ProDefence

Cyber Security Services

"CLICCA QUI, ORA LÀ"

LA FEBBRE DELL'INVESTITORE

L'articolo mira a esplorare in dettaglio queste tattiche insidiose, fornire una comprensione di come operano questi criminali e delineare misure efficaci per prevenire e combattere queste frodi. Forniremo consigli e strategie essenziali per le vittime attuali e potenziali e per le istituzioni finanziarie per rafforzare le difese contro questi attacchi informatici sempre più raffinati. Aumentando la consapevolezza e implementando solide pratiche di sicurezza, possiamo sperare di proteggere meglio sia le nostre risorse finanziarie che le informazioni personali.

Alexandru Angheluş

Un ringraziamento speciale a sostegno del documento

Zaborilă Florin Ionuț – Ufficiale dell'IPJ Iași

Dipartimento investigativo sui crimini informatici

"INVESTOR FEVER" definisce il comportamento delle persone che, da semplici utenti della tecnologia e di Internet, diventano grandi investitori attraverso di esse, ignorando tutto ciò che hanno acquisito entro una certa età: intuizione, fiducia selettiva, sospetto, informazioni rilevanti, ecc.

Dalle dichiarazioni delle vittime si può apprendere ciò che hanno vissuto durante quel periodo della loro vita:

- "Ho investito 20.000 euro e ho già un guadagno di 150.000, ma non riesco a tirarlo fuori. Il consulente afferma che i pareggi influenzano le seguenti operazioni a lungo termine".
- "Dopo 10.000 euro investiti ho ricevuto il 10% dell'importo, ma se continuo a investire dopo 12 mesi posso prelevare il 45% dell'importo dal conto".
- "Ho perso 7500 euro con gli investimenti, e la polizia mi ha detto che era impalato... alcuni sciocchi, non sanno che è così che si investe, si perde... Si vince lo stesso, perché è quello che mi ha detto il consulente fin dall'inizio".
- "Ho iniziato a inviare denaro e ho comprato azioni, ma non lo dico a nessuno... che sai come sono le persone, invidiose".
- "La Banca ha detto che dietro l'investimento c'era un ciarlatano che mi ha ingannato, ma io non ci credo! Io e quell'uomo abbiamo parlato molto, mi ha parlato della sua famiglia, anche lui aveva dei problemi, era sconvolto dal fatto che lavorasse molte ore".

1. Introduzione
    - Evoluzione delle frodi finanziarie
2. Frode sugli investimenti falsi
    - Metodi di inganno
    - Esempi di frode
3. App utilizzate e accesso ai conti bancari
    - Tattiche pericolose per l'installazione di applicazioni
    - Rischi associati alle app utilizzate
4. Illustrazione dello schema antifrode
    - La complessità del processo di frode
    - Analisi delle fasi delle frodi finanziarie
5. Prevenzione e protezione delle vittime
    - Segnali di allarme di una possibile frode
    - Suggerimenti per la prevenzione
6. Il ruolo delle istituzioni finanziarie
    - Misure di sicurezza e monitoraggio
    - Formazione dei clienti in materia di sicurezza informatica
7. Piano di risposta alla compromissione
    - Azione immediata dopo il rilevamento delle frodi
    - Recupero delle perdite e messa in sicurezza dei conti
8. Conclusione
    - L'importanza della consapevolezza e della prevenzione
9. Bonus
    - Campagne di frode in corso
    - Fonti e approfondimenti

1. Introduzione

Evoluzione delle frodi finanziarie

La frode, nel suo senso più ampio, si riferisce a qualsiasi atto intenzionale di inganno eseguito per guadagno personale o per causare danni a qualcun altro. È un concetto che si manifesta in molteplici forme, che vanno dal semplice inganno a schemi complessi che coinvolgono la manipolazione di sistemi o processi.

Quando si parla di frode finanziaria, ci si riferisce a quegli atti di inganno che mirano ad ottenere vantaggi finanziari illeciti. Può comportare la manipolazione o lo sfruttamento di sistemi finanziari, come le banche o i mercati dei capitali, oppure può coinvolgere direttamente le singole vittime attraverso truffe e inganni. Le frodi finanziarie includono un'ampia gamma di attività illegali, come il furto di identità, le frodi con carta di credito, gli schemi Ponzi e altri tipi di truffe volte a ottenere denaro, beni o servizi senza averne un diritto legale.

Frode commessa attraverso sistemi informatici e mezzi di pagamento elettroniciCodice penale

Secondo il codice penale, queste frodi sono menzionate nella parte speciale, che fa riferimento ai "Delitti contro il patrimonio", capo IV, art. 249-250-251 ed è punibile con la reclusione.

Frode informatica - Art. 249 - L'introduzione, la modifica o la cancellazione di dati informatici, la limitazione dell'accesso a tali dati o l'impedimento in qualsiasi modo del funzionamento di un sistema informatico, al fine di ottenere un vantaggio materiale per sé o per altri, se è stato causato un danno a una persona, è punibile con la reclusione da 2 a 7 anni.

Esecuzione fraudolenta di operazioni finanziarie - Art. 250 - L'esecuzione di un prelievo di denaro contante, il caricamento o lo scaricamento di uno strumento di moneta elettronica o il trasferimento di fondi, mediante l'utilizzo, senza il consenso del titolare, di uno strumento di pagamento elettronico o di dati identificativi che ne consentano l'utilizzo, è punita con la reclusione da 2 a 7 anni.

- L'esecuzione di una delle operazioni di cui al comma 1 è punita con la stessa pena. (1) mediante l'uso non autorizzato di dati identificativi o mediante l'uso di dati identificativi fittizi.

- La trasmissione non autorizzata ad altro soggetto di eventuali dati identificativi, al fine di compiere una delle operazioni previste dal par. (1), è punibile con la reclusione da uno a 5 anni.

Accettazione di operazioni finanziarie fraudolentemente compiute – Art. 251 – L'accettazione di un prelievo di denaro contante, il caricamento o lo scarico di uno strumento di moneta elettronica o il trasferimento di fondi, sapendo che è effettuato utilizzando uno strumento di pagamento elettronico falsificato o utilizzato senza il consenso del suo titolare, è punibile con la reclusione da uno a 5 anni.

- L'accettazione di una delle operazioni di cui al comma 1 è punita con la stessa pena. (1), sapendo che ciò avviene attraverso l'uso non autorizzato di dati identificativi o attraverso l'uso di dati identificativi fittizi.

Negli ultimi decenni, con il progresso della tecnologia e la massiccia digitalizzazione dei servizi finanziari, abbiamo assistito a una trasformazione significativa nella natura e nella complessità delle frodi finanziarie. Questa evoluzione riflette non solo i cambiamenti negli strumenti e nei metodi utilizzati dai criminali informatici, ma anche il continuo adattamento ai nuovi ambienti e comportamenti degli utenti nello spazio digitale.

In passato, le frodi finanziarie erano spesso limitate a tattiche più dirette e meno sofisticate, come il furto di identità attraverso metodi tradizionali o le truffe di vendita per corrispondenza. Tuttavia, nell'era di Internet e della connettività onnipresente, i criminali hanno iniziato a sfruttare l'ambiente online per sviluppare schemi molto più complessi e difficili da rilevare.

Le moderne frodi finanziarie si basano su una varietà di tecniche digitali avanzate. Dal phishing all'ingegneria sociale, passando per malware e sofisticati attacchi informatici, i criminali hanno a disposizione un'ampia gamma di strumenti per manipolare, ingannare e derubare le loro vittime. Questi metodi non solo sono più efficaci, ma consentono anche l'anonimato, aumentando così la portata e l'impatto degli attacchi.

Una peculiarità delle frodi finanziarie odierne è la capacità dei criminali di adattarsi rapidamente alle nuove tecnologie e tendenze. Nel contesto di un mondo sempre più connesso, in cui sempre più transazioni avvengono online, i criminali hanno sviluppato la capacità di sfruttare rapidamente qualsiasi vulnerabilità. Ciò include l'utilizzo dei social media per diffondere falsi schemi di investimento, la compromissione della sicurezza delle app mobili per l'accesso non autorizzato ai conti bancari e persino lo sfruttamento di tecnologie emergenti come criptovalute e blockchain per ideare nuovi tipi di truffe.

Questa frode finanziaria in continua evoluzione significa che sia i consumatori che le istituzioni finanziarie devono essere costantemente vigili e adattarsi alle nuove minacce. L'educazione e la consapevolezza sono fondamentali, così come gli investimenti nella sicurezza informatica e nei sistemi di monitoraggio delle transazioni. Comprendendo l'evoluzione di queste frodi, possiamo sviluppare strategie più efficaci per prevenirle e combatterle.

2. Frode sugli investimenti falsi

Metodi di inganno

Le frodi sui falsi investimenti sono una delle principali minacce nel mondo finanziario moderno, che colpisce sia i singoli investitori che talvolta i mercati finanziari su larga scala. Questi schemi di inganno sono progettati per apparire il più convincenti e redditizi possibile, utilizzando vari metodi per attirare e manipolare le vittime.

Annunci fuorvianti: questa tattica è molto efficace grazie all'ampio e facile accesso al pubblico in generale attraverso piattaforme online e social network. Gli annunci possono presentarsi sotto forma di banner accattivanti, post sponsorizzati o persino consigli personalizzati. L'uso di false testimonianze o il coinvolgimento di personaggi pubblici, sia attraverso l'uso non autorizzato delle loro immagini che false associazioni, ha lo scopo di

creare un senso di legittimità e fiducia. Ciò può rendere difficile per gli investitori distinguere tra opportunità autentiche e false.

E-mail e messaggi fraudolenti: i criminali utilizzano spesso e-mail e messaggi diretti per contattare le potenziali vittime. Questi messaggi sono spesso ben scritti e sembrano provenire da istituzioni finanziarie legittime o consulenti di fiducia. L'obiettivo è quello di guadagnare la fiducia delle vittime e convincerle a divulgare informazioni personali o a investire in schemi falsi.

Siti web falsi: i siti web creati per supportare questi schemi falsi sono spesso realizzati con un alto grado di professionalità. Possono includere recensioni false, grafici impressionanti e persino sistemi di trading simulati per fornire una parvenza di autenticità e successo. Questi siti possono essere difficili da distinguere da quelli legittimi, il che li rende pericolosi per gli investitori.

Pressione del tempo: le tattiche di pressione del tempo giocano sulla psicologia umana, creando un senso di urgenza che può indurre le vittime ad agire rapidamente senza avere il tempo di analizzare la situazione in dettaglio. I criminali possono affermare che l'offerta è limitata nel tempo o che le opportunità di investimento sono "una volta nella vita". Questo porta spesso a decisioni avventate e avventate da parte delle vittime.

Essere consapevoli di queste tattiche è il primo passo per proteggersi dalle frodi attraverso investimenti falsi. È essenziale che gli investitori controllino sempre la fonte di qualsiasi offerta di investimento e siano scettici sulle promesse di profitti elevati con un basso rischio. È anche importante consultare consulenti finanziari di fiducia e fare controlli approfonditi prima di impegnarsi in qualsiasi tipo di investimento.

Esempi di frode

La frode sui falsi investimenti rappresenta un territorio vasto e diversificato nel mondo della criminalità finanziaria, ognuno con le proprie peculiarità e meccanismi distinti. Questi schemi sono spesso progettati in modo intelligente, con l'obiettivo principale di sfruttare la fiducia e la mancanza di informazioni delle potenziali vittime. I criminali che orchestrano tali frodi sono spesso molto ben informati sulla psicologia umana e sui meccanismi dei mercati finanziari, utilizzando questa conoscenza per mascherare le loro attività illecite.

Un elemento chiave per il successo di questi schemi è quello di presentarli come opportunità di investimento legittime e altamente redditizie. Sono spesso confezionati e promossi in modo fuorviante, utilizzando il linguaggio e la grafica del settore finanziario per apparire autentici. I criminali possono utilizzare vari canali, da Internet e dai social media alle reti di vendita tradizionali, per raggiungere un pubblico più ampio.

Schemi Ponzi:

- Questi schemi prendono il nome da Charles Ponzi, che utilizzò questo metodo negli anni '20. L'essenza di uno schema Ponzi è quella di pagare i profitti degli investitori esistenti dai fondi portati da nuovi investitori, invece di generare profitti reali.

- Gli schemi Ponzi spesso iniziano pagando profitti elevati per attirare ancora più investitori. Ma man mano che il numero di nuovi investitori diminuisce, i fondi per pagare i profitti si esauriscono, il che porta inevitabilmente al collasso dello schema.
- Un esempio noto è lo schema di Bernie Madoff, che è stata la più grande frode di questo tipo nella storia.

Investimenti in beni inesistenti:

- Questi schemi implicano promesse di investimento in progetti o beni che sono completamente fittizi o grossolanamente esagerati nel loro valore.
- Gli esempi possono includere investimenti in miniere d'oro non sfruttate, terre rare o tecnologie rivoluzionarie. I criminali creano storie avvincenti, complete di documentazione e testimonianze false per apparire legittime.
- Le vittime sono attirate con la prospettiva di grandi e rapidi guadagni, ma in realtà quei beni o progetti non esistono o sono completamente non redditizi.

Offerte di azioni false:

- Questo metodo prevede la vendita di azioni per società che non esistono o che sono sopravvalutate. I criminali possono creare siti Web falsi e materiali di marketing per convincere gli investitori del potenziale della "società".
- Sono spesso utilizzati in quello che viene chiamato un "pump and dump", in cui il valore delle azioni viene gonfiato artificialmente, dopodiché i criminali le vendono rapidamente prima che crollino.
- Le vittime si ritrovano a possedere azioni che sono praticamente prive di valore.

Investire in criptovalute:

- Con la crescente popolarità delle criptovalute, si sono sviluppati anche numerosi schemi di investimento falsi basati sulle criptovalute.
- Questi schemi possono coinvolgere criptovalute nuove e sconosciute pubblicizzate come il prossimo Bitcoin o piattaforme di investimento che promettono alti profitti dal trading di criptovalute.
- Molti di questi schemi crollano dopo aver raccolto una quantità sufficiente di fondi, lasciando gli investitori con perdite significative.

<u>Investimenti effettuati su piattaforme fake:</u>

- La vittima viene convinta a utilizzare una falsa piattaforma di investimento, gestita da criminali.
- La piattaforma è un clone perfetto delle piattaforme di investimento, offrendo agli utenti i valori delle azioni, l'importo guadagnato, la possibilità di acquistare e altre azioni, ma ciò che la vittima non sa è che tutti i valori vengono alterati dal criminale perché la piattaforma non comunica con le infrastrutture di investimento.
- I grandi guadagni si ottengono solo come membro VIP, e questo status si guadagna attraverso investimenti seri, ma in realtà è un modo per convincere l'utente a "investire" più soldi.

Riconoscere questi tipi di schemi falsi è fondamentale per qualsiasi investitore. È fondamentale condurre ricerche approfondite, consultare esperti finanziari di fiducia ed evitare qualsiasi investimento che sembra troppo bello per essere vero. La vigilanza e l'educazione sono le armi migliori contro questo tipo di frodi finanziarie.

3. App utilizzate e accesso ai conti bancari

Tattiche pericolose per l'installazione di applicazioni

I criminali informatici utilizzano una varietà di metodi sofisticati per indurre gli utenti a installare app pericolose che consentono loro di accedere a conti bancari e altre informazioni sensibili. Comprendere queste tattiche è fondamentale per essere in grado di riconoscere e prevenire le minacce alla sicurezza personale e finanziaria.

Messaggi ed e-mail di phishing:

- Uno dei metodi più comuni è l'invio di e-mail o messaggi che sembrano provenire da istituti finanziari o altre entità attendibili. Questi messaggi possono richiedere agli utenti di scaricare un'app per "aggiornamenti di sicurezza" o di "verificare la presenza di transazioni recenti".
- I messaggi di phishing sono spesso molto convincenti e possono includere loghi e design che imitano quelli di istituzioni legittime.

Annunci ingannevoli sulle piattaforme online:

- Gli annunci online possono essere utilizzati per promuovere app che sembrano legittime ma in realtà sono strumenti di malware. Questi annunci possono apparire su siti Web rispettabili, rendendoli più credibili.
- A volte questi annunci possono sfruttare le vulnerabilità del browser per avviare il download automatico dell'applicazione pericolosa.

Spoofing delle app più diffuse:

- I criminali possono creare versioni false di app popolari che, una volta installate, possono accedere a informazioni riservate. Queste app clone possono essere trovate in app store non ufficiali o anche in alcuni casi su piattaforme ufficiali.
- Gli utenti possono essere indotti a scaricare queste app promettendo funzionalità aggiuntive o copiando alcuni aspetti delle app originali.

Sfruttamento di pagine web compromesse o false

- I criminali possono utilizzare pagine web compromesse o false, la cui immagine e funzionalità sono simili a quelle delle piattaforme di investimento legali, ingannando le vittime.
- Gli utenti indirizzati a queste piattaforme false vivranno l'esperienza di un investitore, vedranno

Sfruttamento dei social media e messaggistica:

- I criminali possono utilizzare account di social media compromessi o falsi per inviare link di download ad app dannose. I messaggi possono provenire da amici o conoscenti della vittima, aumentando le possibilità che si fidino e scarichino l'app.

Codice QR e link diretti:

- I codici QR o i link diretti che portano al download dell'app possono essere inseriti in luoghi pubblici o su materiali pubblicitari. Una volta scansionati o acceduti, possono avviare il download di un'applicazione pericolosa all'insaputa dell'utente.

Diventando consapevoli delle tattiche utilizzate dai criminali informatici per diffondere applicazioni pericolose, gli utenti possono prendere precauzioni più efficaci per proteggere i propri dati personali e finanziari. Comprendere i rischi associati al download e all'installazione di app non autorizzate è un primo passo fondamentale per garantire la sicurezza online.

Rischi associati alle app utilizzate

I rischi associati alle applicazioni utilizzate dai criminali informatici sono diversi e possono avere gravi conseguenze sia per la sicurezza individuale che per l'integrità dei dati finanziari degli utenti. Queste app maligne sono progettate per rubare informazioni, compromettere i dispositivi e facilitare l'accesso non autorizzato ad asset finanziari e account personali.

Furto d'identità:
Le app pericolose possono raccogliere informazioni personali come nomi, indirizzi, date di nascita e persino numeri di previdenza sociale. Questi dati possono essere utilizzati per commettere furti di identità, consentendo ai criminali di accedere a conti bancari, aprire nuovi prestiti o commettere altri reati sotto l'identità della vittima.

Accesso alle informazioni finanziarie:
Molte di queste app prendono di mira direttamente il furto di informazioni finanziarie, come numeri di carte di credito, credenziali del conto bancario online e altri dettagli finanziari. L'accesso a queste informazioni può portare al furto di fondi o a transazioni non autorizzate.

Rimuovi/influenza l'autenticazione multipla (2FA/MFA)
L'intercettazione o la manipolazione dell'autenticazione doppia/multipla delle applicazioni bancarie consentirà ai criminali informatici di autenticarsi continuamente nelle applicazioni bancarie, modificare i dati di accesso e fare implicitamente trading direttamente dall'applicazione, senza che la vittima veda le loro attività.

Malware e ransomware:
Alcune app possono installare malware o ransomware sul dispositivo della vittima. Il malware può tracciare le attività degli utenti, intercettare i dati o danneggiare il sistema. Il ransomware blocca l'accesso ai dati sul tuo dispositivo, chiedendo un riscatto per sbloccarlo.

Compromissione della sicurezza del dispositivo:

L'installazione di app pericolose può indebolire la sicurezza complessiva del dispositivo, rendendolo vulnerabile a ulteriori attacchi. Ciò può includere l'apertura di porte di rete, la disabilitazione della protezione antivirus o la creazione di scappatoie per consentire ad altri criminali di accedere al tuo dispositivo.

Spionaggio e monitoraggio:
Alcune app possono essere utilizzate per spiare le attività degli utenti, incluso l'accesso alla fotocamera e al microfono del dispositivo. Ciò può portare a gravi violazioni della privacy e alla raccolta di informazioni sensibili.

Phishing e ingegneria sociale:
Le app possono anche essere utilizzate per eseguire campagne di phishing, inviando messaggi falsi che sembrano provenire da fonti attendibili per ottenere informazioni sensibili.

Danno reputazionale:
Nei casi in cui i criminali ottengono l'accesso agli account dei social media della vittima, possono inviare messaggi o post compromettenti che potrebbero danneggiare la reputazione di quella persona.

4. Illustrazione dello schema antifrode

La complessità del processo di frode

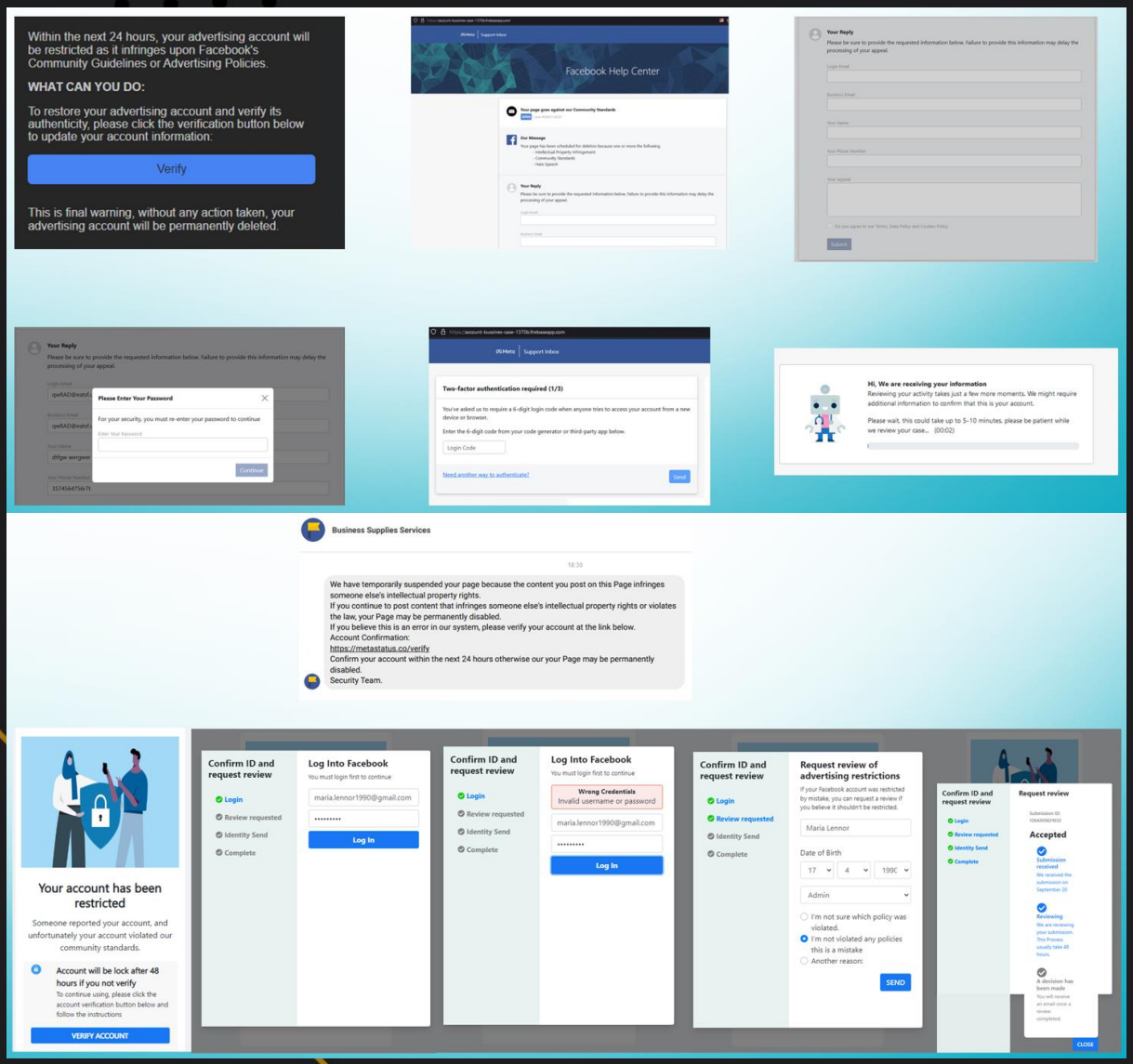
Il processo di frode è piuttosto complesso e presenta diverse varianti di sviluppo, a seconda del livello di formazione dell'utente (potenziale vittima) dal punto di vista tecnico e del potere di persuasione dell'autore del reato rispetto alla persona che ha già raggiunto la fase di comunicazione con lui.

L'attacco iniziale: ottenere le risorse necessarie

Un primo aspetto importante nel processo di frode è il contatto con le potenziali vittime, che può avvenire in modo diretto, attraverso un approccio mirato o in modo indiretto immettendo informazioni false nell'ambiente online, attraverso messaggi, post, commenti e/o pubblicità che promuovono lo scenario di frode.

a. Nuovi account: account di social media o altre piattaforme create appositamente per il lancio di informazioni online. Bassa credibilità nell'approccio diretto, ma d'impatto se aggiunta a pagine di social media compromesse.
b. Account compromessi: account ottenuti acquistandoli o con altri metodi, come malware o phishing.

Un esempio di attacco informatico di phishing, che è stato effettuato tramite messaggi e/o taggando la persona o la pagina posseduta. Questi messaggi annunciavano la violazione delle regole della piattaforma e chiedevano ai proprietari di confermare la propria identità, per non perdere l'accesso.



L'accesso e le informazioni personali aggiunte alle pagine false hanno consentito agli aggressori di accedere agli account delle vittime, con il passo successivo che consiste nel bloccare i legittimi titolari dall'accesso ad account e pagine compromessi. Per semplificare il loro lavoro, i creatori di pagine false hanno anche aggiunto la possibilità per la vittima di dichiarare se è un amministratore della pagina.

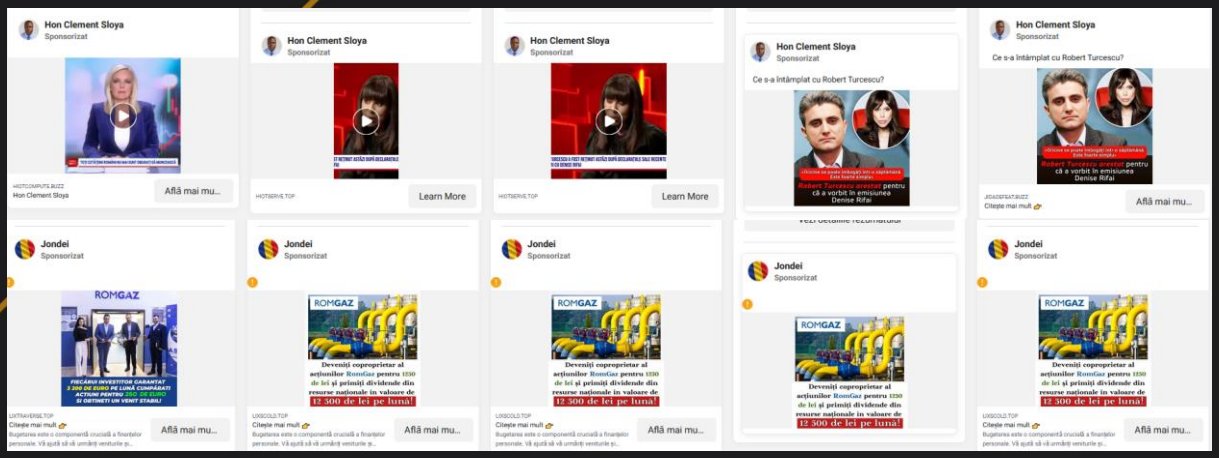
Una singola campagna di questo tipo ha raccolto in pochi giorni 100.000 account di utenti di Facebook, e inizialmente è stato stabilito che il 10% di essi appartiene a vittime in Romania, perché il loro smistamento è stato fatto identificando righe di testo contenenti domini locali ".ro" e la classificazione automatica impostata dagli aggressori "| EN". Successivamente, dopo un'analisi più dettagliata dei dati raccolti dai criminali, si è scoperto che molte vittime non soddisfacevano i criteri di smistamento iniziali, ma i loro nomi e cognomi sono rumeni. Ciò ha portato la percentuale a oltre il 45% a scapito degli utenti rumeni, l'attacco ha chiaramente preso di mira le persone di lingua rumena, indipendentemente dalla loro posizione attuale.

Sfruttare account/pagine compromessi – Prendere di mira le vittime

Quando si tratta dell'attaccante, può avere diversi ruoli nella conduzione dell'attacco iniziale o solo uno:

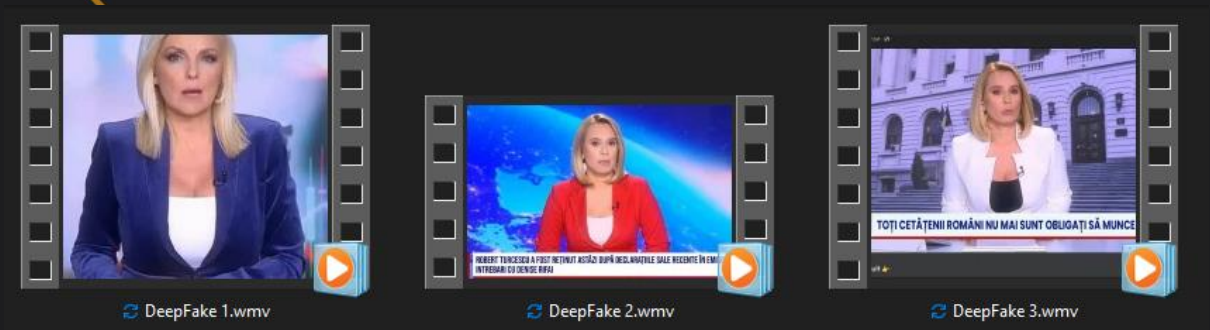
- Il ruolo del criminale informatico che lancia campagne di phishing o malware per ottenere i dati di accesso degli account dei social media,
- Il ruolo dell'autore del reato che ha ricevuto/acquistato i dati di accesso e li sfrutta avviando la fase successiva della frode.

Il più grande interesse degli aggressori è quello di compromettere gli account che gestiscono/generano annunci. Questi account vengono utilizzati per creare annunci che promuovono frodi finanziarie, generando al contempo costi elevati per gli account compromessi e sfruttati. Costi a carico dei titolari di carte bancarie inserite nelle piattaforme di generazione di annunci.



Lo scopo dello sfruttamento degli account è quello di promuovere la frode e indirizzare implicitamente le possibili vittime verso pagine false utilizzate nel processo di frode. Le fasi di esecuzione di questo processo possono essere viste nell'immagine.

E con una frequenza insolitamente alta si ricorre al furto dell'identità visiva di persone influenti e alla generazione di sequenze video fake o Deep Fake (video falsi generati dall'Intelligenza Artificiale attraverso i quali vengono clonate l'immagine e la voce di una persona

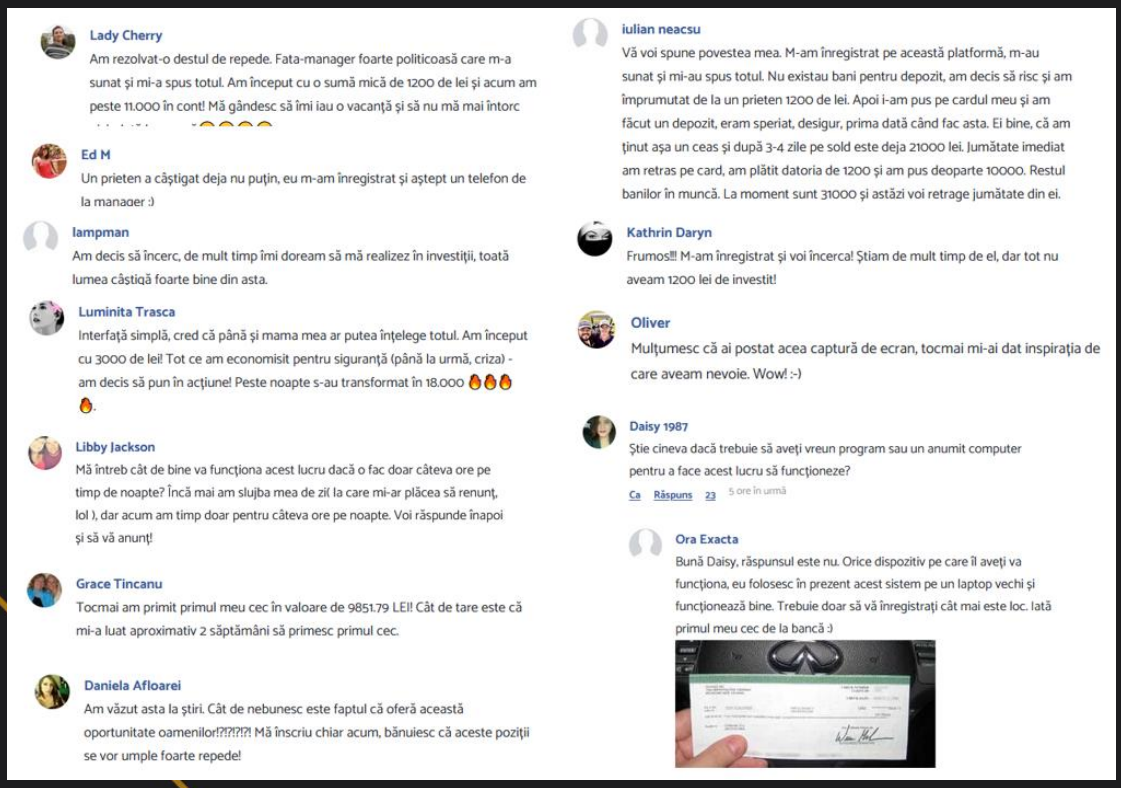


I cyber-utenti disattenti o non istruiti entreranno negli scenari creati dagli aggressori e giocheranno il ruolo della vittima, poiché raggiungono questa posizione accettando la manipolazione visiva. Generalmente, la manipolazione viene effettuata inviando messaggi informativi/di avviso e viene menzionato un limite temporaneo, che ha il ruolo di rimuovere l'utente dal suo stato di comfort, che lo farà non prestare attenzione ai dettagli.

L'utente arrivato sulla pagina fake viene accolto da una valanga di immagini e testi che supportano lo scenario di frode, ma contengono anche dichiarazioni false di persone che affermano di far già parte di quell'attività, di aver acquistato il prodotto o investito in azioni, e i risultati sono quelli descritti dagli amministratori delle pagine false.

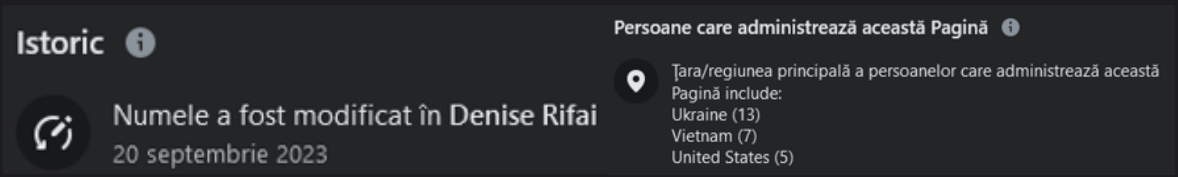
L'ingegneria sociale ha un ruolo importante da svolgere.

I commenti falsi comprendono una moltitudine di situazioni per coprire una vasta scala di utenti di tecnologia desiderosi di guadagnare denaro o commenti su misura per l'obiettivo finale di frode/truffa.

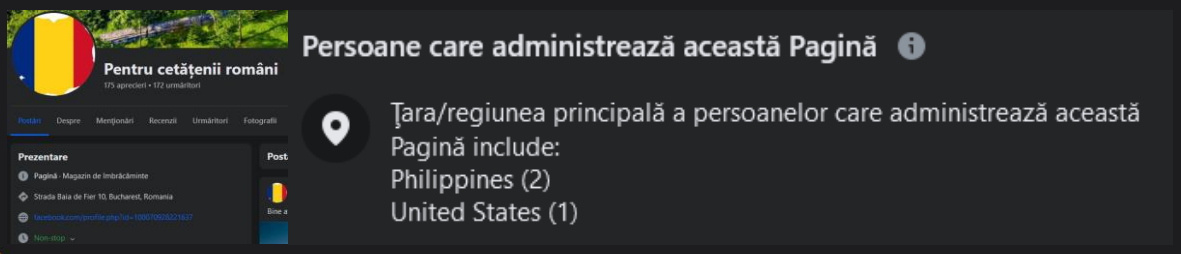


- *Aiuto tecnico per chi non è bravo,* ma vorrebbe,
- *Ho guadagnato un "amico"* - Quindi è qualcosa di testato,
- *Applicazione facile da usare "che anche la mamma potrebbe..."* – Includi sciocchi e persone anziane,
- *Lasciare il lavoro per guadagni elevati* - Se quel ragazzo può, proviamoci.
- *"Ho appena ricevuto il mio primo assegno..."* – "Garanzia" di vincita,
- *"L'ho visto al telegiornale"* – È una cosa detta in TV, quindi va bene...
- *"queste posizioni si riempiranno in fretta..."* – Veloce che forse non riusciamo più a raggiungere tutti.
- *"Non c'erano soldi... Ho preso in prestito"* – Convincere chi non ha soldi, ma potrebbe prendere in prestito.
- *"Ho fatto un deposito, avevo paura, era la prima volta..."* – Sottile eliminazione dei dubbi e convinzione di provare.
- ..... and so on.

Le pagine che generano annunci fraudolenti stanno subendo importanti modifiche all'immagine e all'amministrazione.



Un esempio di campagna di phishing sugli utenti in Romania. Durante il periodo di analisi, l'account aveva generato 420 annunci con la campagna fraudolenta e, a una verifica attuale, l'account indica un numero di 510 annunci generati, l'ultimo dei quali è stato pubblicato il 26 ottobre 2023.



Stato attuale della pagina: Online, ma con un nome diverso...

... un altro paese, altri bersagli di frode.

L'interesse dei criminali e lo scopo di quelli menzionati è quello di convincere gli utenti ad accedere a pagine false e compilare un modulo fornendo i dettagli di contatto, in modo che il responsabile della piattaforma possa mettersi in contatto con loro.

Oppure, a seconda dei casi, lo scopo della truffa è quello di indurre le persone ad acquistare un prodotto o un servizio offerto dalla pagina falsa!

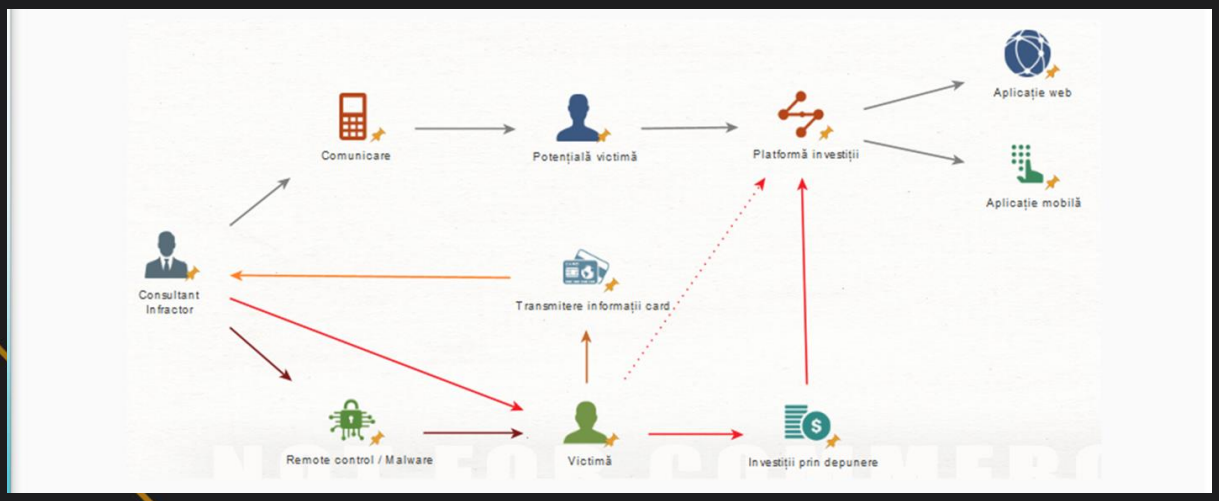
Analisi delle fasi delle frodi finanziarie

I dati di contatto ottenuti dai criminali sono un passo importante nel processo di frode, poiché le persone che hanno visitato la pagina falsa si sono iscritte all'elenco delle possibili vittime.

In questa fase, il ruolo più importante è svolto dal Consulente, il criminale che entra in contatto con la potenziale vittima, perché, attraverso l'ingegneria sociale, farà tutto il possibile affinché il suo interlocutore creda all'intero scenario intorno alla truffa e lo convinca di essere un vincitore al 100% in questa operazione.

Mantenendo come argomento principale le frodi finanziarie attraverso investimenti in criptovalute o azioni di società di successo, va inteso che l'attaccante entrerà in contatto con utenti con diversi livelli di istruzione, competenze tecniche ed età. Le indagini hanno rilevato che le perdite finanziarie si sono verificate attraverso investimenti diretti da parte degli utenti, l'invio di fondi a criminali, l'utilizzo di app false e l'utilizzo di app di controllo remoto, l'accesso ai dispositivi degli utenti per aiutarli a creare account su piattaforme false e persino l'utilizzo delle loro app bancarie.

Il flusso delle attività svolte si può capire dall'immagine qui sotto, ma allo stesso tempo si può osservare l'adattabilità degli autori di reato al livello di formazione delle vittime, a volte parte degli obiettivi da eliminare, perché raggiungono il denaro senza richiedere molto sforzo.



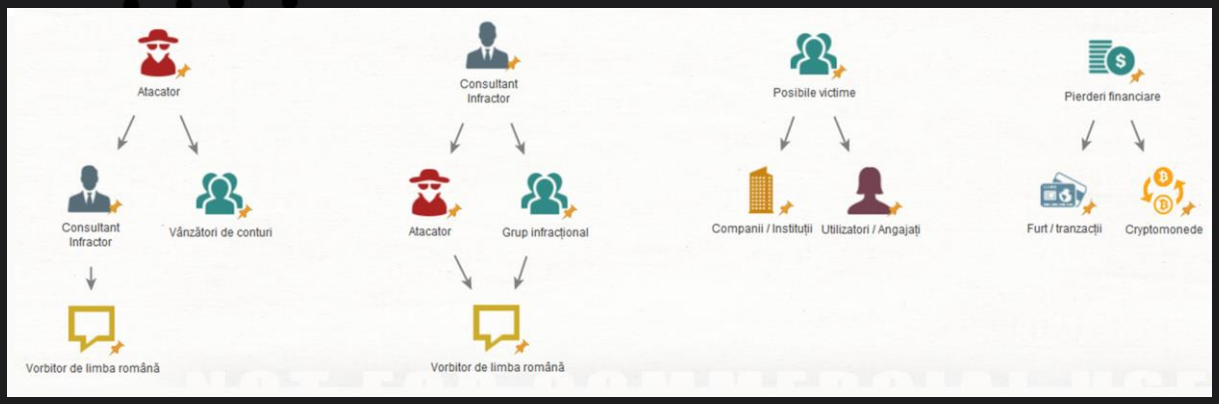
Concludendo analizzando il processo di frode, abbiamo un quadro chiaro del ruolo dei criminali, degli utenti e delle perdite finanziarie.

L'attaccante iniziale può essere solo la persona che lancia le campagne di phishing/malware, per ottenere i dati di accesso e venderli ai criminali che si occuperanno di frodi, può far parte del team antifrode o una sola e medesima persona del consulente che completa il processo di frode.

Il consulente può essere, come detto, l'aggressore originario stesso o far parte di un gruppo criminale, in cui ognuno ha il suo ruolo. Secondo le dichiarazioni delle vittime, gli autori del reato sono di lingua rumena, spesso con uno specifico accento russo.

Le possibili vittime sono aziende/istituzioni i cui account sono stati compromessi e sfruttati per creare annunci e utenti coinvolti in ogni fase dello scenario di frode.

Le vittime delle frodi (investimenti falsi) sono utenti desiderosi di guadagni rapidi, ma privi di educazione digitale, educazione informatica e persone facilmente manipolabili.



Le ingenti perdite finanziarie sono dovute alla manipolazione della vittima nel processo di investimento, ai criminali che applicano tecniche per ottenere la fiducia della vittima, ma possono arrivare all'imposizione di debiti alla piattaforma di investimento e persino alle minacce di recuperare saldi in sospeso fittizi.

5. Prevenzione e protezione per gli utenti

Segnali di allarme di una possibile frode

I segnali di allarme di possibili frodi finanziarie sono fondamentali per riconoscere ed evitare di cadere nelle trappole dei criminali. Ognuno di questi segnali indica potenziali rischi e richiede una maggiore vigilanza da parte degli utenti:

a. Offerte con rese insolitamente elevate:

Nel mondo degli investimenti, una regola generale è che rendimenti elevati di solito comportano dei rischi da abbinare. Qualsiasi offerta che prometta profitti sostanziali senza un rischio corrispondente è sospetta. Queste offerte possono far parte di uno schema Ponzi o di altri tipi di truffe.

b. Pressione ad agire rapidamente:

La tattica di creare urgenza viene spesso utilizzata per impedire ai potenziali investitori di analizzare criticamente l'offerta. In questi casi, i criminali possono sostenere che l'opportunità è "una volta nella vita" o che è necessaria un'azione immediata per beneficiare delle condizioni offerte.

c. Richieste di informazioni personali o finanziarie:

Le richieste inaspettate di informazioni sensibili sono un chiaro segno di frode. I criminali possono utilizzare questi dati per accedere a conti bancari, per furti di identità o altre attività illegali. Qualsiasi richiesta di questo tipo deve essere trattata con grande cautela.

d. Mancanza di trasparenza o documentazione poco chiara:

Le offerte di investimento legittime sono generalmente trasparenti e accompagnate da una documentazione chiara e dettagliata. La mancanza di trasparenza, la documentazione ambigua o poco chiara o la riluttanza a rispondere a domande specifiche sono segni che qualcosa non va.

e. Comunicazioni non richieste:

Le e-mail, le telefonate o i messaggi non richiesti che offrono opportunità di investimento o che richiedono informazioni personali devono essere trattati con sospetto. Questi metodi vengono spesso utilizzati nelle campagne di phishing per ottenere l'accesso a informazioni riservate.

Riconoscere questi segnali di allarme è un passo cruciale nella protezione contro le frodi finanziarie. È importante che gli utenti siano vigili, facciano domande e conducano ricerche approfondite prima di prendere qualsiasi decisione finanziaria. La prevenzione inizia con l'informazione e la consapevolezza dei rischi.

Suggerimenti per la prevenzione

Per evitare le insidie delle frodi finanziarie, è essenziale adottare un approccio proattivo e informato alla gestione delle proprie finanze e delle informazioni personali. Ecco alcuni suggerimenti dettagliati per la prevenzione che possono aiutarti a proteggerti:

a. Conduci ricerche approfondite:

- Verifica della fonte: prima di investire, assicurati che l'entità e l'offerta siano legittime. Cerca informazioni sull'azienda e sui suoi prodotti o servizi.
- Consultazione delle autorità di regolamentazione finanziaria: verificare se l'entità è registrata o regolamentata da un'autorità finanziaria riconosciuta.
- Cercare una consulenza indipendente: è sempre utile ottenere un secondo parere da un consulente finanziario indipendente che possa valutare obiettivamente l'offerta.
- Chiedi il parere di un esperto: chiedi l'opinione di un professionista della sicurezza informatica quando ci sono sospetti sulle pagine web o sulle piattaforme a cui sei stato indirizzato.

b. Proteggi le tue informazioni personali:

- Vigilanza nella comunicazione: sii estremamente cauto quando ti vengono chiesti dati personali o finanziari. Non fornire queste informazioni attraverso canali non sicuri o persone non autorizzate.

- Protezione dei dati: utilizza tecniche di protezione dei dati, come la crittografia e l'archiviazione sicura, per mantenere riservate le tue informazioni. Personale.

c. Utilizzare le procedure di sicurezza online:

- Aggiornamento software: assicurati che il tuo sistema operativo e le tue app siano sempre aggiornati per proteggerti dalle vulnerabilità di sicurezza.
- Usa autenticazione doppia/multipla: abilita l'autenticazione a più fattori su tutti i principali account per aggiungere un ulteriore livello di sicurezza.

d. Evita le decisioni impulsive:

- Analisi e riflessione: prenditi del tempo per valutare ogni opportunità finanziaria e soppesare i pro e i contro. Una decisione finanziaria ben ponderata è sempre più sicura.
- Evita la pressione: non essere costretto a prendere decisioni rapide, soprattutto in situazioni stressanti o sotto pressione.

e. Monitora i tuoi conti finanziari:

- Controlli regolari: esamina regolarmente gli estratti conto bancari e le transazioni per qualsiasi attività sospetta o non autorizzata.
- Avvisi sulle transazioni: l'impostazione di avvisi per transazioni insolite o di grandi dimensioni può essere un modo efficace per rilevare rapidamente le frodi.

Implementando queste pratiche, sarai in grado di aumentare il tuo livello di protezione contro potenziali frodi finanziarie. La consapevolezza e la formazione continua sono essenziali in questo processo, poiché i metodi dei detenuti possono cambiare ed evolversi. Tieni sempre d'occhio le ultime tattiche di frode e adatta le tue strategie di sicurezza di conseguenza per mantenere le tue finanze al sicuro.

6. Il ruolo delle istituzioni finanziarie

Misure di sicurezza e monitoraggio

a. Sistemi avanzati di rilevamento delle frodi:

- Questi sistemi utilizzano algoritmi sofisticati e l'apprendimento automatico per identificare transazioni insolite o sospette, aiutando a rilevare tempestivamente potenziali frodi.
- L'analisi comportamentale e la modellazione del rischio vengono utilizzate anche per valutare i modelli di transazione e identificare attività insolite.

b. Sicurezza dell'infrastruttura tecnologica:

- La protezione dell'infrastruttura IT comporta la protezione dei dati dei clienti e dei sistemi bancari dagli attacchi informatici utilizzando tecnologie di crittografia avanzate e solide soluzioni di sicurezza.
- L'aggiornamento e la manutenzione continui dei sistemi IT sono fondamentali per stare al passo con i metodi sempre più sofisticati dei criminali informatici.

c. Autenticazione a più fattori e sicurezza dell'account:

- L'implementazione dell'autenticazione a più fattori (MFA) fornisce un ulteriore livello di sicurezza, richiedendo più di un semplice nome utente e password per accedere a un account.
- L'autenticazione a più fattori può includere elementi come codici generati dal telefono, domande di sicurezza o impronte digitali, aumentando significativamente la sicurezza degli account online.

Formazione dei clienti in materia di sicurezza informatica

La formazione dei clienti in materia di sicurezza informatica è un aspetto cruciale nella strategia degli istituti finanziari per combattere le frodi. Informando e formando i clienti, possono ridurre significativamente il rischio che cadano vittime di attività illegali online.

a. Programmi di sensibilizzazione alla sicurezza:

- Materiali didattici: fornire brochure, guide e altro materiale informativo che spieghi i diversi tipi di frode informatica, come phishing, vishing, smishing e altre tecniche di ingegneria sociale.
- Esempi reali e casi di studio: la presentazione di casi reali di frode può aiutare i clienti a comprendere meglio i rischi e a riconoscere i segnali di allarme.

b. Comunicazione regolare con i clienti:

- Newsletter: invio periodico di newsletter che includono suggerimenti sulla sicurezza, avvisi su nuovi tipi di frode e raccomandazioni per la protezione online.
- Canali di social media: utilizzo di piattaforme di social media per diffondere la consapevolezza e raggiungere un pubblico più ampio.

c. Formazione sulla sicurezza online:

- Webinar e workshop: organizzazione di sessioni educative ed eventi online in cui esperti di sicurezza informatica forniscono consigli pratici e rispondono alle domande dei clienti.
- Simulazioni e test: implementazione di simulazioni di phishing per insegnare ai clienti come identificare e-mail e messaggi sospetti.

d. Assistenza clienti:

- Linee di assistenza: fornire una hotline dedicata in cui i clienti possono segnalare incidenti sospetti e ricevere supporto immediato.
- Consulenza personalizzata: fornisce consulenza e supporto personalizzati ai clienti che hanno bisogno di aiuto per gestire la sicurezza dei loro account online.

e. Aggiornamenti di sicurezza e avvisi:

- Notifiche di sicurezza: invio di avvisi tramite e-mail o messaggi di testo quando viene rilevata un'attività sospetta sull'account del cliente o quando compaiono nuove minacce.
- Informazioni aggiornate: Mantenere una sezione sul sito web della banca con le ultime notizie e consigli nel campo della sicurezza informatica.

Attraverso queste misure, gli istituti finanziari non solo proteggono le proprie risorse, ma contribuiscono anche a creare un ambiente finanziario più sicuro per tutti gli utenti. La formazione e la collaborazione continua con i clienti, insieme all'implementazione delle più recenti tecnologie di sicurezza, sono essenziali nella lotta contro le frodi finanziarie. Questo approccio combinato aiuta a creare fiducia nel sistema finanziario e a proteggere efficacemente gli asset dei clienti dalle minacce informatiche.

Pertanto, il ruolo delle istituzioni finanziarie è fondamentale non solo per una gestione efficiente delle finanze, ma anche per garantire un ambiente sicuro e protetto per le transazioni finanziarie nell'era digitale. Lavorando a stretto contatto con le autorità di regolamentazione, altre istituzioni e i clienti, possono continuare a migliorare le difese contro le sofisticate frodi finanziarie.

7. Piano di risposta alla compromissione

Azione immediata dopo il rilevamento delle frodi

a. Notifica agli istituti finanziari:

Contatta immediatamente la banca o l'istituto finanziario coinvolto. Annullare o bloccare immediatamente qualsiasi carta di credito/debito e l'accesso online ai conti è fondamentale per prevenire ulteriori perdite.

b. Modificare le credenziali di accesso:

Modificare le password e i dettagli di sicurezza per tutti gli account online interessati. Ciò include account di posta elettronica, piattaforme di social media e qualsiasi servizio online associato.

c. Segnalazione alle autorità competenti:

Segnala le frodi alla polizia, alla direzione nazionale della sicurezza informatica e ad altre autorità competenti, come l'autorità nazionale di vigilanza sulle frodi finanziarie. Può aiutare a indagare e prevenire altri casi simili.

d. Monitoraggio del credito:

In caso di furto di identità, è importante monitorare i rapporti di credito per eventuali attività non autorizzate. I servizi di monitoraggio del credito possono essere presi in considerazione per avvisare di eventuali cambiamenti sospetti.

Recupero delle perdite e messa in sicurezza dei conti

a. Conservazione delle prove:

Salva tutte le discussioni, i documenti, gli indirizzi e-mail, i numeri di telefono delle persone con cui hai interagito. Evita di eliminare le app installate o i dispositivi di formattazione coinvolti nell'incidente.
Le informazioni possono aiutare a identificare come è stata effettuata la frode, ma anche l'identità dei criminali.

b. Revisione delle transazioni:

Esamina tutte le transazioni recenti per rilevare eventuali attività non autorizzate. Ciò contribuirà a determinare il livello di compromesso.

c. Documentazione dettagliata e segnalazione dell'incidente:

Tieni un registro dettagliato di tutte le comunicazioni e le azioni intraprese dopo il rilevamento delle frodi. Ciò include qualsiasi denuncia alla polizia, corrispondenza con la banca e modifiche di sicurezza apportate.

d. Consulenza con un esperto finanziario o legale:

In casi complessi, può essere utile consultare un esperto finanziario o legale che ti guidi attraverso il processo di recupero delle perdite e protegga i tuoi diritti.

e. Rivalutazione delle misure di sicurezza:

Rivedere e migliorare le procedure di sicurezza per prevenire incidenti simili in futuro. Ciò può includere l'investimento in soluzioni di sicurezza più avanzate, la revisione delle politiche di sicurezza e la sensibilizzazione sulla protezione dei dati.

8. Conclusione

L'importanza della consapevolezza e della prevenzione

La sensibilizzazione e la prevenzione sono essenziali nella lotta contro le frodi finanziarie. In un mondo sempre più digitalizzato, in cui le transazioni finanziarie avvengono in gran parte online, il potenziale di attività illegali è amplificato. È quindi fondamentale che sia i privati che gli istituti finanziari siano ben informati e adottino misure proattive per proteggersi da queste minacce.

Il ruolo della consapevolezza:

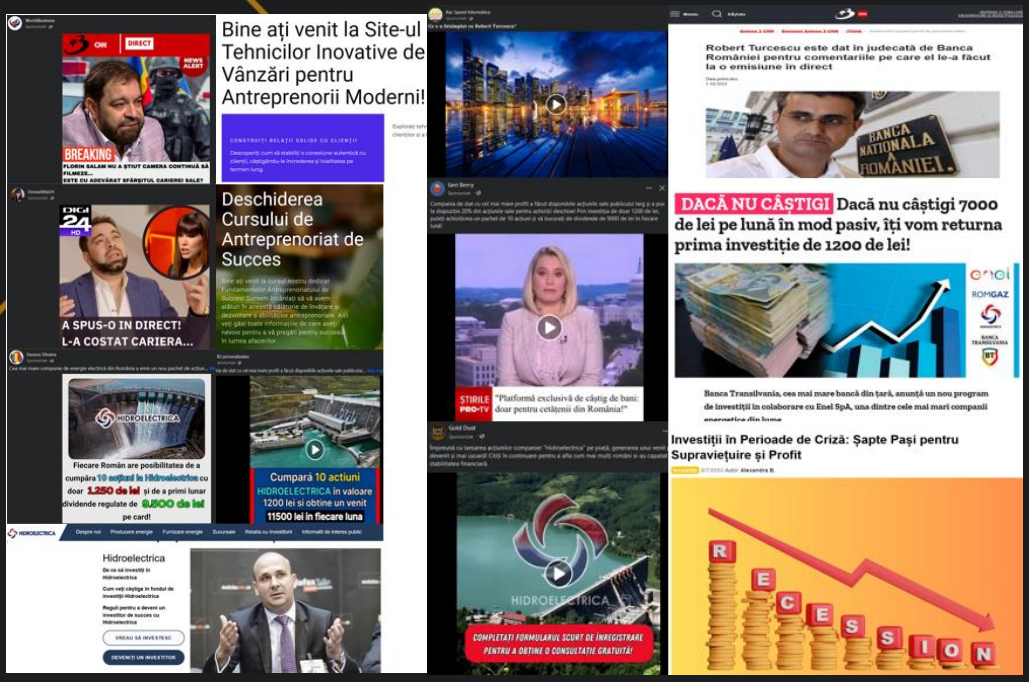
- **Educazione: essere** ben informati sui diversi tipi di frode finanziaria e sui loro segnali di avvertimento può fare la differenza tra essere una vittima e prevenire un attacco. La formazione continua è fondamentale per tenere il passo con i metodi in continua evoluzione dei detenuti.
- **Condivisione delle informazioni:** la diffusione delle conoscenze personali e delle esperienze relative alle frodi finanziarie nelle comunità può aiutare ad aumentare la consapevolezza generale e proteggere gli altri.

L'importanza della prevenzione:

- **Misure di sicurezza: l** 'implementazione di solide misure di sicurezza, sia a livello personale che istituzionale, è essenziale per impedire ai criminali di accedere alle informazioni e alle risorse finanziarie.
- **Vigilanza continua:** mantenere un atteggiamento di vigilanza e rivedere regolarmente le pratiche di sicurezza ci assicura di essere sempre un passo avanti rispetto ai criminali.

Infine, la prevenzione e la lotta contro le frodi finanziarie sono una responsabilità condivisa. Attraverso la collaborazione tra consumatori, istituzioni finanziarie e autorità di regolamentazione, possiamo costruire un ambiente finanziario più sicuro e protetto. La consapevolezza del rischio e le misure di sicurezza proattive non sono solo una salvaguardia contro le perdite finanziarie, ma anche un passo essenziale verso il mantenimento di una società digitale sicura e fiduciosa.

9. Bonus: campagne di frode in corso



Fonti e approfondimenti

Attacco di phishing – **Cyber AID**
https://www.cyberaid.eu/atacul-de-tip-phishing/

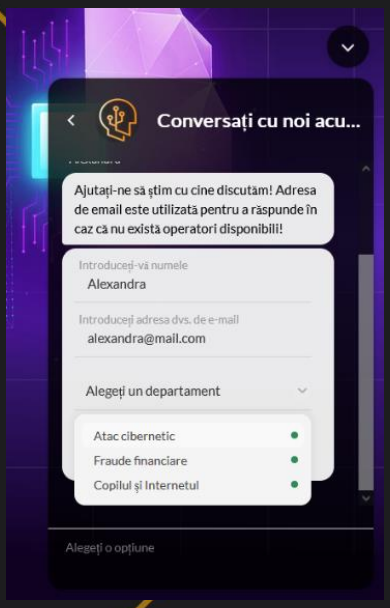
Bank Phishing – **Sicurezza online**
https://sigurantaonline.ro/phishing-ul-bancar/

Articoli sulla sicurezza informatica – **Prodefence**
https://www.prodefence.ro/articole-securitate-cibernetica/

Rilevamento delle frodi online – **DNSC**
https://www.dnsc.ro/cautare?ceCaut=frauda

Cyber Intelligence – Utilizzo della profilazione – **ISACA | DNSC**
https://dnsc.ro/vezi/document/isaca-cyber-intelligence-using-profiling/

Cyber Edequation – Genitori e Figli – **Prodefence**
https://www.youtube.com/@AlexandruAnghelus/videos



Chat cibernetica

Prima di inviare dati personali o denaro a uno sconosciuto, è meglio chiedere il parere di specialisti. È gratuito e posso aiutarti a non prendere decisioni sbagliate!

https://www.cyberaid.eu/ | https://sigurantadigitala.ro/

Disponibile solo in rumeno!

”Dici che è tutto una bugia e che sono tutti ladri, ma lo stesso TU dai tutti i tuoi dati personali e i tuoi soldi a una persona che ti ha raccontato storie tramite SMS o al telefono”

ProDefence

Cyber Security Services