



Siguranța în lumea digitală



Prevenirea fraudelor online, securitatea tranzacțiilor cu cardul,
protecția datelor personale bancare

Proiect instituțional

Creșterea cunoștințelor și abilităților financiare în rândul
tinerilor din România

2026



Cuprins

1. Definirea fraudelor financiare online	▶	3
2. Clasificări oficiale ale fraudelor financiare online	▶	4
3. Tipologii de fraude frecvente în România	▶	5
3.1. Phishing		6
3.2. Investment Scam		8
3.3. Spoofing		11
3.3. Deepfake		13
3.3. Online Shopping Platforms Fraud		14
4. Cum să identifici și să eviți înșelătoriile și fraudele comune pe internet	▶	15
Bibliografie	▶	22

Disclaimer:Într-un mediu online tot mai plin de provocări, unde amenințările cibernetice evoluează constant, să știi cum să identifici și să previi fraudele este pasul cel mai important pentru protejarea economiilor tale. Ghidul de față îți pune la dispoziție cunoștințele esențiale pentru a-ți crea o protecție digitală eficientă. Un management financiar responsabil începe întotdeauna cu siguranța banilor tăi. Facultatea de Finanțe, Asigurări, Bănci și Burse de Valori te îndeamnă să rămâi atent și să anunți fără întârziere orice tentativă suspectă. Verifică mereu canalele oficiale înainte de a furniza date confidențiale sau de a accesa linkuri neobișnuite. Deoarece recomandările se pot actualiza în timp, îți sugerăm să reconsulți periodic informațiile oficiale.

1. Definirea fraudelor financiare online

Frauda financiară în mediul online include toate acțiunile intenționate prin care infractorii folosesc tehnologia, rețelele de comunicații și infrastructurile digitale pentru a înșela victimele, cu scopul de a obține profituri ilicite sau de a cauza pagube materiale persoanelor fizice și companiilor. Această infracțiune are un caracter hibrid: combină metode tehnice (exploatarea breșelor de securitate din programe sau echipamente, interceptarea datelor și manipularea sistemelor) cu ingineria socială, care speculează încrederea, neatenția sau lipsa de cunoștințe ale utilizatorilor.

În general, o fraudă financiară online se bazează pe trei piloni principali:

1. **Canalul tehnologic:** rețelele de internet și de telefonie, platformele bancare, site-urile de e-commerce, aplicațiile mobile și dispozitivele folosite (telefoane, PC-uri, tablete).
2. **Tinta economică:** banii, criptomonede, datele bancare confidențiale (carduri, coduri PIN, parole, coduri de autentificare) și mijloacele de plată electronice.
3. **Mecanismul de atac:** metode precum phishing-ul, programele de tip malware, preluarea ilegală a conturilor, falsificarea tranzacțiilor sau preluarea controlului de la distanță asupra dispozitivelor.

Elementul definitoriu al acestor fraude este mutarea activității infracționale în spațiul virtual. Deoarece atacatorii nu mai sunt limitați de o locație fizică și pot acționa de oriunde din lume, identificarea și tragerea lor la răspundere devin dificile. În plus, caracterul lor transfrontalier depășește adesea cadrul legislațiilor naționale, făcând cooperarea internațională crucială pentru prevenție și anchete.

Din punct de vedere juridic, aceste fapte se încadrează atât la criminalitate informatică, cât și la infracțiuni economico-financiare. Ele sunt reglementate prin legislația națională (Codul Penal, Legea 161/2003) și prin Directive europene sau tratate internaționale (Directiva (UE) 2013/40, Directiva (UE) 2019/713, Convenția de la Budapesta). Impactul lor este dublu: pe de o parte, provoacă pierderi financiare directe victimelor, iar pe de altă parte, slăbesc încrederea publicului în plățile digitale, afectând stabilitatea economică și securitatea cibernetică pe termen lung.

2. Clasificări oficiale ale fraudelor financiare online

O analiză comparativă relevă faptul că tipologiile naționale tind să fie mai pragmatice și strâns aliniată cu realitățile locale, concentrându-se pe amenințările predominante specifice unui anumit mediu socio-economic. În schimb, tipologiile europene adoptă o perspectivă mai largă, care încorporează scenarii și fenomene complexe cu dimensiuni geopolitice semnificative.

Integrarea acestor două perspective distincte, dar complementare, într-un cadru analitic unificat nu numai că sporește acuratețea clasificării fraudelor financiare online, dar consolidează și cooperarea transfrontalieră în combaterea acestor infracțiuni insidioase. Prin armonizarea eforturilor și partajarea informațiilor, națiunile se pot pregăti mai bine pentru a aborda natura din ce în ce mai sofisticată a fraudei financiare online și provocările reprezentate de operațiunile sale transnaționale.

După metoda de comitere (criteriu tehnic)

- **Phishing** – transmiterea de e-mailuri sau mesaje înșelătoare, aparent provenite de la bănci sau platforme de plăți, cu scopul colectării datelor bancare.
- **Vishing și smishing** – obținerea de informații confidențiale prin apeluri telefonice sau mesaje SMS frauduloase.
- **Pharming** – redirectionarea utilizatorilor către site-uri false prin compromiterea serverelor DNS.
- **Malware financiar** – troieni bancari, keyloggere, ransomware cu componentă de furt de date financiare.
- **Compromiterea e-mailului de afaceri** (Business Email Compromise – BEC)
– interceptarea și falsificarea corespondenței comerciale pentru deturnarea plăților



După scopul urmărit

- **Obținere directă de fonduri** – transferuri neautorizate din conturile victimei.
- **Obținere indirectă de fonduri** – revânzarea datelor financiare pe piețe ilegale.
- **Facilitarea spălării banilor** – tranzacții succesive prin platforme fintech sau criptomonede.

După categoria victimei

- **Fraude B2B** – atacuri asupra infrastructurii de plăți și facturare ale companiilor.
- **Fraude B2C** – înșelarea consumatorilor prin platforme false de comerț online.
- **Fraude C2C** – anunțuri înșelătoare pe platforme de tip marketplace

3. Tipologii de fraude frecvente în România

În prezent, fraudă cibernetică a depășit stadiul unor incidente izolate, transformându-se într-un fenomen complex, susținut de rețele infracționale globale bine structurate. Aceste grupări specializate folosesc un mix avansat de instrumente tehnice și tactici psihologice pentru a-și pune în aplicare atacurile.

Infractorii combină exploatarea breșelor din sisteme – cum ar fi erorile software, parolele slabe sau conexiunile nesigure – cu ingineria socială. Această metodă dublă le permite să manipuleze comportamentul uman, determinând victimele să ofere involuntar date confidențiale sau să facă acțiuni care le compromit siguranța. Mai mult, atacatorii se adaptează rapid la noile tehnologii și la schimbările de comportament ale utilizatorilor, ceea ce face detectarea și prevenirea fraudei tot mai dificile.

Înțelegerea acestor mecanisme este un pas esențial pentru crearea unor măsuri de protecție eficiente și pentru consolidarea securității digitale, atât la nivel individual, cât și organizațional.



3.1. Phishing

Phishing-ul reprezintă o formă de fraudă informatică bazată pe transmiterea de comunicări electronice (e-mail, SMS, mesaje în aplicații) care imită surse legitime, cu scopul obținerii de date sensibile (parole, coduri PIN, date card bancar, informații personale). În esență, acest tip de atac combină ingineria socială cu exploatarea tehnologică pentru a compromite securitatea datelor financiare ale victimei.

Indiferent de scenariul folosit, atacurile de tip phishing urmează de regulă aceeași structură:

- Crearea identității false – imitarea identității unei bănci sau instituții financiare;
- Transmiterea mesajului fraudulos – prin canale electronice;
- Inducerea stării de urgență sau frică – pentru a stimula acțiunea rapidă și necriticată;
- Redirecționarea victimei către un mediu controlat de atacator – site clonat sau formular fals;
- Colectarea datelor – stocarea credentialelor în baze de date ilicite;
- Exploatarea datelor – tranzacții frauduloase, vânzarea pe dark web, contractarea de credite.

Scenarii concrete

A. Transmiterea de link-uri în numele băncii pentru actualizarea datelor bancare

Tehnici și instrumente utilizate:

- **Falsificarea expeditorului** (E-mail Spoofing): Atacatorul maschează adresa reală modificând câmpul „De la” (From). Chiar dacă la prima vedere apare un nume legitim (ex: Banca Ta suport@banca.ro), verificarea antetului (header-ului) tehnic va arăta adevăratul expeditor, cum ar fi server123@hosting-dubios.com.
- **Kituri de Phishing** (Pachete de clonare): Reprezintă site-uri gata făcute („la cheie”). Infractorii descarcă arhive cu pagini web ce le imită perfect pe cele ale băncii. Singura diferență este că formularul de autentificare reorienta datele introduse direct către atacator (pe e-mail sau într-o bază de date privată), în loc să te conecteze în cont.

- **Certificate de securitate înșelătoare (SSL/TLS):** Prezența „lacătului” în bara de adrese indică doar o conexiune criptată, nu și faptul că site-ul este de încredere. Atacatorii generează ușor certificate gratuite (ex: Let's Encrypt) pentru site-urile lor clonă, creând o falsă senzație de siguranță.
- **Manipularea psihologică:** Se bazează pe inducerea stării de urgență și pe invocarea autorității. Mesajele de tipul „Contul va fi blocat în 24 de ore dacă nu vă reconfirmați datele” sunt concepute deliberat pentru a declanșa o reacție de panică, determinând victima să acționeze rapid și fără să mai verifice detaliile.

B. Mesaj de informare privind efectuarea unei plăți cu cardul victimei și necesitatea confirmării

Tehnici și instrumente utilizate:

- **Triggerul emoțional al panicii:** Folosirea unor expresii alarmante, cum ar fi „Tranzacție suspectă detectată”. Mesajele nu oferă răgaz — ele utilizează termeni precum „Acum”, „Imediat” sau „În așteptare” pentru a bloca gândirea analitică a victimei.
- **Mesaje text capcană (Smishing):** Trimiterea prin SMS a unor linkuri scurtate care redirectionează către pagini de phishing create special pentru dispozitive mobile.
- **Interfețe mobile simulate:** Pagini web clonă care imită la pixeli aplicațiile bancare oficiale pentru a păcăli utilizatorul.
- **Servere de redirectionare:** Infrastructură tehnică utilizată de atacatori pentru a-și masca adevărata identitate și locație.
- **Mecanismul psihologic din spate:** Inducerea unei stări artificiale de urgență, care determină victima să reacționeze impulsiv și să omită verificările de securitate.



Tip Mesaj	Textul Exemplu (Simulat)	Analiza Tacticii
Urgență Bancară	"INFO [Banca Ta]: O plată de 2.450 RON către 'eMAG' este în așteptare. Dacă nu ați autorizat tranzacția, anulați aici: https://bit.ly/check-secure-ro "	Folosește numele unei bănci cunoscute și o sumă mare pentru a provoca panică imediată.
Securitate Cont	"Alertă Securitate: Un dispozitiv nou s-a conectat la contul dvs. din Moscova. Dacă nu sunteți dvs., securizați contul acum: https://banca-suport.net/login "	Combină frica de acces neautorizat cu locații geografice suspecte.
Verificare Card	"[CardControl]: Cardul dvs. a fost blocat temporar din motive de securitate. Pentru deblocare, confirmați ultimele 4 cifre aici: https://verificare-card.com "	Creează un inconvenient major (card blocat) pentru a forța utilizatorul să dea click.

3.2. Investment Scam

Frauda de tip Investment Scam presupune manipularea victimelor pentru a direcționa capital către oportunități financiare inexistente, prezentate eronat ca având rentabilitate ridicată și risc redus. Obiectivul final este deturnarea fondurilor către conturile atacatorilor. Din punct de vedere operațional, schema se bazează pe promovare cibernetică agresivă și pe utilizarea software-urilor de acces de la distanță pentru preluarea controlului asupra dispozitivelor. Frauda de tip Investment Scam demonstrează o integrare sofisticată între tehnologiile de marketing online, instrumentele de control la distanță și exploatarea directă a infrastructurii bancare personale a victimei. Abordarea tehnico-psihologică hibridă crește considerabil rata de succes a atacurilor.

Etapele tipice se caracterizeaza prin:

A. Identificarea și atragerea victimei

- Anunțuri plătite pe rețelele sociale (Facebook, Instagram, LinkedIn, TikTok): Reclame optimizate prin targetare avansată (microtargeting) pentru a atrage direct utilizatorii interesați de domenii precum investițiile sau educația financiară.
- Pagini de destinație (landing pages) clonate: Site-uri web care copiază fidel aspectul unor platforme reale de tranzacționare sau al unor portaluri financiare de încredere.
- Recenzii și mărturii false: Utilizarea de texte, imagini sau videoclipuri fabricate (cu presupuși „investitori de succes”) pentru a genera o falsă impresie de legitimitate și siguranță.

B. Contactul direct cu victima

- Apeluri de la agenți falși (de tip boiler room): Apeluri telefonice de la Operatori instruiți care folosesc scenarii bine puse la punct (scripturi) pentru a câștiga rapid încrederea victimei.
- Falsificarea numărului de telefon (Call Spoofing): Tehnică prin care atacatorii maschează identitatea apelantului, făcând ca pe ecranul telefonului să apară numărul unei instituții bancare sau al unei autorități legitime.
- Persuasiune și manipulare psihologică: Infracții se recomandă drept „consultanți financiari” sau „experți în investiții”, apelând la tactici de manipulare bazate pe autoritate, urgență și simularea unei atenții personalizate.



Cum să identifici un "Boiler Room Agent"

- Garantarea profitului: „Nu există risc, pierderea este imposibilă.” (În realitate, orice investiție are risc).
- Izolarea victimei: „Nu spuneți nimănui de această ofertă, este confidențială/doar pentru clienți VIP.”
- Presiunea pe timp: „Trebuie să decidem acum, altfel prețul crește.”
- Instalarea de software Solicitarea de a instala programe de control de la distanță (AnyDesk, TeamViewer).

C. Solicitarea instalării aplicațiilor de control la distanță

- Utilizarea abuzivă a aplicațiilor legitime de control la distanță: Folosirea unor programe oficiale precum AnyDesk, TeamViewer sau RemotePC, prezentate fals victimei ca fiind instrumente de „asistență tehnică” pentru configurarea investiției.
- Manipularea pentru obținerea de acces total: Tehnici de inginerie socială prin care victima este determinată să acorde permisiuni extinse pe dispozitiv (control asupra ecranului, tastaturii, fișierelor și notificărilor).
- Mascarea intențiilor reale: Atacatorii justifică instalarea aplicațiilor susținând că este un pas obligatoriu pentru „a te ghida pas cu pas” în deschiderea contului de tranzacționare.



Semne de alarmă clare (Red Flags)

- Orice solicitare de a instala AnyDesk, TeamViewer sau RustDesk venită de la o persoană necunoscută (indiferent cât de politicoasă/profesionistă sună).
- Solicitarea de a te loga în aplicația bancară în timp ce ai o sesiune de control la distanță activă.
- Insistența de a acorda permisiuni de "Accessibility" sau "Screen Recording" pe telefon.



3.3. Spoofing

Spoofing-ul reprezintă falsificarea intenționată a atributelor de identificare ale unui canal de comunicație (IP, adresă e-mail, număr telefonic) pentru simularea unei surse de încredere. În fraudele din sectorul bancar, manipularea identității apelantului (caller ID spoofing) este utilizată pentru a afișa numărul de contact oficial al unei entități financiare sau publice, vizând extragerea de date sensibile sau autorizarea de tranzacții ilicite.

A. Obținerea și utilizarea tehnologiilor de falsificare a identității apelantului

- Servicii de telefonie prin internet (VoIP) cu opțiune de modificare a identității: Platforme operate adesea din țări cu o legislație permisivă, ce permit schimbarea numărului afișat pe ecranul destinatarului (Caller ID).
- Instrumente dedicate falsificării apelurilor: Platforme și aplicații specializate (de tip spoofing) prin care atacatorii pot introduce manual orice număr de telefon doresc să apară pe ecranul victimei.
- Preluarea ilegală a numărului de telefon (SIM Swap): În scenarii mai avansate, infractorii reușesc să poarte sau să transfere fraudulos numărul real al victimei pe o altă cartelă SIM, preluând astfel controlul asupra apelurilor și mesajelor acesteia.

B. Impersonarea instituțiilor de încredere

1. Usurparea identității serviciului Call Center al unei bănci

- Falsificarea numărului oficial: Atacatorul apelează de pe numărul real al băncii și susține că datele de acces au fost compromise, cerând „validarea” lor de urgență.
- Scenarii conversaționale complexe: Folosirea unor scenarii bine pregătite, în care atacatorii introduc date reale ale clientului (obținute anterior din scurgeri de date) pentru a elimina orice suspiciune.

2. Usurparea identității Băncii Naționale a României (BNR)

- Pretextul contramăsurilor financiare: Apelantul susține că reprezintă BNR și că încearcă să „protejeze” victima prin blocarea unui presupus credit ilegal deschis pe numele ei.
- Tactica falsei autorități: Atacatorii se recomandă cu numele unor angajați reali ai BNR și invocă legi sau reglementări fictive pentru a părea pe deplin legitimi.

3. Usurparea identității Poliției

- Invocarea unei anchete penale: Apelul apare ca provenind de la o secție oficială de poliție. Victima este informată că datele i-au fost furate și i se cere să retragă de urgență banii (inclusiv din credite rapide) și să-i depună într-un ATM Bitcoin pentru „siguranță”.
- Presiune psihologică și șantaj emoțional: Crearea unei stări extreme de urgență sub pretextul sprijinirii unei anchete secrete, impunând un termen limită strict pentru executarea ordinelor.

Strategii de apărare imediată

Regula „Închide și Sună Înapoi”: Dacă primești un apel de la „Bancă” sau „Poliție” care îți cere date sau transferuri, închide imediat. Caută numărul oficial pe site-ul lor și sună tu. Spoofing-ul funcționează doar pe apelurile primite, nu și pe cele efectuate de tine.

Verificarea Identității: Nicio instituție (BNR, Poliție, Bancă) nu îți va cere niciodată prin telefon:, Codul PIN sau codurile primite prin SMS, Să instalezi aplicații (AnyDesk), Să transferi bani în „conturi de siguranță”.

Protecție SIM Swap: Dacă observi că telefonul tău își pierde brusc semnalul (scrie „No Service” sau „Emergency calls only”) fără un motiv clar, contactează imediat operatorul de telefonie de pe alt aparat și verifică dacă s-a solicitat o portare sau o înlocuire de SIM.



3.4. Deepfake

Frauda prin deepfake presupune utilizarea inteligenței artificiale generative și a rețelelor neuronale pentru a crea sau modifica imagini, clipuri video ori înregistrări audio extrem de realiste, dar complet false. În domeniul financiar, infractorii folosesc tehnologia deepfake pentru a impersona persoane publice, instituții sau branduri de încredere, oferind o falsă legitimitate unor scheme de investiții fictive destinate atragerii de bani.

1. Exploatarea imaginii persoanelor publice (politicieni, economiști, antreprenori)

- **Exemple de investiții fabricate:** Crearea de materiale video sau foto în care o personalitate pare că promovează oportunități financiare cu profituri mari. Aceasta se realizează prin:
 - Schimbarea feței și sincronizarea buzelor (face-swapping și lip-syncing): Tehnologii bazate pe modele AI generative (ex. DeepFaceLab, FaceSwap) care adaptează mimica pe un alt corp.
 - Clonarea vocală (voice cloning): Software-uri precum ElevenLabs sau Respeecher, utilizate pentru a sintetiza și imita fidel vocea și intonația persoanei reale.
- **Manipularea prin autoritate:** Atacatorii folosesc reputația și notorietatea unei figuri publice pentru a garanta în mod fals siguranța investiției.

2. Preluarea abuzivă a numelui și identității instituțiilor publice

- **Anunțuri oficiale contrafăcute:** Generarea de clipuri video deepfake în care reprezentanți reali sau fictivi ai unor ministere sau agenții de stat anunță oportunități „exclusive” de cumpărare de acțiuni, prin:
 - Generare video combinată: Suprapunerea chipului și vocii sintetizate pe un actor care citește un scenariu de înșelăciune.
 - Elemente vizual-grafice autentice: Utilizarea siglelor, a identității vizuale și a elementelor grafice originale preluate direct de pe site-urile oficiale pentru a păcăli privitorul.

3.5. Online Shopping Platforms Fraud

Frauda pe platformele de cumpărături online (Online Shopping Platforms Fraud) include toate practicile ilegale derulate pe site-uri de comerț electronic, platforme de anunțuri sau rețele sociale, prin care cumpărătorii ori vânzătorii sunt înșelați pentru a obține bani de la aceștia. În general, această schemă speculează încrederea în plățile și tranzacțiile online, creând iluzia unei vânzări sau achiziții complet legitime.

Ca mecanism al fraudei, infractorul postează anunțuri extrem de atractive, cu prețuri mult sub nivelul pieței, pentru a grăbi decizia de cumpărare. Odată ce primește banii (integral sau ca avans), acesta întrerupe orice contact și nu mai trimite produsul.

Tehnicile folosite frecvent constau în:

- Profiluri sau conturi false create pe platforme populare (cum ar fi OLX, eMAG Marketplace sau eBay).
- Imagini și descrieri preluate direct din anunțuri reale ale altor vânzători.
- Canale de comunicare greu de depistat, precum adrese de e-mail temporare și numere de telefon virtuale (VoIP).



Ce să faci dacă ai introdus deja datele cardului?

- Blochează cardul imediat din aplicația bancară.
- Contactează banca pentru a raporta fraudă și a solicita un card nou.
- Depune plângere la Poliție (chiar și online pe portalul Poliției Române), oferind dovezi: capturi de ecran cu conversația, link-ul fraudulos și dovada tranzacției.

4. Cum să identifici și să eviți înșelătoriile și fraudele comune pe internet

Din fericire, vă puteți proteja informațiile personale printr-o abordare proactivă a securității cibernetice. Vigilența vă protejează de criminalitatea informatică, însă ar trebui să fiți pregătiți să acționați rapid dacă informațiile vă sunt furate. Suntem aici să vă ajutăm — ghidul nostru cuprinzător pentru securitatea cibernetică personală vă poate pregăti să vă protejați împotriva înșelătoriilor și a fraudelor sau să vă recuperați după acestea.

Preluarea controlului asupra contului (Account hijacking)

Preluarea controlului asupra contului (account hijacking) înseamnă că un hoț de identitate obține datele tale de autentificare pentru un cont de rețele sociale, e-mail sau banking online. Printre alte consecințe posibile, atacatorul ar putea folosi contul furat pentru a pune victima într-o lumină proastă, pentru a-i fura banii sau pentru a se da drept victimă cu scopul de a înșela o altă persoană care are un cont cu o valoare mai mare.

Ultimul deceniu a fost marcat de breșe de date de profil înalt:

- În 2023, T-Mobile a suferit două breșe de date care au afectat 37 de milioane de clienți.
- Din 2019 până în 2023, Facebook a expus peste 540 de milioane de înregistrări ale utilizatorilor.

Cu alte cuvinte, este foarte probabil ca unele dintre informațiile tale personale să fi fost deja expuse. Este important să îți iei măsuri de precauție pentru a împiedica pe cineva să obțină suficiente informații suplimentare pentru a-ți accesa conturile.

Cum să îl identifici?

- Cineva pe care îl cunoști te contactează cu o ofertă „prea frumoasă ca să fie adevărată”.
- Cineva pe care îl cunoști te contactează de pe un număr de telefon ciudat.
- Cineva pe care îl cunoști începe să posteze oferte ciudate pe rețelele sociale.



Cum să îl eviți?

- Actualizează-ți regulat parolele, folosește autentificarea cu doi factori (2FA) și protejează-ți traficul web cu o rețea privată virtuală (VPN). În plus, asigură-te că toate parolele tale — sau, și mai bine, frazele de acces (passphrases) — sunt unice pentru diferitele tale conturi. Automatizarea a facilitat testarea datelor de autentificare de către infractori pe diferite site-uri, așa că, dacă repeți parolele, odată ce un cont este compromis, și celelalte ar putea fi.
- Dacă suspectezi că unul dintre conturile tale a fost accesat fără permisiunea ta și contactează imediat departamentul de asistență clienți al institutiei bancare.

Înșelătorii prin impersonare

Un fraudator pretinde că este cineva pe care îl cunoști, un reprezentant al guvernului sau un angajat al unei companii cu care ai putea avea relații de afaceri. Aceștia vor să te manipuleze pentru a trimite bani sau pentru a partaja informații personale. Pot falsifica numere de telefon sau adrese de e-mail pentru a părea legitimi. Ar putea încerca să preia controlul asupra computerului tău prin trimiterea unui link malițios sau să îți ceară să le trimiți bani prin card cadou (gift card) sau transfer bancar, ceea ce este ca și cum ai da bani gheață fraudatorului dacă ești victima unei astfel de înșelătorii, cel mai probabil nu îți vei recupera fondurile.



Cum să îl identifici?

- Susțin că sunt de la suportul tehnic și te sună în legătură cu o problemă la computerul tău.
- Trebuie să îi plătești sau să dai clic pe un link pe care ți-l trimit.
- Susțin că datorezi bani la ANAF.
- Tocmai ai câștigat un premiu la un concurs la care nu-ți amintești să fi participat, dar trebuie să plătești taxe pentru a primi premiul.
- Un prieten are probleme și are nevoie de ajutorul tău.
- Ai primit un transfer bancar cu o sumă prea mare și trebuie să trimiți înapoi diferența (o rambursare).



Cum să îl eviți?

- Nu trimite carduri cadou sau transferuri bancare către persoane pe care nu le cunoști.
- Nu trimite niciodată bani fără a verifica mai întâi cine te-a contactat, chiar dacă crezi că cunoști persoana respectivă sau dacă aceasta susține că este un prieten sau o rudă.
- Nu oferi informații personale persoanelor pe care nu le cunoști.
- Nu permite accesul la computerul tău persoanelor pe care nu le cunoști.

Înșelătoria „persoanei iubite” (Sweetheart scam)

O înșelătorie de tip „sweetheart” este un truc în care un fraudator folosește manipularea emoțională pentru a câștiga încrederea țintei sale. Folosind aplicații de întâlniri online și instrumente similare, fraudatorul își convinge ținta să trimită bani sau să partajeze informații personale.

Fiți, de asemenea, precauți cu privire la varianta cunoscută sub numele de „pig-butchering” (tăierea porcului). Aceasta începe de obicei cu un mesaj text sub pretextul contactării accidentale a unui număr greșit sau al încercării de a restabili legătura cu un vechi prieten. Fraudatorii încearcă să mențină ținta în conversație pentru a construi o relație (proces numit „îngrășarea porcului”) înainte de a introduce perspectiva unei oportunități de investiții lucrative, adesea prin criptomonede.



Cum să îl identifiți?

- O cunoștință din mediul online își declară sentimente puternice, deși nu v-ați întâlnit niciodată.
- Cineva pe care l-ai cunoscut online solicită un cec, un mandat poștal sau un transfer bancar.
- Cineva te contactează prin intermediul unui site de întâlniri, dar susține că locuiește în alt oraș sau în altă țară.
- Un străin are nevoie de ajutor urgent și/sau oferă un stimulent financiar.



Cum să îl eviți?

- Fii extrem de precaut cu privire la solicitările venite de la cineva pe care nu l-ai întâlnit niciodată, mai ales dacă nu aveți conexiuni comune. Acești fraudatori profită de dorința noastră de a fi prețuiți și de disponibilitatea noastră de a ajuta – este o înșelătorie extrem de eficientă și necesită un nivel ridicat de vigilență.
- Nu trimite niciodată bani unui străin pe care l-ai cunoscut online.
- Recunoaște faptul că fraudatorii de tip „sweetheart” vor încerca să te manipuleze emoțional.
- Vor pretinde că s-au îndrăgostit de tine, iar apoi vor cere bani pentru un scop care mizează pe simpatia ta.
- Scopul lor este să obțină cât mai mulți bani de la tine, fie treptat, fie pe toți deodată.

Phishing, vishing, smishing, quishing

Phishing-ul este o formă de inginerie socială în care fraudatorii folosesc e-mailul pentru a impersona o afacere sau o persoană de încredere, cu scopul de a păcăli sau intimida oamenii să ofere informații sensibile, să trimită bani sau să descarce malware. Mesajele de phishing sunt adesea trimise unui număr mare de persoane în același timp. O variantă mai direcționată se numește „spear phishing”, unde fraudatorii folosește ingineria socială și mesaje falsificate pentru a viza unul sau mai mulți indivizi dintr-o organizație specifică. De exemplu, aceștia ar putea simula un mesaj de la angajatorul țintei, cerându-i să furnizeze informații critice sau să efectueze o tranzacție financiară care ocolește procedurile normale.

Atunci când un fraudator folosește apeluri telefonice, procesul este cunoscut sub numele de phishing vocal sau „vishing”. În mod similar, tacticile de „smishing” folosesc mesaje SMS, iar „quishing-ul” folosește coduri QR care direcționează către site-uri web false sau malware. În toate formele sale, phishing-ul imită comunicările de la branduri, companii și persoane în care aveți încredere.



Cum să îl eviți?

- Scopul este de a te convinge să renunți la informațiile tale personale sau confidențiale prin crearea unui fals sentiment de urgență sau dorință. Acești fraudatori folosesc adesea frica, falsa autoritate sau alte manipulări emoționale pentru a te face să lași garda jos. Dacă ai îndoieli cu privire la un mesaj:
- Nu avea niciodată încredere într-o solicitare pentru parola ta – parola ta este doar pentru tine. O sursă legitimă nu va avea nevoie de parola ta, de un cod PIN și nici de numărul cardului tău de debit/credit pentru a accesa informațiile contului tău.
- Sună direct organizația, nu accesa niciun link din mesaj.
- Caută informații despre compania care a trimis comunicarea.
- Raportează incidentul la Directoratul Național de Securitate Cibernetică (DNSC)

Bani rapizi, câștiguri neașteptate și oferte „prea frumoase ca să fie adevărate”

Aceste mesaje promit bani neașteptați, adesea în schimbul unei taxe sau al unui impozit. Cea mai cunoscută variantă implică un prinț aflat în criză care solicită ajutor pentru a transfera fonduri în afara țării sale. Totuși, fraudatorii pot pretinde, de asemenea, că reprezintă concursuri cu premii în bani, programe de rabat sau moștenirea unor rude bogate. Scopul este să te momească pentru a furniza bani sau informații personale.

Unele variante moderne implică anunțuri pe site-uri de schimb online, cum ar fi Facebook Marketplace:

- Un vânzător oferă articole la un preț mult mai mic decât valoarea lor reală.
- Un potențial cumpărător se oferă să plătească mai mult în schimbul promisiunii de a i se rambursa acea diferență.
- Un anunț de închiriere în care „proprietarul” insistă că are nevoie de un transfer bancar pentru depozit înainte de a vă întâlni sau de a vizita locuința.



Cum să îl identifici?

- Cineva îți oferă bani în mod neașteptat.
- Primești un mesaj de la cineva cunoscut, dar de pe o adresă de e-mail sau un număr de telefon necunoscut.
- Cineva îți cere să depui un cec în numele său și îți oferă o parte din banii gheață.
- Un anunț online specifică faptul că „proprietarul” nu dorește să se întâlnească mai întâi și solicită un depozit.
- Un vânzător online dorește să îți „verifice” identitatea printr-un cod trimis prin Google Voice.



Cum să îl eviți?

Ar trebui să fi întotdeauna suspicios dacă un avocat, o bancă sau o companie te contactează oferindu-ți orice sumă de bani — chiar dacă oferta include documente care par oficiale. Dacă ești contactat, nu trimite bani și nu încerca să depui fonduri neverificate, mai ales dacă nu l-ai întâlnit niciodată pe expeditor. Un cec ar putea fi fals, iar un transfer printr-o aplicație de plăți s-ar putea dovedi fraudulos. Fondurile pot fi făcute disponibile inițial de către instituția ta financiară, dar dacă depunerea este ulterior anulată și banii sunt retrași din contul tău, vei pierde orice parte din acel depozit pe care ai retras-o sau ai cheltuit-o. Solicită sfatul unui avocat sau al unui consultant financiar dacă ai suspiciuni cu privire la o comunicare.

Mesaje de aprobare false

Un exemplu comun al acestei înșelătorii este cel în care atacatorii trimit notificări de aprobare false către consumatori, susținând că ținta a fost „pre-aprobată” pentru o linie de credit, un credit ipotecar sau un împrumut personal. Scopul este de a convinge ținta să furnizeze informații personale sau detalii despre conturile financiare pentru a accepta oferta.

Proaspeții absolvenți de facultate sunt adesea ținta ofertelor frauduloase de carduri de credit. Cumpărătorii de locuințe sunt vulnerabili la înșelătorii imobiliare. În mod similar, atacatorii pot pretinde că sunt companii de asigurări care oferă scutiri de taxe federale după un dezastru natural. Înșelătoriile prin impersonare reprezintă cea mai frecventă plângere adresată Directoratul Național de Securitate Cibernetică (DNSC)



Cum să îl identificeți?

- Ești aprobat pentru o ofertă pentru care nu îți amintești să fi aplicat.
- Ți se oferă o despăgubire de asigurare pentru o poliță pe care nu o deții.



Cum să îl eviți?

- Fii întotdeauna precaut cu privire la împrumutătorii care:
- Promit să negocieze o modificare a creditului pentru a evita executarea silită.
- Garantează acordarea creditului dacă plătești o taxă în avans.
- Oferă o rată a dobânzii suspect de mică sau extrem de mare; ori oferte de credit care nu menționează deloc rata dobânzii.



Bibliografie

- [1] European Central Bank (2024). Report on Payment Fraud. Frankfurt am Main: European Central Bank.
- [2] European Union Agency for Cybersecurity (2024). ENISA Threat Landscape for Engineering and Financial Cyber Threats. Heraklion: ENISA.
- [3] Europol (2024). Internet Organised Crime Threat Assessment (IOCTA). Luxembourg: Publications Office of the European Union.
- [4] Federal Bureau of Investigation (2025). 2024 Internet Crime Report. Washington, D.C.: FBI Internet Crime Complaint Center.
- [5] Federal Trade Commission (2025). Consumer Sentinel Network Data Book 2024. Washington, D.C.: Federal Trade Commission.
- [6] Financial Action Task Force (2023). Cyber-enabled Financial Scams. Paris: FATF/OECD.
- [7] INTERPOL (2024). Global Financial Fraud Threat Assessment. Lyon: INTERPOL General Secretariat.
- [8] International Organization of Securities Commissions (2023). Retail Fraud and Regulated Entities. Madrid: IOSCO Technical Committee.
- [9] Organisation for Economic Co-operation and Development (2023). Consumer Protection in E-Commerce and Digital Financial Fraud. Paris: OECD Publishing.
- [10] World Bank (2022). Consumer Protection in Digital Financial Services: Enhancing Fraud Resilience. Washington, D.C.: World Bank Group.
- [11] Regulamentul (UE) 2022/2554 privind reziliența operațională digitală a sectorului financiar (DORA).
- [12] Strategia Națională de Educație Financiară – SNEF Romania 2024-2030.
- [13] Educația tinerilor în scopul prevenției fraudelor financiare online, studiu realizat de Academia de Studii Economice din București (ASE) sprijinit de Raiffeisen Bank România