FUNDAȚIA ACADEMIEI DE STUDII ECONOMICE

Raiffeisen Bank

2025

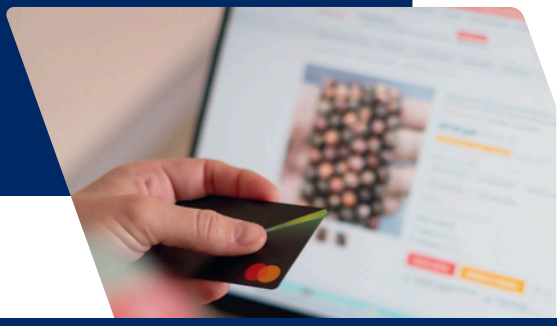
Fraudele financiare online

Ghid practic

Educația tinerilor în scopul prevenției fraudelor financiare online

Disclaimer: Într-o eră digitală în care tehnologia face parte din viața de zi cu zi, este esențial să îți dezvolți competențele necesare pentru a te proteja împotriva fraudelor financiare online. Acest ghid îți oferă informații, exemple și recomandări practice menite să te ajute să recunoști tentativele de fraudă și să adopți comportamente sigure în mediul digital. De la identificarea mesajelor suspecte și protejarea datelor personale, până la înțelegerea mecanismelor prin care acționează infractorii cibernetici, vei învăța cum să îți protejezi resursele financiare și identitatea digitală. Reține că acest ghid are scop exclusiv educațional și nu înlocuiește recomandările specialiștilor în securitate cibernetică sau ale instituțiilor financiare. Amenințările online evoluează constant, așa că îți recomandăm să te informezi periodic din surse oficiale și actualizate. ASE și Raiffeisen Bank susțin educația financiară și digitală responsabilă, încurajându-te să rămâi vigilent și informat atunci când interacționezi în mediul online.

Cuprins



FRAUDELE FINANCIARE ONLINE – O PERSPECTIVĂ GENERALĂ

Fraudele financiare online reprezintă un ansamblu de acțiuni intenționate și premeditate de inducere în eroare, concepute și executate prin utilizarea tehnologiilor informatice, a infrastructurilor digitale și a rețelelor de comunicații electronice.

De regulă, frauda financiară online presupune interacțiunea dintre mai multe elemente:

1. **Vectorul tehnologic** – rețelele publice sau private de comunicații (internet, rețele mobile), sistemele informatice (servere, platforme de e-commerce, aplicații bancare) și dispozitivele terminale (PC, smartphone, tablete).

2. **Obiectul economic** – fonduri bănești, active digitale, date financiare sensibile (numere de card, coduri PIN, parole, date de autentificare multi- factor) și instrumente de plată fără numerar.

3. **Modul de acțiune** – tehnici precum phishing, malware financiar, compromiterea conturilor online, manipularea tranzacțiilor electronice sau falsificarea datelor informatice, preluarea controlului device-urilor.

La nivel național, diverse organisme de reglementare și de aplicare a legii, cum ar fi Banca Națională a României (BNR), Direcția Națională de Securitate Cibernetică (DNSC) și Inspectoratul General al Poliției Române, au elaborat scheme de clasificare care pun accentul în principal pe trei dimensiuni critice: modus operandi (tehnicile și tacticile utilizatede făptași), natura țintei (consumatori individuali, întreprinderi sau instituții financiare) și canalele tehnologice utilizate.

1. Tipologii recunoscute în România și la nivel european

La nivel național (România)

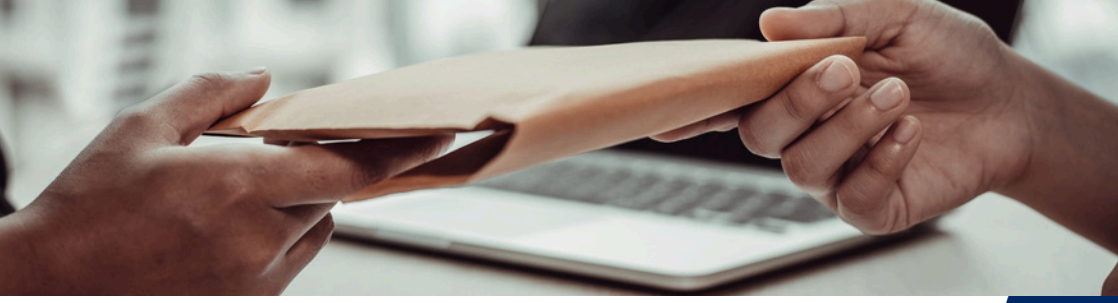
Conform rapoartelor Directoratului Național de Securitate Cibernetică (DNSC), Băncii Naționale a României (BNR) și Poliției Române, tipologiile frecvente includ:

- **Phishing bancar personalizat** – imitarea paginilor web ale băncilor românești.
- **Fraude cu investiții online** – oferte false în criptomonede sau acțiuni, promovate prin reclame agresive.
- **Fraude cu plăți avansate** – solicitarea de sume pentru „deblocarea" unor câștiguri inexistente.
- **Fraude în comerțul electronic** – vânzători inexistenți sau bunuri fictive. Compromiterea conturilor de utilizator pe platforme de plăți și retragerea neautorizată de fonduri.

La nivel european:

Potrivit Europol – Internet Organised Crime Threat Assessment (IOCTA) și EuropeanBanking Authority (EBA),tipologiile dominante sunt:

- **Social engineering avansat**– atacuri complexe combinând phishing, vishing și deepfake audio/video
- **Fraude cu carduri și date de plată** – clonarea cardurilor și tranzacții frauduloase transfrontaliere
- **Abuzul de sisteme de plăți instant** – exploatarea transferurilor rapide SEPA Instant
- **Fraude cu criptomonede**– scheme Ponzi, „rug pull" și platforme false de exchange
- **Fraude în sistemele B2B internaționale** – deturnarea facturilor și falsificarea instrucțiunilor de plată



2. Instrumente și tehnici folosite de infractorii cibernetici

În peisajul digital de astăzi, frauda cibernetică a evoluat într-un fenomen complex care transcende incidente izolate, acum susținute de infrastructuri criminale globale extinse. Aceste rețele sunt sofisticate și specializate, folosind o serie de instrumente tehnice și strategii psihologice pentru a-și desfășura activitățile ilicite.

Infractorii cibernetici combină cu pricepere exploatarea vulnerabilităților tehnologice - cum ar fi slăbiciunile software-ului, parolele inadecvate și rețelele nesigure - cu tehnici avansate de inginerie socială.

Această abordare dual le permite să manipuleze comportamentul uman, convingând indivizii să dezvăluie informații sensibile sau să ia măsuri care le compromit securitatea. În plus, acești infractori sunt extrem de adaptivi, modificându-și în mod constant metodele ca răspuns la progresele tehnologice și la schimbările în comportamentul utilizatorilor, făcând din ce în ce mai dificile detectarea și prevenirea

Înțelegerea acestor forme diferitede fraudă cibernetică este esențială pentru dezvoltarea unor contra-măsuri eficiente și pentru îmbunătățirea poziției de securitate a persoanelor și organizațiilor.

2.1. 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 pentru a determina utilizatorul să acționeze rapid, fără a avea timp să treacă acțiunea prin filtrul critic;
- Redirecționarea victimei către un mediu controlat de atacator – site clonat sau formular fals;
- Colectarea datelor – stocarea credențialelor 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

- E-mail spoofing: falsificarea antetului mesajului pentru a părea trimis de instituția bancară legitimă;
- Kits phishing: pachete software ce conțin pagini web clonă și scripturi pentru colectarea datelor;
- Hosting anonim: servere plasate în jurisdicții cu legislație permisivă; SSL/TLS fals: certificate obținute de atacatori pentru a simula conexiuni securizate („https”).
- Mecanism psihologic: utilizarea unui pretext administrativ („actualizarea obligatorie a datelor”) care invocă conformitatea cu procedurile băncii.

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

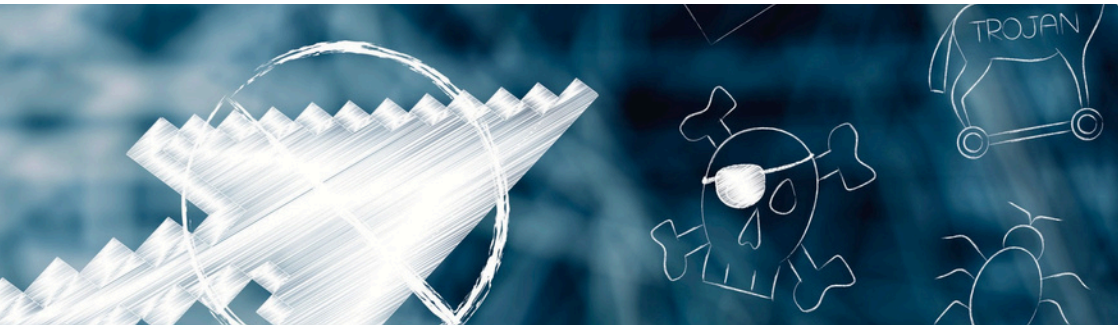
Tehnici și instrumente utilizate

- Trigger emoțional de panică: formulăriprecum „Tranzacție suspectă detectată”;
- Mesaje SMS (smishing): trimiterea de link-uriscurte către pagini de phishing optimizate pentru mobil;
- Interfețe mobile simulate: pagini ce imităexact aplicațiile bancareoficiale; Servere de redirecționare: pentru ascunderea surseireale a atacului.
- Mecanism psihologic: crearea unui sentiment de urgență care determină victima să acționeze imediat, fără verificări suplimentare.

C. Mesaj privind contractarea unui credit în numele victimei și solicitarea confirmării datelor

Tehnici și instrumente utilizate

- Scenariu de fraudă cu identitate furată: invocarea riscului imediat de îndatorare neautorizată;
- Canale multiple de contact: e-mail,telefon (vishing) pentru validarea falsei urgențe;
- Formulare interactive frauduloase: câmpuri de completat ce solicită CNP, date de card, coduri de securitate;
- Integrarea cu baze de date furate: pentru a personaliza mesajul cu numele real al victimei, sporind credibilitatea.
- Mecanism psihologic: exploatarea fricii de prejudiciu financiar pe termen lung și presiunea de a „opri”un proces ilegal în desfășurare.



Infrastructura folosită

În toate scenariile, instrumentele tehnice au elemente comune:

- Domenii web similare (typosquatting, ex. „banck-romania.ro”);
- Certificate SSL ieftine sau gratuite pentru crearea iluziei de securitate;
- Servere proxy și VPN-uri pentru anonimizarea locației atacatorului;
- Baze de date cu informații compromise achiziționate din dark web.

2.2. Investment Scam

Frauda de tip Investment Scam reprezintă o schemă frauduloasă prin care victimele sunt determinate să investească sume de bani în așa-zise oportunități financiare, prezentate ca fiind extremde profitabile și cu risc scăzut sau inexistent.

În realitate, aceste investiții sunt fictive, iar scopul final este transferul fondurilor către conturi controlate de infractori.

Caracterul modern al acestor fraude constă în combinarea publicității agresive pe platforme online cu manipularea directă a dispozitivelor victimei prin instrumente tehnice de control de la distanță.

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 caracterizează prin:

A. Identificarea și atragerea victimei

- **Reclame sponsorizate pe rețele sociale** (Facebook, Instagram, LinkedIn, TikTok), optimizate prin tehnici de microtargeting pentru a ajunge la persoane cu interes potențial în investiții.
- **Paginile de aterizare (landing pages)** care imită platforme legitime de trading sau portaluri financiare cunoscute.
- **Testimoniale false** (texte, fotografii sau videoclipuri cu „investitori mulțumiți") pentru crearea unei aparențe de credibilitate.

B. Contactul direct cu victima

- **Apeluri telefonice inițiate de operatori frauduloși** (așa-numiții boiler room agents), care urmează un script prestabilit pentru a câștiga încrederea victimei.
- **Spoofing de număr** – tehnică prin care numărul afișat pe telefon pare a fi cel al unei instituții legitime.
- **Persuasiune prin tehnici de influențare psihologică** (autoritate, reciprocitate, urgență) – fraudatorii se prezintă drept „consultanți financiari" sau „specialiști în piețe de capital".

C. Solicitarea instalării aplicațiilor de control la distanță

- **Software legitim reutilizat în scop fraudulos,** precum AnyDesk, TeamViewer, RemotePC – prezentate victimei drept instrumente pentru „asistență tehnică"în procesul de investiție.
- **Inginerie socială** pentru obținerea permisiunilor extinse pe dispozitivul victimei (acces la ecran, tastatură, fișiere, notificări).
- **Ascunderea scopului real:** atacatorii afirmă că instalarea este necesară pentru „ghidarea pas cu pas" în crearea contului de investiții.

D. Preluarea controlului asupra aplicației de Mobile Banking

- **Interacțiune directă cu aplicația băncii,** în timp ce victima este prezentă, sub pretextul „alimentării contului de investiții".
- **Capturarea codurilor OTP** primite prin SMS sau aplicații de autentificare, datorită accesului în timp real la telefon.
- **Transferuri imediate** către conturi de tip „mule account" (conturi bancare deschise pe numele unor terți, folosite pentru spălarea banilor).

Mecanisme psihologice exploatate

- **Lăcomia** – promisiunea unor câștiguri rapide și semnificative;
- **Frica de a pierde oportunitatea** (fear of missing out – FOMO);
- **Autoritatea** – prezentarea fraudatorului ca expert sau reprezentant al unei instituții de prestigiu;
- **Reciprocitatea** – oferirea de „informații privilegiate" în schimbul unei acțiuni imediate.

Infrastructura utilizată

- **Servere de găzduire offshore** – pentru site-urile de promovare și platformele false;
- **Servicii VoIP internaționale** – pentru apeluri cu identificator fals;
- **Rețele de conturi bancare intermediare** – pentru dispersarea rapidă a fondurilor;
- **Platforme de conversiecrypto** – pentru transformarea sumelor în criptomonede greu de urmărit.

2.3. Spoofing

În domeniul criminalității informatice, spoofing-ul desemnează tehnica prin care un atacator falsifică informațiile de identificare ale unei surse de comunicare (număr de telefon, adresăde e-mail, IP) pentru a se prezenta ca o entitate legitimă și de încredere.

În contextul financiar, *caller ID spoofing* este folosit pentru a afișa pe telefonul victimei un număr real aparținând unei bănci, unei instituții financiare sau unei autorități publice, cu scopul de a obține acces la date sensibile ori de a determina victima să efectueze tranzacții financiare.

A. Obținerea și utilizarea tehnologiilor de falsificare a identității apelantului

- **Servicii VoIP cu funcție de schimbare a caller ID-ului** – multe operate din jurisdicții externe, cu reglementare redusă;
- **Platforme specializate în spoofing** (de ex. spoof card services) care permit introducerea manuală a numărului afișat;
- **SIM swap** – furtul numărului de telefon real al unei victime prin portare frauduloasă către alt operator (în cazuri mai complexe).

B. Impersonarea instituțiilor de încredere

Impersonarea Call Center-ului unei bănci

- Falsificarea numărului oficial al băncii - atacatorul informează victima că datele bancare au fost compromise și solicită „validarea" acestora.
- Scripturi verbale predefinite, în care sunt inserate detalii reale despre client (posibil obținute din baze de date obținute ilicit.

Impersonarea Băncii Naționale a României

- Prezentarea apelului ca fiind efectuat din partea BNR, cu pretextul „protejării" victimei prin contractarea unui credit pe numele său.
- Utilizarea unui nume real al unui salariat BNR și invocarea unor reglementări fictive pentru a spori credibilitatea.

Impersonarea Poliției

- Apel cu număr oficial al unei secții de poliție, în care victima este informată că datele sale personale au fost furate. Se sugerează urgent contractarea unui credit, retragerea banilor și depunerea acestora într-un ATM Bitcoin „pentru securizare".
- Crearea unei presiuni psihologice intense prin invocarea unei anchete în desfășurare și a unui „termen limită"pentru acțiune.

Mecanisme Psihologice Exploatate

- Autoritatea – atacatorii se prezintă drept funcționari ai unor instituții puternice (bancă, BNR, poliție);
- Frica – amenințarea cu pierderi financiare iminente sau consecințe legale;
- Urgența – inducerea ideii că acțiunea trebuie efectuată imediat, fără verificări;
- Confuzia procedurală – utilizarea unui limbaj tehnic sau birocratic pentru a inhiba întrebările victimei.

Infrastructura tehnică utilizată

- Rețele VoIP anonimizate – cu servereîn țări diferite de cele ale victimelor, pentru îngreunarea urmăririi;
- Sisteme de redirecționare a apelurilor pentru mascarea traseuluireal;
- Baze de date cu informații personale achiziționate din dark web, pentru personalizarea apelului;
- Rețele de ATM-uri Bitcoin folosite ca metodă finală de conversie și transfer a fondurilor, dat fiind caracterul pseudonim al tranzacțiilor crypto.

2.4. Deepfake

Frauda de tip *deepfake* reprezintă utilizarea tehnologiilor bazate pe **inteligență artificială generativă (IA)** și **rețele neuronale profunde** pentru a crea, modifica sau suprapune imagini, înregistrări audio ori video astfel încât acestea să pară autentice, deși sunt fabricate.

În mediul financiar, deepfake- urile sunt exploatate pentru a induce în eroare investitori și consumatori prin falsificarea aparenței unor persoane publice, instituții sau branduri, cu scopul de a legitima oferte fictive de investiții și de a obține transferuri de bani.

1. Utilizarea imaginii unor persoane cunoscute (ex. politicieni, economiști, antreprenori de succes) pentru promovarea investițiilor

✓ Generarea de videoclipuri sau imagini în care persoana respectivă „vorbește" și „recomandă" achiziția de acțiuni cu randament ridicat prin:

- Platformede *face-swapping* și *lip-syncing* bazate pe GAN (Generative Adversarial Networks) – ex. *DeepFaceLab, FaceSwap.*
- Software de generare vocală *(voice cloning)* precum *ElevenLabs* sau *Respeecher,* pentru imitarea vocii persoanei.

✓ Exploatarea reputației și credibilității unei figuri publicepentru a valida o schemă frauduloasă.

2. Utilizarea numelui unor instituții publice (ex. ministere, agenții de stat) pentru promovarea „vânzării de acțiuni”

✓ Crearea de materiale video deepfake în care reprezentanți fictivi ai instituției (ori figuri reale falsificate) anunță o ofertă de acțiuni „cu acces limitat” prin:

- Suprapunerea feței și vocii pe corpul unui actor care citește un script comercial fals.
- Integrarea siglelor oficiale și a graficii instituționale autentice preluate de pe site-urile reale.

✓ Exploatarea reputației și credibilității unei figuri publicepentru a valida o schemă frauduloasă.

3. Crearea materialului deepfake

- **Colectarea datelor sursă**: imagini și înregistrări audio-video cu ținta (preluate din interviuri, rețele sociale, arhive media).
- **Antrenarea modelului AI**: folosirea unui set de date cu sute sau mii de cadre ale feței țintei pentru a antrena rețeaua neuronală.
- **Generarea materialului final**: combinarea feței și vocii falsificate cu un mesaj comercial sau investițional adaptat audienței-țintă.

4. Distribuirea materialului

- **Canale folosite:** platforme sociale (Facebook, Instagram, TikTok), site-uri de știri false, YouTube Ads sau reclame plătite în rețele de display.
- **Targetare:** folosirea algoritmilor de microtargetare pentru a afișa materialul către utilizatori cu profil financiar interesat (investitori, antreprenori).

5. Apelarea victimei

- **Call-to-action fals**: link către un site de tip phishing sau o platformă frauduloasă de investiții.
- **Escaladarea:** apel telefonic de la un „consilier de investiții" care finalizează tranzacția și solicită date bancare sau instalarea unei aplicații de control la distanță.

6. Instrumente și infrastructură tehnică utilizată

- **Software open-source de deepfake**: DeepFaceLab, FaceSwap, Avatarify.
- **Servicii comerciale de AI video editing** (SaaS) cu interfețe prietenoase, folosite fără cunoștințe tehnice avansate.
- **Voice cloning** – reconstituirea vocii din mostre de câteva secunde
- **Site-uri frauduloase de investiții** – realizate cu șabloane predefinite, integrate cu procesatoare de plăți crypto sau conturi de transfer rapide. Campanii de publicitate plătită – pentru a amplifica vizibilitatea materialului deepfake și a-i conferi aparență de legitimitate.

7. Mecanisme psihologice exploatate

- **Efectul de autoritate:** folosirea figurilor publice pentru a transfera încredere schemei.
- **Aversiuneafață deratarea oportunității (FOMO):** promisiunea unor câștiguri rapide și „oferte limitate".
- **Confirmarea socială:** prezentarea deepfake-ului ca parte dintr-o „campanie națională"sau „parteneriat cu statul".
- **Iluzia profesionalismului:** folosirea unor elemente vizuale și sonore oficiale (sigle, decoruri instituționale, ton formal).

2.5. Online Shopping Platforms Fraud

Frauda de tip Online Shopping Platforms Fraud reprezintă totalitatea acțiunilor ilicite desfășurate prin intermediul platformelor de comerț electronic, site-urilor de anunțuri sau rețelelor de socializare, având ca scop inducerea în eroare a cumpărătorilor sau vânzătorilor în vederea obținerii de beneficii patrimoniale necuvenite.

Acest tip de fraudă implică, de regulă, exploatarea încrederii în mecanismele de tranzacționare online, prin crearea unor scenarii aparent legitime de vânzare sau cumpărare.

Etapele tipice se caracterizeaza prin:

1. Anunțuri false de vânzare de bunuri – plata în avans, fără livrare

Fraudatorul publică un anunț atractiv, cu un preț sub media pieței, pentru a stimula achiziția rapidă. După ce primește plata integrală sau un avans substanțial, dispare fără a expedia produsul. Cum:

- Conturi false pe platforme consacrate (OLX, eMAG Marketplace, eBay).
- Fotografii și descrieri copiate de la anunțuri legitime.
- Adrese de e-mail temporare și numere de telefon virtuale (VoIP) pentru comunicare.

2. Postarea unui anunț real de către un vânzător, dar „cumpărătorul” solicită datele cardului sub pretextul livrării banilor

Infractorul pretinde că dorește să cumpere produsul, însă afirmă că plata se face printr-un „serviciu de livrare” al platformei, care ar necesita introducerea datelor cardului (număr, data expirării, CVC pe un link transmis prin mesaj. În realitate, datele sunt folosite pentru fraudarea contului bancar. Cum:

- Site-uri de phishing care imită perfect pagina oficială a platformei de comerț,
- Link-uri scurtate sau mascate pentru a ascunde adresa reală a site-ului fraudulos,
- Scripturi automatizate de captare a datelor introduse de victimă.

3. Confuzia intenționată între numărul de cont și datele cardului

Victima este convinsă că, pentru a primi bani, trebuie să ofere datele complete ale cardului, deși, în realitate, transferul bancar necesită doar IBAN-ul. Această tehnică exploatează necunoașterea procedurilor bancare de către utilizatorii obișnuiți. Cum:

- Comunicarea directă prin platformă sau mesagerie instant (WhatsApp, Messenger).
- Capturi de ecran false cu „interfața” băncii sau platformei, pentru a „dovedi” procedura.

4. Tehnici operaționale ale fraudatorilor

Inginerie socială

- Exploatarea urgenței („produsul are multe cereri”, „oferta este valabilă doar azi”) pentru a forța decizia rapidă.
- Crearea unui fals sentiment de legitimitate prin folosirea unui profil cu recenzii furate sau istoric fictiv de vânzări.
- Manipularea prin prezentarea de dovezi false (chitanțe falsificate, confirmări de plată inexistente).

Tehnici informatice

- Phishing avansat: pagini web clonă care trimit datele direct către serverul infractorului.
- Obfuscare URL: mascarea adresei reale prin domenii similare (typosquatting) sau folosirea serviciilor de scurtare a link-urilor.
- Anonimizare: folosirea de VPN-uri, servere proxy și numere virtuale pentru a evita identificarea.

Infrastructura și instrumentele utilizate

- Platforme de anunțuri clonate sau create special pentru fraudă.
- Servicii VoIP (Skype, Google Voice, TextNow) pentru a apela victimele din numere cu prefixe credibile.
- Servicii de e-mail temporar pentru crearea rapidă de conturi. Instrumente grafice (Photoshop, Canva) pentru falsificarea chitanțelor și capturilor de ecran.
- Rețele de conturi false pentru recenzii pozitive fictive, menite să crească încrederea.

Mecanisme psihologice exploatate

- **Efectul de raritate:** teama că oferta va fi pierdută determină acțiuni impulsive.
- **Transferul de încredere:** încrederea acordată platformei legitime este transferată, în mod eronat, către profilul fals.
- **Presiunea socială:** indicarea unor „alți cumpărători interesați” pentru a grăbi tranzacția.
- **Confuzia procedurală:** exploatarea necunoașterii diferenței dintre IBAN și datele cardului.

3. Factori care favorizează expunerea la fraude online

Există o expunere inegală a tinerilor la tehnologiile digitale și, în general, cei care sunt vulnerabili în viața de zi cu zi tind să fie mai vulnerabili și în online (Burns și Gottschalk, 2019). Există trei aspecte distincte care evidențiază acest lucru:

Accesul la internet: Între cei care au acces la internet și cei care nu au există diferențe majore între țări, între mediile rurale și urbane sau între gospodăriile care aparțin unor medii socio-economice diferite. Acesta este primul și cel mai evident obstacol.

Utilizare și competențe: Între modelele de utilizare și inegalitățile în competențele digitale: diferențele în utilizarea tehnologiilor și a internetului între tinerii avantajați și cei dezavantajați sunt semnificative, mai ales atunci când este luat în considerare modul în care elevii utilizează internetul și ehnologiile digitale. Tinerii avantajați au mai multe șanse să citească știrile și să folosească internetul pentru a obține informații practice decât colegii lor dezavantajați, care au mai multe șanse să-și petreacă timpul online jucând jocuri sau conversând. Astfel, chiar și atunci când accesul există, calitatea și utilitatea acestuia variază enorm.

Rezultate: tinerii dezavantajați, mai puțin decât tinerii avantajați, utilizează internetul și tehnologiile digitale pentru a beneficia de servicii precum serviciile financiare sau platformele de căutare a locurilor de muncă, ceea ce are ca rezultat și reflectă inegalități în rezultatele offline. Aceste diferențe pot conduce la concluzia că disparitatea digitală se transformă în inegalitate socio-economică concretă.

Factorii precum mediul socio-economic și genul afectează inegalitățile digitale. Pentru tinerii vulnerabili, cum ar fi cei care trăiesc cu dizabilități, tehnologiile digitale și conectivitatea pot fie să agraveze vulnerabilitățile și excluziunea socială, fie să ofere oportunități de integrare. Potențialul de transformare este imens, însă politicile și măsurile implementate determină în mod direct rezultatul final.

Principalii factori care favorizează expunerea la fraudele online sunt: situația financiară personală, statutul de ocupare, gradul de alfabetizare financiară, percepția serviciilor financiare, infrastructura digitală și normele culturale, sociale sau religioase

1. Situația financiară personală și statutul de ocupare influențează în mod semnificativ incluziunea financiară a tinerilor. Rata ridicată a șomajului în rândul tinerilor, precum și lipsa resurselor financiare, sunt frecvent menționate ca principale obstacole în accesul la servicii financiare. În unele contexte, șomajul tinerilor este perceput drept barieră majoră pentru economii de pensii sau alte produse financiare, iar lipsa unui venit stabil este unul dintre motivele principale pentru excluziunea financiară a tinerilor.

2. Nivelul scăzut de alfabetizare financiară reprezintă un factor important care contribuie la excluziunea financiară a tinerilor. Aceștia nu doar că au cunoștințe limitate despre finanțe, dar lîntâmpină carențe și în ceea ce privește competențele și conștientizarea privind serviciile și produsele financiare. Pentru a contracara această situație, factorii de decizie au implementat politici și programe de educație financiară, inclusiv în curricula școlară. Dovezile sugerează că astfel de inițiative conduc la o mai bună gestionare a creditelor, reducerea datoriilor și utilizarea unor metode de împrumut mai avantajoase.

3.Percepția tinerilor asupra necesității serviciilor financiare este influențată de mai mulți factori, inclusiv lipsa cunoștințelor și a resurselor financiare. Mulți tineri consideră că nu au nevoie de servicii financiare și nu le găsesc utile, ceea ce îi determină să nu acceseze produse precum conturi de economii, carduri de debit, împrumuturi sau asigurări. Această percepție redusă a necesității reprezintă un obstacol semnificativ în calea incluziunii financiare a tinerilor.

4. Lipsa accesului la infrastructură digitală limitează posibilitatea tinerilor de a fi incluși financiar în mediul digital. Pentru cei fără acces la internet sau la un telefon mobil, dezvoltarea unei infrastructuri digitale accesibile reprezintă o condiție esențială pentru promovarea incluziunii financiare digitale.

5. Normele culturale, sociale sau religioase, inclusiv controlul parental sau diferențele de gen, pot reprezenta un obstacol semnificativ pentru incluziunea financiară a tinerilor.

Diferențele de percepție digitală menționate anterior riscă să amplifice și mai mult inegalitățile dintre tineri în ceea ce privește accesul la învățarea digitală sau riscul de abandon școlar din educație și formare. Accesul tinerilor la dispozitive mobile și la internet accesibil servește drept condiție prealabilă pentru asigurarea incluziunii lor financiare digitale. Prin urmare, inegalitățile în accesul la tehnologiile digitale se pot reflecta în inegalități care au ca rezultat niveluri de incluziune financiară. În concluzie, dreptul la conectivitate devine, astfel, strâns legat de dreptul la participare economică și socială în societatea contemporană.

4. Rolul familiei, instituțiilor de învățământ și a mediului financiar-bancar în formarea competențelor financiare digitale în rândul tinerilor

Formarea competențelor financiare digitale în rândul tinerilor este un proces de lungă durată și există mai mulți actori ce trebuie să fie implicați pentru ca acest segment de populație să câștige aceste abilități: familia, instituțiile de învățământ și entitățile din domeniul financiar – bancar

1. Familia

Familia, părinții sau persoanele care au grijă de copii/tineri au un rol esențial în a cultiva educația financiară și a modela abilitățile digitale în rândul acestora. Furnham et al (2024) arată că, până la vârsta de șapte ani, copiii își formează deja primele obiceiuri legate de bani, ceea ce evidențiază rolul major al părinților în conturarea acestor deprinderi timpurii. Dezvoltarea capacității părinților de a discuta deschis și de a-și ghida copiii în privința aspectelor financiare creează o bază solidă pentru formarea unor adulți responsabili și încrezători în gestionarea resurselor proprii.

Importanța începerii educației financiare de la o vârstă fragedă are în vedere creșterea nivelului de alfabetizare financiară și digitală. Concentrarea pe anii timpurii urmărește să formeze o generație capabilă să își administreze corect finanțele, să înțeleagă modul în care serviciile financiare pot fi accesate online și să fie capabilă să detecteze posibile fraude financiare. Pregătirea părinților pentru a transmite obiceiuri financiare sănătoase și abilități digitale este un pas decisiv către dezvoltarea unui comportament financiar responsabil pe termen lung.

Totuși pentru a putea crea competențe financiare digitale solide în rândul copiilor/tinerilor, trebuie ca adulții să aibă încredere în propriile abilități de administrare a finanțelor persoanale, mai ales cei din medii socio-economice vulnerabile. De aceea, sprijinirea părinților este crucială, întrucât discuțiile despre bani în familie sporesc încrederea copiilor în propriile competențe financiare, dar și competențe digitale.

Totodată, este important de recunoscut că unii părinți se simt nesiguri sau nepregătiți să abordeze aceste subiecte, iar depășirea acestei bariere este necesară nu doar pentru educația individuală, ci și pentru reducerea inegalităților economice. Din acest motiv considerăm ca rezultatele acestui studiu și ghidurile ce se vor realiza sunt un bun punct de plecare pentru ca adulții să fie mai bine pregătiți în transmiterea unor informații relevante copiilor lor.

Mai mult, tinerii gestionează deja sume de bani sau obțin venituri proprii, rolul părinților de ghizi în educația financiară devening și mai vizibil.

Prin urmare, gestionarea veniturilor și cheltuielilor, realizarea bugetului personal, investițiile realizate prin intermediul aplicațiilor online puse la dispoziție de brokeri, utilizarea serviciilor bancare online sunt abilități pe care tinerii ar trebui să le deprindă mai ales prin relația cu membrii familiei. În acest sens, cele mai importante măsuri trebuie să aibă în vedere:

- Încurajarea părinților și îngrijitorilor să inițieze și să întrețină discuții despre bani cu copiii lor, folosind resursele existente și canalele de comunicare disponibile, pentru a întări lecțiile despre educația financiară în mediul online și în mediul familial;

- Susținerea proceselor de învățare de acasă, prin ghiduri practice (ce vor fi parte a rezultatului acestui studiu) oferind părinților instrumentele și materialele necesare pentru a prezenta conceptele financiare într-un mod eficient.

2.Instituțiile de învățământ

Instituțiile de învățământ au un rol esențial în dezvoltarea competențelor financiare ale tinerilor (Johnson și Sherraden, 2007), prin transmiterea conținuturilor educaționale și cultivarea dorinței de învățare pe tot parcursul vieții.

Perfecționarea pregătirii cadrelor didactice și accesul sporit la resurse educaționale în domeniul educației financiare, cât și a celei digitale le oferă profesorilor instrumentele necesare pentru predarea unor abilități fundamentale, precum înțelegerea modului în care funcționează mediul online și a gestionării banilor personali.

Prin adaptarea noțiunilor financiare complexe în lecții accesibile, profesorii răspund diversității nevoilor elevilor și transformă educația financiară într-un sprijin practic pentru viața adultă.

Creșterea competențelor cadrelor didactice în domeniul alfabetizării financiare permite realizarea unor conținuturi care fac legătura între teoria predată la clasă și deciziile financiare reale, sporind încrederea și capacitatea de decizie a elevilor.

Dotarea profesorilor cu instrumente moderne și oferirea de oportunități de formare continuă contribuie la dezvoltarea unei culturi a responsabilității financiare, ce include familiile și comunitatea largă, sprijinind astfel prosperitatea economică a generațiilor viitoare.

Strategia Națională de Educație Financiară 2024-2030 a României vine cu un set de acțiuni concrete în care instituțiile de învățământ, dar și alți actori din piață ar trebui să se implice, acțiuni ce au în vedere OS1, Dezvoltarea și introducerea elementelor de educație financiară în curriculumul național la toate nivelurile de învățământ, OS2.

Realizarea de acțiuni de educație financiară complementare, adresate învățământului preuniversitar și universitar, OS3. Introducerea educației financiare în universități, OS4. Promovarea unor comportamente financiar responsabile în rândul copiilor, tinerilor prin intermediul mass-media și al canalelor de comunicare social media, OS5. Implementarea unor programe de educație financiară destinate cadrelor didactice din învățământul preuniversitar și universitar, OS6.

Implementarea unui program național de conștientizare, consiliere și sprijin pentru părinți în vederea educării copiilor din perspectivă financiară. Astfel, învățământul are un rol crucial în dezvoltarea abilităților financiare digitale în rândul tinerilor.

Conform analizei realizate în baza Raportului OECD/INFE 2023 International Survey Of Adult Financial Literacy [1], cele mai importante acțiuni ale instituțiilor de învățământ trebuie să aibă în vedere:

- Dezvoltarea programelor de formare a cadrelor didactice, care să includă atât activități de perfecționare profesională continuă (CPD), cât și cursuri specializate dedicate predării educației financiare și produselor financiare disponibile online.
- Creșterea gradului de conștientizare privind resursele și inițiativele existente în diverse sectoare, astfel încât profesorii să fie bine informați și să utilizeze eficient materialele necesare pentru consolidarea competențelor financiare digitale.

3. Mediului financiar-bancar

Instituțiile financiar-bancare au o acoperire excelentă în rândul populației locale, dispun de datele necesare pentru a fundamenta deciziile și utilizează tehnologii avansate, capabile să proceseze volume mari de analize pentru a genera impact. Pentru a valorifica aceste atuuri, instituțiile financiar-bancare trebuie să:

- Organizeze datele – să le facă accesibile în timp real, permanent, și suficient de bine structurate pentru a oferi o imagine clară asupra comportamentului fiecărui client.
- Oferă servicii relevante – să pună la dispoziție, într-o manieră simplă și intuitivă, funcționalități de gestionare financiară precum bugete, rapoarte, prognoze de cashflow sau obiective de economisire.
- Furnizeze informații personalizate – să își sprijine clienții prin analize adaptate comportamentului lor financiar, să le explice consecințele anumitor decizii și să recomande, la momentul oportun, produsele financiare care le pot aduce beneficii reale.

Serviciile financiare digitale pot reprezenta un factor esențial pentru creșterea incluziunii financiare, în special în România, unde majoritatea populației are acces mai ușor la un telefon mobil decât la o bancă. Incluziunea financiară, în sensul său deplin, înseamnă accesul și utilizarea unor produse și servicii financiare de calitate, la prețuri accesibile, care contribuie la bunăstarea financiară a individului.

Având în vedere cele menționate anterior, cele mai importante măsuri ale instituțiilor financiar-bancare trebuie să aibă în vedere:

- Dezvoltarea de aplicații digitale ușor de utilizat, cu componentă educațională care să sprijine utilizatorul în a lua cele mai bune decizii pentru finanțele personale.

- Un nivel ridicat de siguranță pentru serviciile financiare oferite online, care să protejeze utilizatorul de posibile fraude ce pot apărea.

Un obstacol major în atingerea incluziunii financiare îl reprezintă nivelul redus de alfabetizare digitală și financiară prezent în România.

Pe măsură ce produsele și serviciile financiare sunt livrate tot mai mult în format digital, competențele în ambele domenii devin esențiale. Implementarea unor inițiative eficiente de creștere a nivelului de alfabetizare ar putea îmbunătăți considerabil protecția consumatorilor și sănătatea financiară, în special în rândul grupurilor defavorizate.

Totuși, proiectarea și aplicarea unor programe de alfabetizare digitală și financiară de succes este un proces complex.

Colaborarea dintre sectorul public și cel privat, împreună cu societatea civilă, este esențială pentru elaborarea conținutului educațional, definirea strategiilor de atingere a utilizatorilor finali și evaluarea programelor-pilot între toți actorii menționați în acest subcapitol.

FUNDAȚIA ACADEMIEI DE STUDII ECONOMICE
București, România
Fondată în 2013

Fraude online

Raiffeisen Bank