presso università e alberghi all'estero, in ricompense in denaro per mettere "like" a video pubblicati online. Insomma, ciò che viene promesso sono pagamenti anticipati, orari ridotti, lavoro da casa e una buona retribuzione complessiva.

Come Funziona

Primo contatto e proposta: La vittima viene contattata tramite messaggio sul suo profilo social (FB, IG, TikTok) o sulla sua utenza telefonica (sms, WhatsApp, Telegram) da un utente sconosciuto, prospettandole un'allettante proposta di lavoro che le permetta di guadagnare elevate cifre dietro uno sforzo minimo.
I messaggi più diffusi al momento sono quelli apparentemente ricevuti da Booking.com, come il seguente.

- *“Abbiamo bisogno di qualcuno che valuti le prenotazioni alberghiere. Paghiamo tra i 200 e i 1.000 euro. Tutto quello che devi fare è valutare o mettere “Mi piace” all’hotel su *** (un falso link a Booking.com)”*

Richiesta apertura conto: Il finto reclutatore dopo aver dettato le istruzioni iniziali circa i compiti assegnati, comunica che per ricevere la retribuzione è necessaria l’apertura di un conto bancario o su una piattaforma di criptovalute indicando alla vittima anche un link della finta piattaforma o altro sito in cui visualizzare le rendite. Per ogni valutazione, prenotazione o mi piace di solito si richiede una somma di denaro che poi, secondo quanto detto dal reclutatore, viene riaccreditata con una maggiorazione sul conto del dipendente, consistente nello stipendio.

Loop (Escalation incalzante): Questo meccanismo, forgiato sulla base delle più disparate motivazioni, genera un loop che porta a richieste sempre più elevate di denaro per la vittima, la quale viene spinta ad investire sempre più per ottenere maggiori profitti. In realtà, la vittima perderà tutti i soldi investiti.

Segnali di allarme

- L’annuncio o la proposta di lavoro non contiene informazioni chiare e complete.
- Promessa di facili guadagni e retribuzioni elevate.
- Richieste di denaro anticipate per l’acquisto di materiale, per presentare la domanda, per partecipare a un corso di formazione indispensabile per ottenere il lavoro o come anticipo dell’assicurazione sanitaria e pensionistica.
- Assenza di un contratto scritto da firmare. In alcuni casi viene anche inviata una bozza di contratto con contestuale richiesta di documenti d’identità, codice fiscale e iban con la falsa promessa di un successivo accredito di somme elevatissime.

Come difendersi

- Non rispondere, bloccare i messaggi ricevuti da mittenti sconosciuti e non aprire link che possano compromettere il dispositivo.
- Diffidare delle offerte pervenute tramite l’invio di mail o profili social e non precedute da alcuna richiesta.
- Diffidare di richieste in denaro finalizzate alla copertura di ipotetiche “spese”, per sbloccare il denaro guadagnato o ancora per concludere il contratto di lavoro.

- Rifiutare richieste di apertura di conti correnti per “facilitare” trasferimenti di denaro.
- Rifiutare la richiesta di reclutamento di altri soggetti cui rivolgere la medesima offerta di lavoro mediante lo schema “piramidale”.
- Non inviare i documenti d’identità in quanto potrebbero essere utilizzati con ogni probabilità per aprire ulteriori conti a nome delle ignare vittime per commettere reati.

Ricorda diffidare delle offerte di lavoro ricevute, non richieste, che promettono facili ed elevati guadagni al minimo sforzo. Tutti vorrebbero che esistessero ma è una grande **truffa**.

CONCLUSIONI

Se sei arrivato fino a qui, significa che ora sei più consapevole dei pericoli che si annidano in rete e più preparato ad affrontare diverse sfide.

Il viaggio che hai intrapreso leggendo **Un Calcio alle Frodi** è stato come preparare le strategie per affrontare ogni singola partita di un intero campionato. Così come nella realtà calcistica ci sono avversari che cambiano schema di gioco a seconda di chi sfidano, anche nel mondo delle frodi i cybercriminali possono cambiare tattica. Per questo occorre farsi trovare sempre pronti e non abbassare mai la guardia.

Ora hai uno strumento in più per affrontare il campionato con maggiore consapevolezza e determinazione, come un vero cyberallenatore.
Se vuoi sapere di più seguici sui canali dedicati con lo **Sportello per la Sicurezza degli utenti del web** della **Polizia di Stato**:

https://www.commissariatodips.it/

e con **i consigli su come difendersi dalla truffe di Poste Italiane**:

https://www.poste.it/come-difendersi-dalle-truffe.html

FAQ

Ecco a voi le FAQ, strumenti mirati che offrono un'opportunità strategica di difesa dai cybercriminali. Immaginate di avere l'opportunità di calciare un calcio di rigore: pronti per segnare goal?

- **Ho ricevuto un'e-mail di phishing, cosa devo fare?**

  Non clicchi su eventuali link presenti e non scarichi eventuali allegati in quanto potrebbero contenere dei malware. Effettui una scansione con un antivirus aggiornato del suo dispositivo.

- **Mi hanno contattato per il ritiro del premio da me vinto ad una lotteria straniera. Posso ritirarlo?**

  Queste e-mail rientrano nello schema delle truffe nigeriane. Per ritirare il premio, verrà richiesto preliminarmente il pagamento di spese elevate che costituiscono la finalità della truffa. Si riconoscono con facilità, poiché il biglietto che viene segnalato come vincente non è stato acquistato dall'utente.

- **Intendo rispondere alle e-mail di spam, che ne pensate?**

  L' indirizzo indicato nel campo "From" non corrisponde quasi mai al reale indirizzo di posta elettronica dello spammer. Consigliamo, quindi, di non rispondere a tali messaggi poiché, rispondendo, non farebbe che confermare allo spammer che l'indirizzo è attivo ed utilizzato.

- **Ho ricevuto un messaggio da una società di trasporti/consegne in cui mi si diceva che avrei dovuto prenotare l'appuntamento per la consegna. Dovendo ricevere un pacco, ho cliccato il link contenuto nel messaggio, ho fatto bene?**

  È un tentativo di phishing/smishing in cui viene inserito un link fraudolento che porta ad un sito clone in cui si devono inserire i propri dati personali e bancari. Se ha inserito questi dati, le consigliamo di informare la sua banca per evitare delle transazioni non autorizzate sul suo conto.
  Quando è in attesa di una consegna, le suggeriamo di verificare lo stato della spedizione esclusivamente attraverso il sito ufficiale su cui hai effettuato l'ordine e, nel caso di dubbi, la invitiamo a contattare il servizio clienti del venditore. Si raccomanda, in ogni caso, di non divulgare mai i propri dati personali e bancari.

- **Ho ricevuto per e-mail una lettera di accusa di reati contro i minori e successiva richiesta di denaro per archiviare il procedimento instaurato contro di me, cosa devo fare?**

  Si tratta della campagna di phishing riguardante false convocazioni giudiziari a firma del Capo della Polizia – Direttore Generale della Pubblica Sicurezza. Lo scopo è quello di causare nel destinatario uno stato di agitazione e di indurlo a ricontattare il truffatore entro 72 ore, inviando le proprie giustificazioni. Successivamente, viene chiesto il pagamento di una somma di denaro per evitare le condanna.
  Deve diffidare da simili messaggi in quanto nessuna forza di Polizia contatterebbe mai direttamente i cittadini, attraverso e-mail o messaggi, per chiedere loro dati personali o pagamenti in denaro, con la minaccia procedimenti penali a loro carico.

- **Mi hanno hackerato il profilo social, come posso recuperarlo?**

  Se riesce ad accedere ancora sul suo profilo procedere al cambio della password e all'attivazione dell'autenticazione a due fattori, aggiungendo come procedura di sicurezza anche il suo numero di telefono.
  Se non riesce a reimpostare la password perché hanno già modificato l'e-mail e il numero associato, avvii la procedura di recupero dell'account rubato attraverso il centro assistenza della piattaforma e si rechi presso un qualunque ufficio di polizia per formalizzare la denuncia entro tre mesi dalla conoscenza del fatto.

- **Hanno pubblicato dei post sul mio profilo social che disconosco completamente, cosa posso fare per tutelarmi?**

  Si deve recare in qualsiasi ufficio di polizia per sporgere denuncia di disconoscimento dei post con contestuale denuncia di accesso abusivo sul suo profilo social.
  Se ha ancora accesso al profilo, deve provvedere a scollegare gli altri dispositivi collegati al suo profilo e procedere immediatamente al cambio della password con una più forte e sicura, aggiungendo l'autenticazione a due fattori. Tale metodo di sicurezza rende ancora più arduo al cybercriminale poter accedere al suo profilo, in quanto laddove si acceda con altro dispositivo, viene inviato un codice univoco al numero di cellulare registrato.

- **Guardando la mia home banking ho notato delle operazioni da me non eseguite, cosa mi consigliate di fare?**

  Può recarsi in qualsiasi ufficio di polizia per sporgere una denuncia di disconoscimento delle operazioni e recarsi presso la sua banca per compilare l'apposito reclamo al fine di ottenere il rimborso delle somme di denaro fraudolentemente sottratte.
  In ogni caso, se qualcuno ha disposto tali transazioni significa che hanno avuto accesso ai dati personali della sua carta. Le consigliamo di procedere alla sostituzione e all'inserimento dell'autenticazione a due fattori anche per le transazioni di piccola entità.

- **Come posso capire se le credenziali della mia casella e-mail sono note ai cybercriminali?**

  Può controllare sul sito https://haveibeenpwned.com/ e inserire il proprio indirizzo e-mail. Verrà restituito il risultato di eventuali data breach (ossia violazione e diffusione dei dati), dai quali si evincono i dati che sono conosciuti e in che anno c'è stata la pubblicazione. Nel caso l'esito sia positivo e dunque le sue credenziali siano esposte deve procedere immediatamente al cambio delle stesse con una password più sicura ed efficace (non utilizzata in precedenza o in altre applicazioni) e attivare l'autenticazione a due fattori.

RESTA AGGIORNATO
CON LO SPORTELLO PER
LA SICUREZZA DEGLI UTENTI
DEL WEB DELLA **POLIZIA DI STATO**,
VISITANDO IL SITO:

https://www.commissariatodips.it/

E CON I CONSIGLI
SU COME DIFENDERSI DALLE
TRUFFE DI **POSTE ITALIANE**,
VISITANDO IL SITO:

https://www.poste.it/come-difendersi-dalle-truffe.html