ProDefence

Cyber Security Services

”APASĂ AICI, ACUM ACOLO”

FEBRA INVESTITORULUI

Articolul își propune să exploreze în detaliu aceste tactici insidioase, să ofere o înțelegere a modului în care operează acești infractori și să prezinte măsuri eficiente de prevenire și de combatere a acestor fraude. Vom oferi sfaturi esențiale și strategii atât pentru victimele actuale și potențiale, cât și pentru instituțiile financiare, în scopul de a consolida apărarea împotriva acestor atacuri cibernetice tot mai rafinate. Prin creșterea gradului de conștientizare și prin implementarea de practici de securitate robuste, putem spera să ne protejăm mai bine atât resursele financiare, cât și informațiile personale.

Alexandru Angheluș

Mulțumiri speciale în susținerea documentului

Zaborilă Florin Ionuț – Ofițer în cadrul IPJ Iași
Compartimentul de Investigare a Infracțiunilor Informatice

”**FEBRA INVESTITORULUI**” definește comportamentul oamenilor care din simpli utilizatori ai tehnologiei și ai internetului ajung mari investitori prin intermediul acestora, ignorând tot ceea ce au dobândit până la o anumită vârstă: intuiție, încrederea selectivă, suspiciunea, informații relevante etc.

Din declarațiile victimelor puteți învăța ceea ce au experimentat în acea perioadă a vieții:

- ”Am investit 20.000 euro și deja am un câștig de 150.000, dar nu îi pot scoate. Consultantul zice că extragerile afectează pe termen lung următoarele tranzacții”
- ”După 10.000 euro investiți am primit 10% din sumă, dar dacă continui să investesc după 12 luni pot extrage 45% din suma din cont”.
- ”Am pierdut 7500 de euro cu investițiile, iar la Poliție mi-au spus că este țeapă... niște proști, ei nu știu că așa este în investiții, mai pierzi... mai câștigi, că așa mi-a spus de la început consultantul”
- ”M-am apucat de trimis bani și am cumpărat acțiuni, dar nu zic la nimeni... că știi cum sunt oamenii, invidioși”.
- ”Cei de la Bancă au spus că în spatele investiției este un șarlatan care m-a păcălit, dar nu cred! Eu cu omul ăla am discutat multe, mi-a spus despre familia lui, avea și el probleme, era supărat că muncește multe ore..”

1. Introducere
    - Evoluția fraudelor financiare
2. Fraude prin Investiții False
    - Metode de înșelăciune
    - Exemple de fraudă
3. Aplicații utilizate și Acces la Conturi Bancare
    - Tactici de instalare a aplicațiilor periculoase
    - Riscurile asociate cu aplicațiile utilizate
4. Ilustrarea Schemei de Fraudare
    - Complexitatea procesului de fraudare
    - Analiza etapelor fraudei financiare
5. Prevenire și Protecție pentru Victime
    - Semne de avertizare ale unei posibile fraude
    - Sfaturi de prevenire
6. Rolul Instituțiilor Financiare
    - Măsuri de securitate și monitorizare
    - Educația clienților în domeniul securității cibernetice
7. Planul de Răspuns în Caz de Compromitere
    - Acțiuni imediate după detectarea fraudei
    - Recuperarea pierderilor și securizarea conturilor
8. Concluzie
    - Importanța conștientizării și prevenției
9. Bonus
    - Campanii de fraudă în derulare
    - Surse și lecturi suplimentare

1. Introducere

Evoluția fraudelor financiare

Frauda, în sensul său cel mai larg, se referă la orice act intenționat de inducere în eroare realizat pentru câștig personal sau pentru a provoca un prejudiciu altcuiva. Este un concept care se manifestă în multiple forme, variind de la simpla înșelăciune la scheme complexe care implică manipularea unor sisteme sau procese.

Când vorbim despre frauda financiară, ne referim la acele acte de înșelăciune care au ca obiectiv obținerea de beneficii financiare ilegale. Aceasta poate implica manipularea sau exploatarea sistemelor financiare, cum ar fi băncile sau piețele de capital, sau poate implica direct victime individuale prin escrocherii și înșelăciuni. Frauda financiară include o gamă largă de activități ilegale, cum ar fi furtul de identitate, frauda cu carduri de credit, schemele Ponzi, și alte tipuri de înșelăciuni care vizează obținerea de bani, bunuri sau servicii fără a avea dreptul legal la ele.

Fraude comise prin sisteme informatice și mijloace de plată electronice
Codul Penal

Conform Codului penal aceste fraude sunt menționate în partea specială, care face referire la ”Infracțiuni contra patrimoniului” Capitolul IV Art. 249 - 250 – 251 și se pedepsește cu închisoarea.

Frauda informatică - Art. 249
- Introducerea, modificarea sau ștergerea de date informatice, restricționarea accesului la aceste date ori împiedicarea în orice mod a funcționării unui sistem informatic, în scopul de a obține un beneficiu material pentru sine sau pentru altul, dacă s-a cauzat o pagubă unei persoane, se pedepsește cu închisoarea de la 2 la 7 ani.

Efectuarea de operațiuni financiare în mod fraudulos - Art. 250
- Efectuarea unei operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, prin utilizarea, fără consimțământul titularului, a unui instrument de plată electronică sau a datelor de identificare care permit utilizarea acestuia, se pedepsește cu închisoarea de la 2 la 7 ani.

- Cu aceeași pedeapsă se sancționează efectuarea uneia dintre operațiunile prevăzute în alin. (1), prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive.

- Transmiterea neautorizată către altă persoană a oricăror date de identificare, în vederea efectuării uneia dintre operațiunile prevăzute în alin. (1), se pedepsește cu închisoarea de la unu la 5 ani.

Acceptarea operațiunilor financiare efectuate în mod fraudulos – Art. 251
- Acceptarea unei operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, cunoscând că este efectuată prin folosirea unui instrument de plată electronică falsificat sau utilizat fără consimțământul titularului său, se pedepsește cu închisoarea de la unu la 5 ani.

- Cu aceeași pedeapsă se sancționează acceptarea uneia dintre operațiunile prevăzute în alin. (1), cunoscând că este efectuată prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive.

În ultimele decenii, cu avansarea tehnologiei și digitalizarea masivă a serviciilor financiare, am fost martorii unei transformări semnificative în natura și complexitatea fraudelor financiare. Această evoluție reflectă nu doar schimbările în instrumentele și metodele folosite de infractorii cibernetici, dar și adaptarea continuă la noile medii și comportamente ale utilizatorilor în spațiul digital.

În trecut, fraudele financiare erau adesea limitate la tactici mai directe și mai puțin sofisticate, cum ar fi furtul de identitate prin metode tradiționale sau escrocherii prin corespondență. Cu toate acestea, în era internetului și a conectivității omniprezente, infractorii au început să exploateze mediul online pentru a dezvolta scheme mult mai complexe și mai greu de detectat.

Fraudele financiare moderne se bazează pe o varietate de tehnici digitale avansate. De la phishing și inginerie socială, la malware și atacuri cibernetice sofisticate, infractorii au la dispoziție o gamă largă de instrumente pentru a manipula, înșela și fura de la victimele lor. Aceste metode nu sunt doar mai eficiente, dar permit și anonimatul, mărind astfel raza și impactul atacurilor.

O particularitate a fraudei financiare actuale este capacitatea infractorilor de a se adapta rapid la noile tehnologii și tendințe. În contextul unei lumi tot mai conectate, unde tot mai multe tranzacții se desfășoară online, infractorii au dezvoltat abilitatea de a exploata rapid orice vulnerabilitate. Aceasta include folosirea rețelelor sociale pentru a răspândi scheme de investiții false, compromiterea securității aplicațiilor mobile pentru acces neautorizat la conturi bancare și chiar exploatarea tehnologiilor emergente, cum ar fi criptomoneda și blockchain-ul, pentru a concepe noi tipuri de escrocherii.

Această evoluție constantă a fraudelor financiare înseamnă că atât consumatorii, cât și instituțiile financiare trebuie să fie în permanență vigilente și să se adapteze la noile amenințări. Educația și conștientizarea sunt vitale, la fel ca investițiile în securitatea cibernetică și în sistemele de monitorizare a tranzacțiilor. Prin înțelegerea evoluției acestor fraude, putem dezvolta strategii mai eficiente pentru a le preveni și combate.

2. Fraude prin Investiții False

Metode de înșelăciune

Fraudele prin investiții false reprezintă o amenințare majoră în lumea financiară modernă, afectând atât investitori individuali cât și, uneori, piețele financiare la scară largă. Aceste scheme de înșelăciune sunt concepute pentru a părea cât mai convingătoare și profitabile, folosind diverse metode pentru a atrage și manipula victimele.

Reclamele Înșelătoare: Această tactică este extrem de eficientă datorită accesului larg și ușor la publicul larg prin intermediul platformelor online și a rețelelor sociale. Reclamele pot apărea sub forma unor bannere atrăgătoare, postări sponsorizate sau chiar recomandări

personalizate. Utilizarea mărturiilor false sau implicarea persoanelor publice, fie prin utilizarea neautorizată a imaginilor lor, fie prin false asocieri, este menită să creeze o senzație de legitimitate și încredere. Acest lucru poate face dificilă pentru investitori să distingă între oportunitățile autentice și cele false.

Email-uri și Mesaje Frauduloase: Infractorii folosesc adesea email-uri și mesaje directe pentru a contacta potențialele victime. Aceste mesaje sunt adesea bine redactate și par să provină de la instituții financiare legitime sau consultanți de încredere. Scopul este de a câștiga încrederea victimelor și de a le determina să divulge informații personale sau să facă investiții în schemele false.

Site-uri Web Falsificate: Site-urile web create pentru a susține aceste scheme false sunt adesea realizate cu un grad înalt de profesionalism. Ele pot include recenzii false, grafice impresionante, și chiar sisteme de tranzacționare simulate pentru a oferi o aparență de autenticitate și succes. Aceste site-uri pot fi dificil de deosebit de cele legitime, făcându-le periculoase pentru investitori.

Presiunea Timpului: Tactica presiunii timpului joacă pe psihologia umană, creând o senzație de urgență care poate determina victimele să acționeze rapid, fără a avea timp să analizeze situația în detaliu. Infractorii pot susține că oferta este limitată în timp sau că oportunitățile de investiție sunt "o dată în viață". Aceasta duce adesea la decizii pripite și nesăbuite din partea victimelor.

Conștientizarea acestor tactici este primul pas în protejarea împotriva fraudelor prin investiții false. Este esențial ca investitorii să verifice întotdeauna sursa oricărei oferte de investiții și să fie sceptici în fața promisiunilor de profituri mari cu risc scăzut. De asemenea, este important să se consulte cu consultanți financiari de încredere și să se facă verificări amănunțite înainte de a se angaja în orice tip de investiție.

Exemple de fraudă

Fraudele prin investiții false reprezintă un teritoriu vast și diversificat în lumea criminalității financiare, fiecare cu particularitățile și mecanismele sale distincte. Aceste scheme sunt adesea ingenios concepute, având ca scop principal exploatarea încrederii și a lipsei de informare a potențialelor victime. Infractorii care orchestrează astfel de fraude sunt adesea foarte bine informați în privința psihologiei umane și a mecanismelor pieței financiare, folosind aceste cunoștințe pentru a-și masca activitățile ilicite.

Un element cheie în succesul acestor scheme este prezentarea lor ca oportunități de investiții legitime și foarte profitabile. Ele sunt adesea ambalate și promovate într-o manieră care induce în eroare, folosindu-se de limbajul și grafica tipică industriei financiare pentru a părea autentice. Infractorii pot folosi diverse canale, de la internet și social media până la rețele tradiționale de vânzări, pentru a ajunge la un public cât mai larg.

Scheme Ponzi:

- Aceste scheme sunt numite după Charles Ponzi, care a folosit această metodă în anii 1920. Esența unei scheme Ponzi constă în plătirea profiturilor investitorilor existenți din fondurile aduse de noi investitori, în loc să genereze profituri reale.

- Schemele Ponzi adesea încep plătind profituri mari pentru a atrage și mai mulți investitori. Dar, pe măsură ce numărul de noi investitori scade, fondurile pentru plata profiturilor se epuizează, ceea ce duce inevitabil la prăbușirea schemei.
- Un exemplu notoriu este schema lui Bernie Madoff, care a fost cea mai mare fraudă de acest tip din istorie.

Investiții în Bunuri Inexistente:

- Aceste scheme implică promisiuni de investiții în proiecte sau bunuri care sunt fie complet fictive, fie extrem de exagerate în ceea ce privește valoarea lor.
- Exemple pot include investiții în mine de aur neexploatate, terenuri rare sau tehnologii revoluționare. Infractorii creează povești convingătoare, complete cu documentații false și mărturii pentru a părea legitime.
- Victimele sunt ademenite cu perspectiva unor câștiguri mari și rapide, dar în realitate, bunurile sau proiectele respective nu există sau sunt complet neviabile.

Oferte de Acțiuni False:

- Această metodă implică vânzarea de acțiuni pentru companii care nu există sau care sunt supraevaluate. Infractorii pot crea site-uri web false și materiale de marketing pentru a convinge investitorii de potențialul "companiei".
- Sunt adesea folosite în ceea ce se numește "pump and dump", unde valoarea acțiunilor este artificial umflată, după care infractorii le vând rapid înainte de a se prăbuși.
- Victimele se trezesc deținând acțiuni care sunt practic fără valoare.

Investiții în Criptomonede:

- Odată cu creșterea popularității criptomonedelor, s-au dezvoltat și numeroase scheme de investiții false bazate pe criptomonede.
- Aceste scheme pot implica criptomonede noi, necunoscute, promovate ca fiind următoarea Bitcoin, sau platforme de investiții care promit profituri mari din tranzacționarea criptomonedelor.
- Multe dintre aceste scheme se prăbușesc după ce atrag o sumă suficientă de fonduri, lăsând investitorii cu pierderi semnificative.

<u>Investiții realizate pe platforme false:</u>

- Victima este convinsă să utilizeze o platformă falsă de investiții, care este administrată de infractori.
- Platforma este o clonă perfectă a platformelor de investiții, oferind utilizatorilor valorile acțiunilor, sumă câștigată, posibilitatea de a cumpăra și alte acțiuni, dar ceea ce nu știe victima este că toate valorile sunt modificate de infractor, deoarece platforma nu comunică cu infrastructurile de investiții.
- Câștigurile mari se realizează doar ca membru VIP, iar acest statut se câștigă prin investiții serioase, dar în realitate este un mod de a convinge utilizatorul să ”investească” mai mulți bani.

Recunoașterea acestor tipuri de scheme false este vitală pentru orice investitor. Este crucial să se efectueze cercetări amănunțite, să se consulte experți financiari de încredere și să se evite orice investiție care pare prea bună pentru a fi adevărată. Vigilența și educația sunt cele mai bune arme împotriva acestor tipuri de fraude financiare.

3. Aplicații utilizate și Acces la Conturi Bancare

Tactici de instalare a aplicațiilor periculoase

Infractorii cibernetici folosesc o varietate de metode sofisticate pentru a convinge utilizatorii să instaleze aplicații periculoase, care le permit accesul la conturile bancare și alte informații sensibile. Înțelegerea acestor tactici este crucială pentru a putea recunoaște și preveni amenințările la adresa securității personale și financiare.

Mesaje și Email-uri Phishing:

- Una dintre cele mai comune metode este trimiterea de email-uri sau mesaje care par a fi de la instituții financiare sau alte entități de încredere. Aceste mesaje pot solicita utilizatorilor să descarce o aplicație pentru "actualizări de securitate" sau pentru a "verifica tranzacții recente".
- Mesajele de phishing sunt adesea foarte convingătoare și pot include logouri și design-uri care imită cele ale instituțiilor legitime.

Reclame Înșelătoare pe Platforme Online:

- Reclamele online pot fi folosite pentru a promova aplicații care par legitime, dar care sunt, de fapt, instrumente de malware. Aceste reclame pot apărea pe site-uri web respectabile, făcându-le să pară mai credibile.
- Uneori, aceste reclame pot exploata vulnerabilități ale browserului pentru a iniția descărcarea automată a aplicației periculoase.

Falsificarea Aplicațiilor Populare:

- Infractorii pot crea versiuni false ale aplicațiilor populare, care odată instalate, pot accesa informații confidențiale. Aceste aplicații clone pot fi găsite în magazine de aplicații neoficiale sau chiar și în unele cazuri pe platforme oficiale.
- Utilizatorii pot fi ademeniți să descarce aceste aplicații prin promisiuni de funcții suplimentare sau prin copierea unor aspecte ale aplicațiilor originale.

Exploatarea paginilor web compromise sau false

- Infractorii pot utiliza pagini web compromise sau false, a căror imagine și funcționalitate este asemănătoare cu cea a platformelor legale de investiții, inducând în eroare victimele.
- Utilizatorii direcționați pe aceste platforme false vor trăi experiența unui investitor, vor vedea

Exploatarea Rețelelor Sociale și Mesagerie:

- Infractorii pot folosi conturi compromise sau false pe rețelele sociale pentru a trimite linkuri de descărcare a aplicațiilor maligne. Mesajele pot veni de la prieteni sau cunoscuți ai victimei, crescând șansele ca aceasta să aibă încredere și să descarce aplicația.

QR Code și Linkuri Directe:

- Codurile QR sau linkurile directe care conduc la descărcarea aplicațiilor pot fi plasate în locuri publice sau pe materiale publicitare. Odată scanate sau accesate, acestea pot iniția descărcarea unei aplicații periculoase fără știrea utilizatorului.

Prin conștientizarea tacticilor folosite de infractorii cibernetici pentru a răspândi aplicații periculoase, utilizatorii pot adopta măsuri de precauție mai eficiente pentru a-și proteja datele personale și financiare. Înțelegerea riscurilor asociate cu descărcarea și instalarea aplicațiilor neautorizate este un prim pas crucial în asigurarea securității online.

Riscurile asociate cu aplicațiile utilizate

Riscurile asociate cu aplicațiile utilizate de infractorii cibernetici sunt diverse și pot avea consecințe grave atât pentru securitatea individuală, cât și pentru integritatea datelor financiare ale utilizatorilor. Aceste aplicații maligne sunt concepute pentru a fura informații, a compromite dispozitive și a facilita accesul neautorizat la active financiare și conturi personale.

Furtul de Identitate:
Aplicațiile periculoase pot colecta informații personale, cum ar fi nume, adrese, date de naștere și chiar codul numeric personal (CNP). Aceste date pot fi folosite pentru a comite furt de identitate, permițând infractorilor să acceseze conturi bancare, să deschidă noi credite sau să comită alte infracțiuni sub identitatea victimei.

Accesul la Informații Financiare:
Multe dintre aceste aplicații vizează direct furtul de informații financiare, cum ar fi numerele de carduri de credit, datele de autentificare la conturile bancare online și alte detalii financiare. Accesul la aceste informații poate duce la furtul de fonduri sau la tranzacții neautorizate.

Eliminare/ Influențare autentificare multiplă (2FA/ MFA)
Interceptarea sau manipularea autentificării duble/ multiple a aplicațiilor bancare va permite infractorilor cibernetici autentificarea continua în aplicațiile bancare, modificarea datelor de acces și implicit tranzacționarea direct din aplicatie, fără ca victima să vadă activitățile acestora.

Malware și Ransomware:
Anumite aplicații pot instala malware sau ransomware pe dispozitivul victimei. Malware-ul poate urmări activitățile utilizatorului, intercepta date sau deteriora sistemul. Ransomware-ul blochează accesul la datele de pe dispozitiv, cerând o răscumpărare pentru deblocarea acestora.

Compromiterea Securității Dispozitivului:
Instalarea aplicațiilor periculoase poate slăbi securitatea generală a dispozitivului, făcându-l vulnerabil la atacuri suplimentare. Acest lucru poate include deschiderea porturilor de rețea, dezactivarea protecției antivirus sau crearea de breșe prin care alți infractori pot accesa dispozitivul.

Spionaj și Monitorizare:
Unele aplicații pot fi folosite pentru a spiona activitățile utilizatorilor, inclusiv prin accesarea camerei și microfonului dispozitivului. Aceasta poate duce la încălcări grave ale vieții private și la colectarea de informații sensibile.

Phishing și Inginerie Socială:
Aplicațiile pot fi folosite și pentru a desfășura campanii de phishing, trimițând mesaje false care par să provină de la surse de încredere pentru a obține informații sensibile.

Deteriorarea Reputației:
În cazurile în care infractorii obțin acces la conturile de social media ale victimei, pot trimite mesaje compromițătoare sau postări care pot afecta reputația persoanei respective.

4. Ilustrarea Schemei de Fraudare

Complexitatea procesului de fraudare

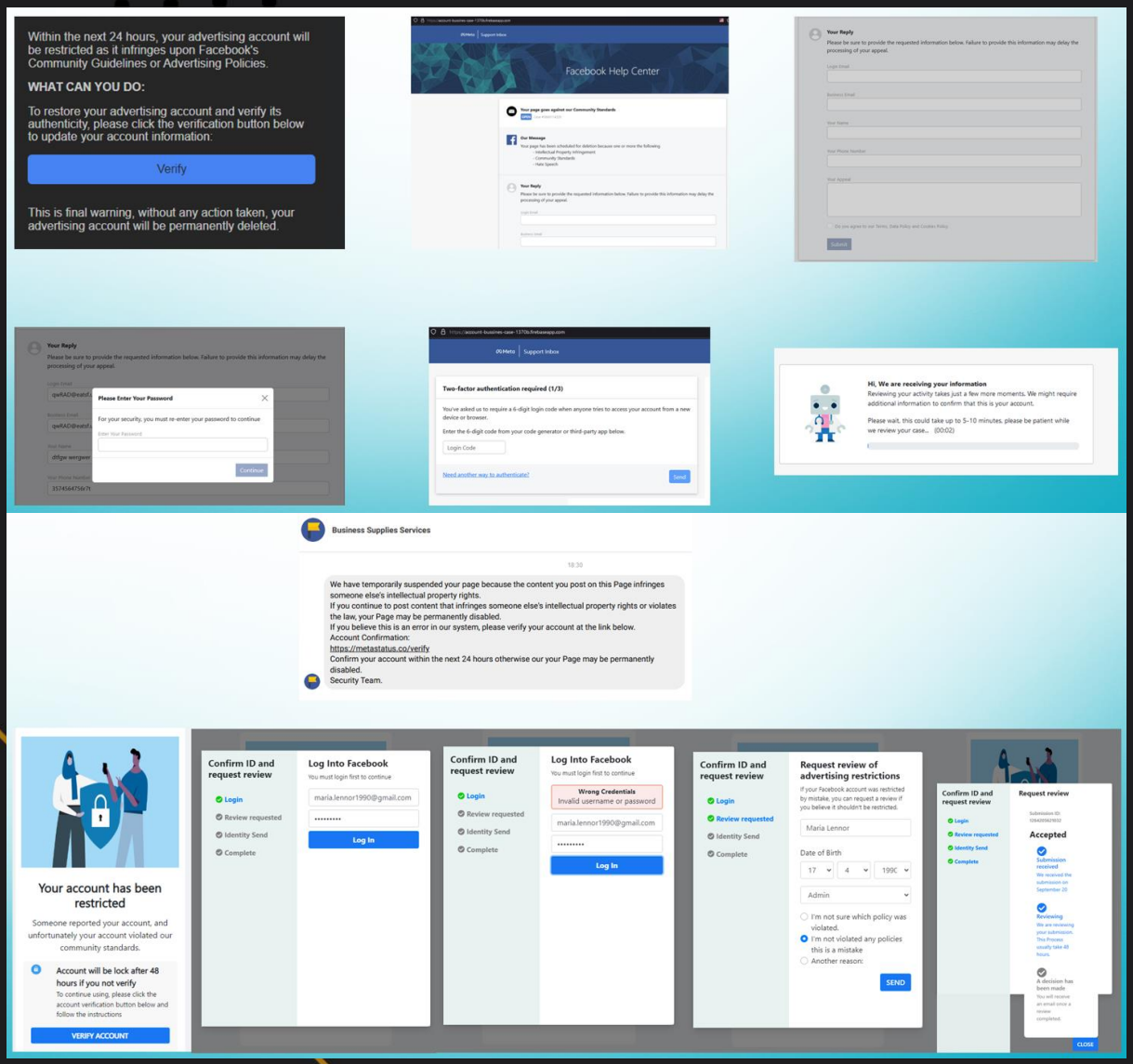
Procesul de fraudare este unul destul de complex și are mai multe variante de desfășurare, în funcție de nivelul de pregătire a utilizatorului(potențială victimă) din punct de vedere tehnic și de puterea de convingere a infractorului asupra persoanei care a ajuns deja la faza de comunicare cu acesta.

Atacul inițial – obținerea resurselor necesare

Un prim aspect important în procesul de fraudare este contactul cu potențialele victime, care se poate efectua într-un mod direct, prin abordare țintită sau într-un mod indirect prin plasarea informațiilor false în mediul online, prin mesaje, postări, comentarii și/ sau reclame de promovare a scenariului de fraudare.

a. Conturi noi: Conturi de social media sau alte platforme, create în mod special pentru lansarea informațiilor în mediul online. Credibilitate scăzută în abordarea directă, dar cu impact dacă sunt adăugate la pagini de social media compromise.
b. Conturi compromise: Conturi obținute prin cumpărarea acestora sau prin alte metode, cum ar fi programele malițioase sau phishing-ul.

Un exemplu de atac cibernetic de tip phishing, care s-a realizat prin intermediul mesajelor sau/ și prin etichetarea persoanei sau a paginii deținute. Aceste mesaje anunțau încălcarea regulilor platformei și cereau deținătorilor să își confirme identitatea, pentru a nu pierde accesul.



Informațiile de acces și cele personale adăugate în paginile false, ofereau acces atacatorilor la conturile victimelor, următorul pas fiind blocarea accesului deținătorilor de drept la conturile și paginile compromise. Pentru a își ușura munca, creatorii paginilor false au adăugat și posibilitatea ca victima să declare dacă este administrator de pagină.

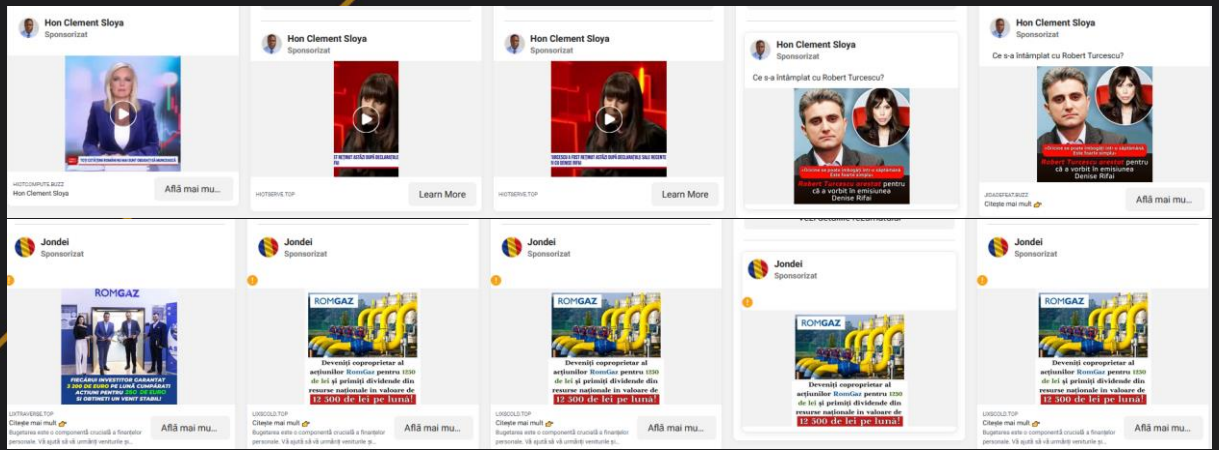
O singură campanie de acest tip, a strâns în câteva zile 100.000 de conturi ale utilizatorilor platformei Facebook, iar inițial s-a stabilit ca 10% dintre acestea aparțin victimelor din România, deoarece sortarea lor s-a făcut prin identificarea liniilor din text care conțin domenii locale ”.ro” și clasificarea automată setată de atacatori ”| RO”. Ulterior, după analizarea mai amănunțită a datelor colectate de infractori s-a constatat că foarte multe victime nu îndeplineau criteriile de sortare inițiale, dar numele și prenumele acestora sunt românești. Acest aspect a schimbat procentajul la peste 45% în defavoarea utilizatorilor români, atacul având ca țintă clară persoane vorbitoare de limba română, indiferent de locația actuală a acestora.

Exploatarea conturilor/ paginilor compromise – Direcționarea victimelor

Când vine vorba de Atacator, acesta poate avea mai multe roluri în desfășurarea atacului inițial sau unul singur:

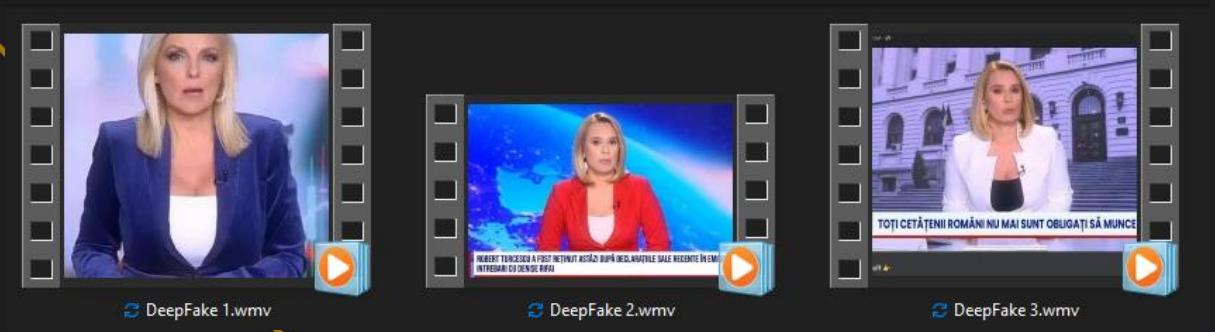
- Rolul infractorului cibernetic care lansează campaniile de phishing sau malware, pentru obținerea datelor de acces ale conturilor de social media,
- Rolul infractorului care a primit/ cumpărat datele de acces și le exploatează prin lansarea următoarei etape a fraudei.

Cel mai mare interes al atacatorilor este să compromită conturi care administrează/ generează reclame. Aceste conturi sunt utilizate la crearea reclamelor de promovare a fraudei financiare, totodată generând costuri mari conturilor compromise și exploatate. Costuri care vor fi suportate de deținătorii cardurilor bancare introduse în platformele de generare a reclamelor.



Scopul exploatării conturilor este promovarea fraudei și implicit direcționarea posibilelor victime spre paginile false utilizare în procesul de fraudare. Etapele realizării acestui proces se pot vedea în imagine.

Și cu o frecvență neobișnuit de mare se utilizează furtul de identitate vizuală a unor persoane influente și generarea de secvențe video false sau de tip Deep Fake (filmări false generate de Inteligența Artificială prin care se clonează imaginea și vocea unei persoane)

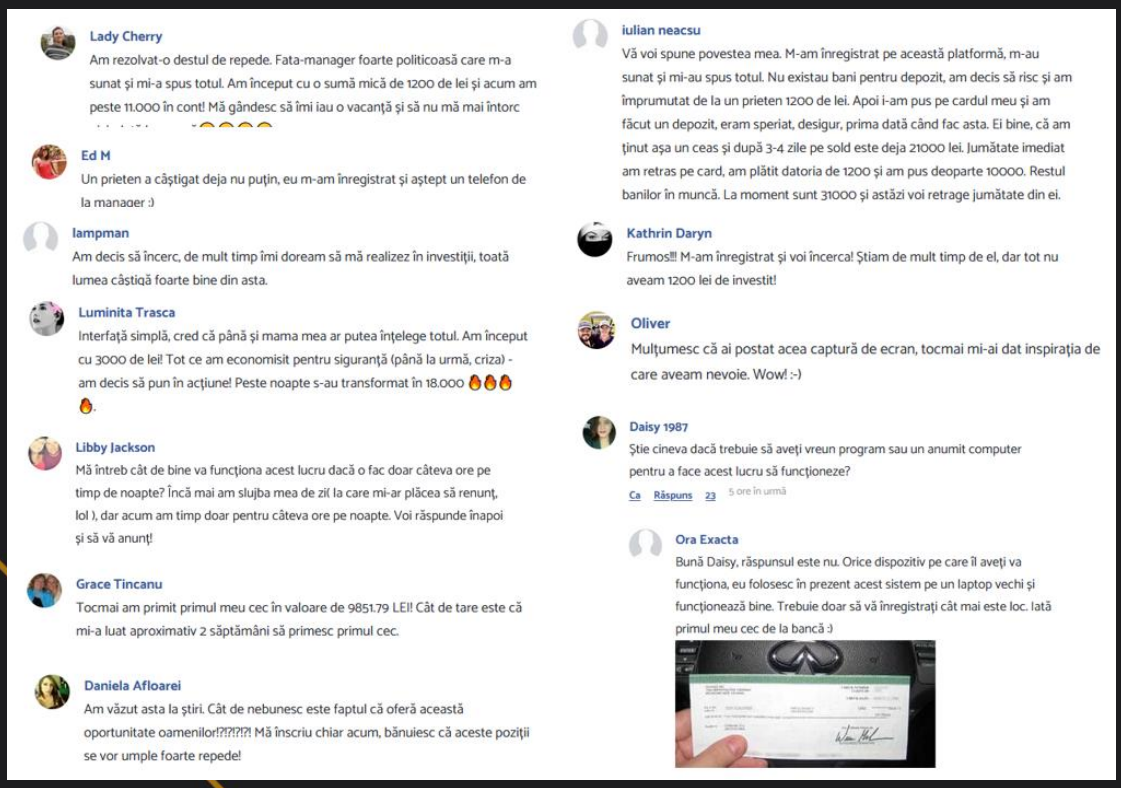


Utilizatorii neglijenți sau lipsiți de educație cibernetică vor intra în scenariile create de atacatori și vor juca rolul victimei, deoarece aceștia ajung în această poziție prin acceptarea manipulării vizuale. În general manipularea se face prin trimiterea de mesaje de informare/ avertizare și este menționată o limită temporară, care are rolul de a scoate utilizatorul din starea sa de confort, detaliu care îl va face să nu acorde importanță detaliilor.

Utilizatorul ajuns pe pagina falsă este întâmpinat de o avalanșă de imagini și texte care susțin scenariul fraudei, dar conțin și declarații false ale unor persoane care susțin că deja sunt parte din acea afacere, au cumpărat produsul sau au investit în acțiuni, iar rezultatele sunt cele descrise de administratorii paginilor false.

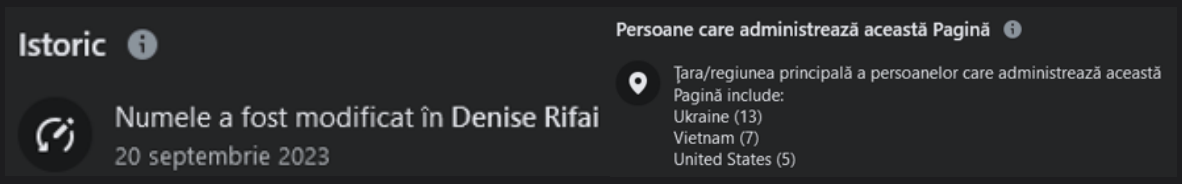
Ingineria socială are un rol important.

Comentariile false cuprind o multitudine de situații încât să acopere o scară largă de utilizatori ai tehnologiei, dornici de a câștiga bani sau comentarii adaptate la scopul final al fraudei/ înșelătoriei.

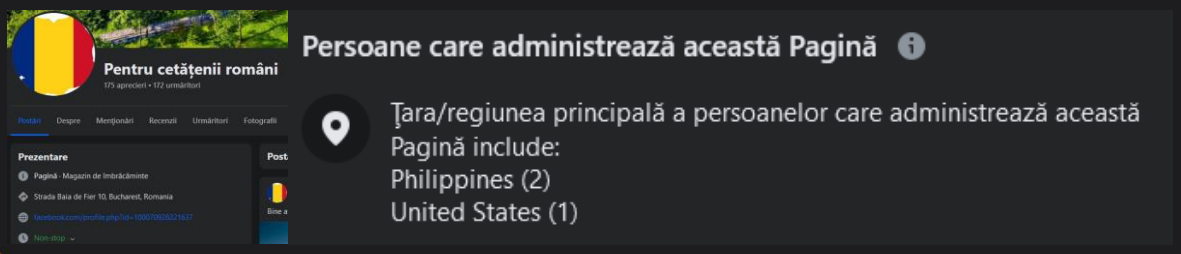


- *Ajutor tehnic pentru cei care nu se pricep*, dar ar vrea,
- *A câștigat un "prieten"* - Deci este ceva testat,
- *Aplicație ușor de utilizat "încât și mama ar putea..."* – Includere nepricepuți și persoane vârstnice,
- *Renunțare la job pentru câștigurile mari* – Dacă ăla poate, hai să încerc și eu..
- *"Tocmai am primit primul meu cec..."* – "Garantarea" câștigurilor,
- *"Am văzut asta la știri"* – Este ceva spus la TV, deci e de bine...
- *"aceste poziții se vor umple repede..."* – Repede că poate nu mai apucăm toți..
- *"nu au existat bani... am împrumutat"* – Convingerea celor care nu au bani, dar ar putea împrumuta..
- *"am făcut un depozit, eram speriat, era prima data..."* – Eliminarea subtilă a îndoielilor și convingerea să încerce..
- .....etc.

Paginile generatoare de reclame frauduloase au parte de schimbări majore de imagine și în administrare.



Un exemplu de campanie phishing asupra utilizatorilor din România.
În perioada analizei contul avea generate 420 de reclame cu campania de fraudă, iar la o verificare actuală, contul indică un număr de 510 reclame generate, ultima rulând la data de 26 Octombrie 2023.



Starea actuală a paginii: Online, dar cu altă denumire...

... altă țară, alte ținte pentru fraudă.

Interesul infractorilor și scopul celor menționate este acela de a convinge utilizatorii să acceseze paginile false și să completeze un formular prin care oferă datele de contact, pentru ca responsabilul platformei să intre în contact cu ei.

Sau după caz, scopul înșelătoriei este de a îi convinge pe utilizatori să cumpere un produs sau un serviciu oferit de pagina falsă!

Analiza etapelor fraudei financiare

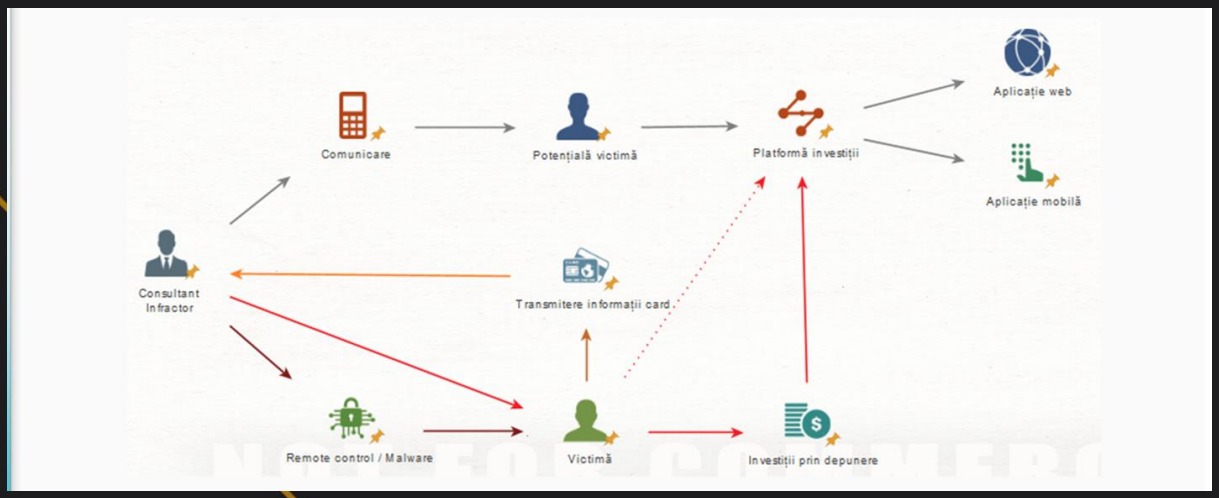
Datele de contact obținute de infractori sunt un pas important în procesul de fraudare, deoarece persoanele care au vizitat pagina falsă s-au înscris singure în lista de posibile victime.

În această etapă rolul cel mai important îl joacă Consultantul, infractorul care intră în legătura cu potențiala victimă, deoarece, prin inginerie socială, va face tot posibilul ca interlocutorul

său să creadă tot scenariul din jurul fraudei și să îl convingă că el este 100% un câștigător în această operațiune.

Menținând ca subiect principal frauda financiară prin intermediul investițiilor în cripto monede sau acțiuni ale unor companii de succes, trebuie înțeles că atacatorul va intra în contact cu utilizatori cu nivele diferite de educație, de pricepere în zona tehnică și vârstă. În urma investigațiilor s-a constatat că pierderile financiare au avut loc prin investiții directe ale utilizatorilor, prin trimiterea de fonduri către infractori, prin utilizarea unor aplicații false și prin utilizarea aplicațiilor de suport la distanță (remote control), oferind infractorilor acces la dispozitivele utilizatorilor pentru a îi ajuta la setările conturilor pe platformele false și chiar la utilizarea aplicațiilor bancare ale acestora.

Fluxul activităților desfășurate poate fi înțeles din imaginea de mai jos, dar tot odată se poate observa adaptabilitatea infractorilor la nivelul de pregătire a victimelor, uneori o parte din obiective să fie eliminate, deoarece aceștia ajung la bani fără a fi necesar un efort foarte mare.



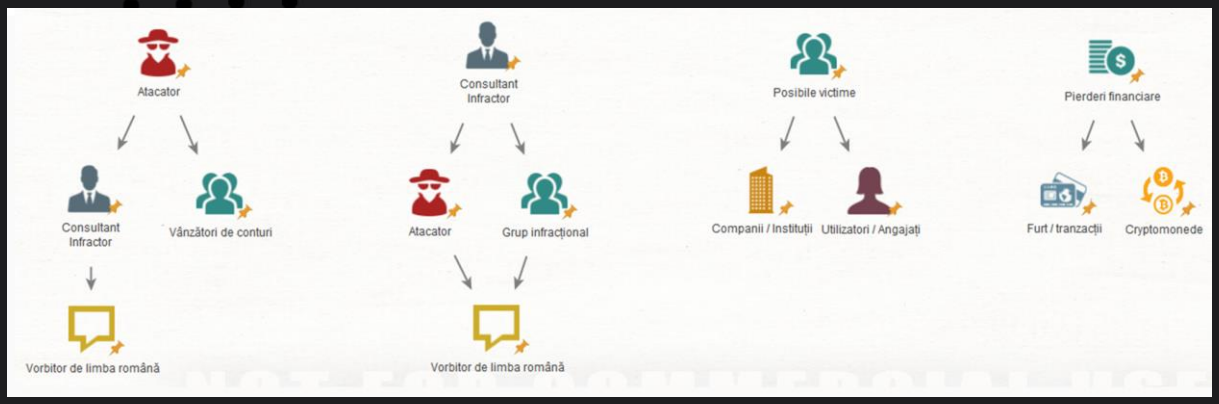
Concluzionând analizarea procesului de fraudare, avem o imagine clară a rolurilor infractorilor, a utilizatorilor și a pierderilor financiare.

Atacatorul inițial poate fi doar persoana care lansează campaniile de phishing/ malware, pentru obținerea datelor de acces și vânzarea acestora către infractorii care se vor ocupa de fraudă, pot fi parte din echipa de fraudare sau una și aceiași persoană cu consultantul care finalizează procesul de fraudă.

Consultantul poate fi, așa cum am menționat, chiar atacatorul inițial sau face parte dintr-un grup infracțional, în care fiecare are rolul său. Conform declarațiilor victimelor, infractorii sunt vorbitori de limbă română, de cele mai multe ori cu accent specific vorbitorilor de limbă rusă.

Posibilele victime sunt companiile/ instituțiile ale căror conturi au fost compromise și exploatate pentru crearea de reclame și utilizatorii implicați în fiecare etapă a scenariului de fraudare.

Victimele fraudei(investiții false) sunt utilizatorii dornici de câștiguri rapide, dar lipsiți de educație digitală, de educație cibernetică și persoane ușor de manipulat.



Pierderile financiare mari se datorează modalității de manipulare a victimei în procesul de investiții, infractorii aplicând tehnici de câștigare a încrederii victimei, dar se poate ajunge până la impunerea unor datorii către platforma de investiții și chiar amenințări pentru recuperarea soldurilor restante fictive.

5. Prevenire și Protecție pentru utilizatori

Semne de avertizare ale unei posibile fraude

Semnele de avertizare ale unei posibile fraude financiare sunt cruciale pentru a recunoaște și preveni căderea în capcanele infractorilor. Fiecare dintre aceste semne indică potențiale riscuri și necesită vigilență sporită din partea utilizatorilor:

a. Oferte cu randamente neobișnuit de ridicate:

În lumea investițiilor, o regulă generală este că randamentele mari vin de obicei cu riscuri pe măsură. Orice ofertă care promite profituri substanțiale fără un risc corespunzător este suspectă. Aceste oferte pot fi parte a unei scheme Ponzi sau a altor tipuri de escrocherii.

b. Presiunea de a acționa rapid:

Tactica de a crea urgență este des folosită pentru a împiedica potențialii investitori să analizeze oferta în mod critic. În aceste cazuri, infractorii pot susține că oportunitatea este "o dată în viață" sau că este necesară o acțiune imediată pentru a beneficia de condițiile oferite.

c. Solicitări pentru informații personale sau financiare:

Solicitările neașteptate de informații sensibile sunt un semn clar de fraudă. Infractorii pot folosi aceste date pentru a accesa conturi bancare, pentru furt de identitate sau alte activități ilegale. Orice solicitare de acest gen ar trebui tratată cu mare precauție.

d. Lipsa transparenței sau documentației neclare:

Ofertele legitime de investiții sunt de obicei transparente și însoțite de documentație clară și detaliată. Lipsa transparenței, documentația ambiguă sau neclară, sau reticența de a răspunde la întrebări specifice, sunt semne că ceva nu este în regulă.

e. Comunicare nesolicitată:

Email-urile, apelurile telefonice sau mesajele nesolicitate care oferă oportunități de investiții sau solicită informații personale trebuie tratate cu suspiciune. Aceste metode sunt adesea folosite în campaniile de phishing pentru a obține acces la informații confidențiale.

Recunoașterea acestor semne de avertizare este un pas crucial în protejarea împotriva fraudelor financiare. Este important ca utilizatorii să fie vigilenți, să pună întrebări și să efectueze cercetări amănunțite înainte de a lua orice decizie financiară. Prevenirea începe cu informarea și conștientizarea riscurilor.

Sfaturi de prevenire

Pentru a evita capcanele fraudelor financiare, este esențial să adoptați o abordare proactivă și informată în gestionarea finanțelor și a informațiilor personale. Iată câteva sfaturi detaliate de prevenire care vă pot ajuta să vă protejați:

a. Efectuați cercetări amănunțite:

- Verificarea sursei: Înainte de a investi, asigurați-vă că entitatea și oferta sunt legitime. Căutați informații despre companie și produsele sau serviciile sale.
- Consultarea reglementatorilor financiari: Verificați dacă entitatea este înregistrată sau reglementată de o autoritate financiară recunoscută.
- Solicitarea de sfaturi independente: Este întotdeauna util să obțineți o a doua opinie de la un consultant financiar independent, care poate evalua obiectiv oferta.
- Solicitare de sfaturi specializate: Cereți opinia unui specialist în securitate cibernetică atunci când există suspiciuni cu privire la paginile web sau platformele la care ați fost direcționați.

b. Protejați-vă informațiile personale:

- Vigilență în comunicare: Fiți extrem de precauți atunci când vi se solicită date personale sau financiare. Nu furnizați aceste informații prin canale nesigure sau persoanelor neautorizate.
- Protecția datelor: Utilizați tehnici de protecție a datelor, cum ar fi criptarea și stocarea securizată, pentru a păstra confidențialitatea informațiilor dvs. personale.

c. Folosiți practici de securitate online:

- Actualizarea software-ului: Asigurați-vă că sistemul de operare și aplicațiile sunt mereu actualizate pentru a proteja împotriva vulnerabilităților de securitate.

- Utilizarea autentificării duble/ multiple: Activează autentificarea multi-factor pe toate conturile importante pentru a adăuga un nivel suplimentar de securitate.

d. Evitați deciziile impulsive:

- Analiză și reflecție: Luați timp să evaluați fiecare oportunitate financiară și să cântăriți avantajele și dezavantajele. O decizie financiară bine gândită este întotdeauna mai sigură.
- Evitarea presiunii: Nu vă lăsați presați să luați decizii rapide, în special în situații de stres sau sub presiune.

e. Monitorizați-vă conturile financiare:

- Verificări regulate: Examinați regulat extrasele de cont și tranzacțiile pentru a identifica orice activitate suspectă sau neautorizată.
- Alerte de tranzacție: Setarea alertelor pentru tranzacții neobișnuite sau mari poate fi un mod eficient de a detecta rapid frauda.

Implementând aceste practici, veți putea crește nivelul de protecție împotriva potențialelor fraude financiare. Conștientizarea și educația continuă sunt esențiale în acest proces, deoarece metodele infractorilor se pot schimba și evolua. Fiți întotdeauna atenți la cele mai recente tactici de fraudă și adaptați-vă strategiile de securitate în consecință pentru a vă păstra finanțele în siguranță.

6. Rolul Instituțiilor Financiare

Măsuri de securitate și monitorizare

a. Sisteme Avansate de Detectare a Fraudei:

- Aceste sisteme utilizează algoritmi sofisticați și învățare automată pentru a identifica tranzacții neobișnuite sau suspecte, ajutând la detectarea timpurie a potențialelor fraude.
- Analiza comportamentală și modelarea riscului sunt de asemenea folosite pentru a evalua tiparele tranzacțiilor și pentru a identifica activități neobișnuite.

b. Securitatea Infrastructurii Tehnologice:

- Securizarea infrastructurii IT implică protejarea datelor clienților și a sistemelor bancare de atacurile cibernetice, utilizând tehnologii avansate de criptare și soluții de securitate robuste.
- Continua actualizare și întreținere a sistemelor IT sunt vitale pentru a rămâne un pas înaintea metodelor din ce în ce mai sofisticate ale infractorilor cibernetici.

c. Autentificare Multi-factor și Securitatea Conturilor:

- Implementarea autentificării multi-factor (MFA) asigură un nivel suplimentar de securitate, necesitând mai mult decât un simplu nume de utilizator și parolă pentru a accesa un cont.
- MFA poate include elemente cum ar fi coduri generate pe telefon, întrebări de securitate sau amprente digitale, sporind semnificativ securitatea conturilor online.

Educația clienților în domeniul securității cibernetice

Educația clienților în domeniul securității cibernetice este un aspect crucial în strategia instituțiilor financiare de a combate fraudele. Prin informarea și instruirea clienților, acestea pot reduce semnificativ riscul ca aceștia să devină victime ale activităților ilegale online.

a. Programe de Conștientizare a Securității:

- Materiale Educative: Oferirea de broșuri, ghiduri și alte materiale informative care explică diferite tipuri de fraude cibernetice, cum ar fi phishing, vishing, smishing și alte tehnici de inginerie socială.
- Exemple Reale și Studii de Caz: Prezentarea de cazuri reale de fraudă poate ajuta clienții să înțeleagă mai bine riscurile și să recunoască semnele de avertizare.

b. Comunicare Regulată cu Clienții:

- Buletine Informative: Trimiterea periodică a buletinelor informative care includ sfaturi de securitate, avertizări despre noi tipuri de fraude și recomandări pentru protecția online.
- Canale de Social Media: Utilizarea platformelor de social media pentru a răspândi conștientizare și pentru a atinge un public mai larg.

c. Instruirea Privind Siguranța Online:

- Webinarii și Workshop-uri: Organizarea de sesiuni educaționale online și evenimente unde experți în securitate cibernetică oferă sfaturi practice și răspund la întrebările clienților.
- Simulări și Teste: Implementarea de simulări de phishing pentru a-i învăța pe clienți cum să identifice email-uri și mesaje suspecte.

d. Asistență pentru Clienți:

- Linii de Asistență: Oferirea unei linii telefonice dedicate unde clienții pot raporta incidente suspecte și pot primi asistență imediată.
- Consultanță Personalizată: Oferirea de sfaturi și asistență personalizată pentru clienții care au nevoie de ajutor în gestionarea securității conturilor lor online.

e. Actualizări și Avertizări de Securitate:

- Notificări de Securitate: Trimiterea de alerte prin email sau mesaje text atunci când se detectează activități suspecte pe contul clientului sau când apar noi amenințări.
- Informații Actualizate: Menținerea unei secțiuni pe site-ul web al băncii cu ultimele noutăți și sfaturi în domeniul securității cibernetice.

Prin intermediul acestor măsuri, instituțiile financiare nu numai că își protejează propriile resurse, dar și contribuie la crearea unui mediu financiar mai sigur pentru toți utilizatorii. Educația și cooperarea continuă cu clienții, alături de implementarea celor mai noi tehnologii de securitate, sunt esențiale în lupta împotriva fraudelor financiare. Această abordare combinată ajută la consolidarea încrederii în sistemul financiar și la protejarea eficientă a activelor clienților împotriva amenințărilor cibernetice.

Astfel, rolul instituțiilor financiare este crucial nu doar în gestionarea eficientă a finanțelor, ci și în asigurarea unui mediu sigur și protejat pentru tranzacții financiare în era digitală. Prin colaborarea strânsă cu autoritățile de reglementare, alte instituții și clienții, acestea pot continua să îmbunătățească mecanismele de apărare împotriva fraudelor financiare sofisticate.

7. Planul de Răspuns în Caz de Compromitere

Acțiuni imediate după detectarea fraudei

a. Notificarea instituțiilor financiare:

Contactați imediat banca sau instituția financiară implicată. Anularea sau blocarea imediată a oricăror carduri de credit/debit și a accesului online la conturi este crucială pentru a preveni pierderi suplimentare.

b. Schimbarea datelor de autentificare:

Modificați parolele și detaliile de securitate pentru toate conturile online afectate. Acest lucru include conturile de email, platformele de social media și orice alt serviciu online asociat.

c. Raportarea la autoritățile competente:

Raportați frauda la Poliție, Directoratul Național de Securitate Cibernetică și la alte autorități relevante, cum ar fi autoritatea națională de supraveghere a fraudelor financiare. Aceasta poate ajuta la investigarea și prevenirea altor cazuri similare.

d. Monitorizarea creditului:

În cazul furtului de identitate, este important să monitorizați rapoartele de credit pentru orice activitate neautorizată. Pot fi luate în considerare serviciile de monitorizare a creditului pentru a alerta despre orice schimbare suspectă.

Recuperarea pierderilor și securizarea conturilor

a. Păstrarea dovezilor:

Salvați toate discuțiile, documentele, adrese de email, numere de telefon ale persoanelor cu care ați interacționat.
A se evita ștergerea aplicațiilor instalate sau formatarea dispozitivelor implicate în incident.

Informațiile pot ajuta la identificarea modalității prin care s-a realizat frauda, dar și a identității infractorilor.

b. Revizuirea tranzacțiilor:

Examinați toate tranzacțiile recente pentru a identifica orice activitate neautorizată. Acest lucru va ajuta la determinarea nivelului de compromitere.

c. Documentarea și raportarea detaliată a incidentului:

Păstrați o înregistrare detaliată a tuturor comunicațiilor și acțiunilor întreprinse după detectarea fraudei. Aceasta include orice plângere/ denunț la poliție, corespondența cu banca și schimbările de securitate efectuate.

d. Consultarea cu un expert financiar sau juridic:

În cazuri complexe, poate fi util să consultați un expert financiar sau juridic pentru a vă ghida în procesul de recuperare a pierderilor și de protejare a drepturilor.

e. Reevaluarea măsurilor de securitate:

Revizuiți și îmbunătățiți practicile de securitate pentru a preveni incidente similare în viitor. Acest lucru poate include investiții în soluții de securitate mai avansate, revizuirea politicilor de securitate și sensibilizarea sporită în ceea ce privește protecția datelor.

8. Concluzie

Importanța conștientizării și prevenției

Conștientizarea și prevenția sunt esențiale în lupta împotriva fraudelor financiare. Într-o lume tot mai digitalizată, unde tranzacțiile financiare se desfășoară în mare parte online, potențialul pentru activități ilegale se amplifică. Prin urmare, este crucial ca atât indivizii, cât și instituțiile financiare, să fie bine informați și să adopte măsuri proactive pentru a se proteja împotriva acestor amenințări.

Rolul Conștientizării:

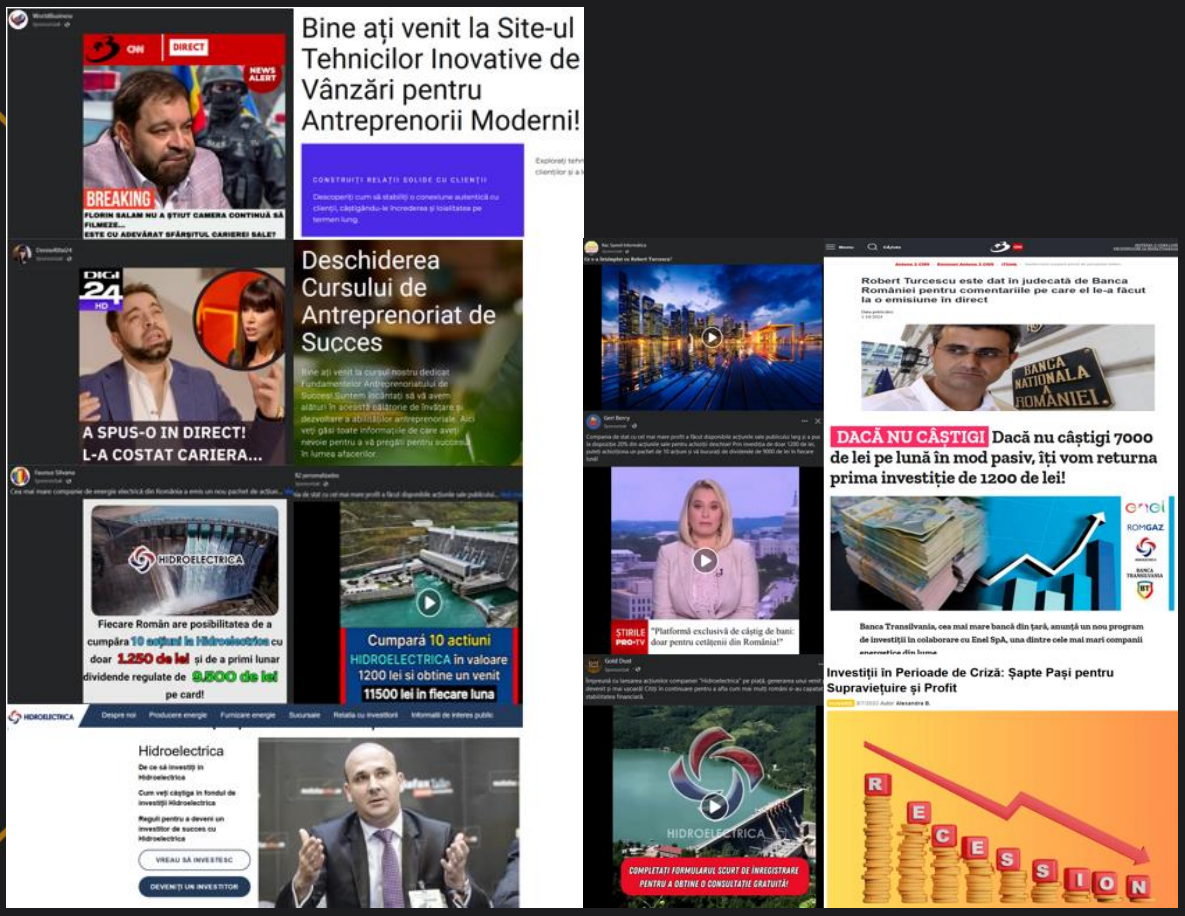
- **Educația:** A fi bine informat despre diferitele tipuri de fraude financiare și semnele lor de avertizare poate face diferența între a fi o victimă și a preveni un atac. Educația continuă este vitală pentru a ține pasul cu metodele în continuă schimbare ale infractorilor.
- **Partajarea informațiilor:** Diseminarea cunoștințelor și experiențelor personale referitoare la fraudele financiare în comunități poate ajuta la creșterea conștientizării generale și la protejarea altora.

Importanța Prevenției:

- **Măsuri de securitate:** Implementarea de măsuri de securitate robuste, atât la nivel personal, cât și instituțional, este esențială pentru a bloca accesul infractorilor la informații și resurse financiare.
- **Vigilență continuă:** Menținerea unei atitudini de vigilență și revizuirea periodică a practicilor de securitate asigură că suntem mereu un pas înaintea infractorilor.

Într-un final, prevenirea și combaterea fraudelor financiare este o responsabilitate comună. Prin colaborarea dintre consumatori, instituții financiare și autoritățile de reglementare, putem construi un mediu financiar mai sigur și mai protejat. Conștientizarea riscurilor și adoptarea unor măsuri proactive de securitate nu sunt doar o protecție împotriva pierderilor financiare, ci și un pas esențial către menținerea unei societăți digitale sigure și încrezătoare.

9. Bonus: Campanii de fraudă în derulare



Surse și lecturi suplimentare

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

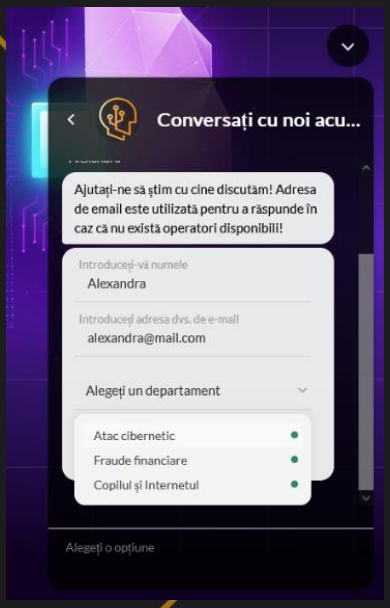
Phishing-ul bancar – **Siguranța Online**
https://sigurantaonline.ro/phishing-ul-bancar/

Articole securitate cibernetică – **Prodefence**
https://www.prodefence.ro/articole-securitate-cibernetica/

Identificarea fraudelor din mediul online – **DNSC**
https://www.dnsc.ro/cautare?ceCaut=frauda

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

Edcuație cibernetică – Părinți și Copii – **Prodefence**
https://www.youtube.com/@AlexandruAnghelus/videos



Cyber Chat

Înainte de a trimite datele personale sau banii către un necunoscut, mai bine cere părerea unor specialiști. Este gratis și te pot ajuta să nu iei decizii greșite!

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

”Spui că totul este o minciună și că toți sunt hoți, dar același TU oferi toate datele personale și banii unei persoane care ți-a spus povești prin SMS sau la telefon”

ProDefence

Cyber Security Services