

Cum funcționează fraudele de inginerie socială și cum ne protejăm de ele (phishing, vishing, smishing, spoofing etc)

Un singur apel telefonic, un SMS aparent banal, sau un cod QR scanat în grabă pot declanșa coșmarul pierderii economiilor de-o viață. În era inteligenței artificiale și a fraudelor digitale tot mai sofisticate, escrocii nu mai încearcă doar să spargă parole sau sisteme informatice, aceștia aleg, tot mai des, să manipuleze frica, graba și încrederea oamenilor în instituții autorității și apropiați. Astfel, cea mai vulnerabilă verigă în acest ecosistem nu mai este tehnologia, ci omul.

Deși autoritățile, operatorii din telecomunicații, operatorii serviciilor de plăți și presa și-au intensificat și coordonat acțiunile de informare și prevenire reușind o mobilizare extraordinară a societății pentru prevenirea fraudelor telefonice, phishing-ul continuă să facă victime. Totodată, în spațiul public rămâne neclar ce rol și responsabilități au diferiți actori în prevenirea și combaterea fraudelor de inginerie socială. În acest context, prezenta notă își propune să explice cum funcționează fraudele financiare bazate pe utilizarea telecomunicațiilor și a tehnicilor de inginerie socială, care sunt principalele riscuri și ce pot face atât autoritățile, mediul de afaceri, dar și cetățenii pentru a reduce probabilitatea de a deveni victime ale escrocilor.

Diferența dintre o fraudă și o încălcare din domeniul protecției consumatorului

Protecția consumatorului este domeniul care vizează relația dintre consumator și un profesionist, persoană fizică sau juridică care desfășoară o activitate comercială legitimă. De cealaltă parte, o fraudă are loc atunci când o persoană sau grup de persoane fac promisiuni care, din capul locului, sunt false, sau nu se intenționează a fi îndeplinite și se fac doar cu scopul de a deposea victima de bunurile și banii ce-i aparțin¹. Mai nou, escrocii, prin fel de fel de manipulări și minciuni, pot chiar să determine persoana să se împrumute și să le transfere banii împrumutați.

Când profesioniștii ajung să inducă în eroare consumatorii sau devin prea insistenți sau chiar agresivi în efortul de a determina consumatorii să cumpere un produs sau serviciu pe care în alte circumstanțe nu l-ar fi procurat, în astfel de cazuri este vorba despre o practică comercială incorectă și aceasta face parte din domeniul de protecție a consumatorului.

Diferența între o practică comercială incorectă și o fraudă constă în faptul că în primul caz se urmărește vânzarea unui produs sau serviciu (legitim). În cazul fraudelor, escrocul vrea, pur și simplu, să-l deposeze pe om de averea acestuia. În consecință, intenția comerciantului este să vândă, iar cea a escrocului este, din start, să intre fraudulos în posesia averii străine. Tocmai din acest motiv, de practici comerciale incorecte se ocupă autoritățile în domeniul protecției consumatorului, iar fraudă cade în competența organelor de drept.

¹ Art. 190 al (1) al [Codului penal al Republicii Moldova](#), escrocheria reprezintă: "sustragerea bunurilor altei persoane prin abuz de încredere, inducere sau menținere în eroare"

Ce sunt fraudele de inginerie socială

Odată cu evoluția sistemelor de plăți și a tranzacțiilor la distanță, au evoluat și fraudele. În conformitate cu datele Agenției UE pentru securitate cibernetică (ENISA), phishingul și tacticile de inginerie socială sunt principala portiță prin care sunt comise fraudele². În raportul său pentru 2026 Europol menționează că drept răspuns la introducerea pe scară tot mai largă a autentificării stricte a clienților, de exemplu autentificarea în 2 pași (demonstrarea cunoașterii – cum ar fi parola; și a posesie ex: dispozitivul pe care se trimite codul OTP sau care scanează amprenta sau fața), escrocii cresc presiunea pe exploatarea erorilor și vulnerabilităților umane³.

Astfel, în loc să dezvolte soluții tehnologice tot mai sofisticate pentru a putea accesa conturile sau portofelele electronice ale utilizatorilor, escrocii pun un accent mai mare pe manipularea psihologică a victimelor pentru a le determina să divulge informații confidențiale, să ofere acces, sau să efectueze voluntar anumite acțiuni în beneficiul autorilor fraudei. Astfel, escrocii conving victima fie să transfere bani, fie să instaleze o aplicație prin care se fură identitate, datele posesorului sau se preia controlul dispozitivului pentru delapidarea mijloacelor bănești ale posesorului. Prin tehnici de inginerie socială escrocii creează un sentiment puternic de urgență, panică sau autoritate, astfel încât victima să reacționeze rapid și să nu mai analizeze critic situația.

Cea mai cunoscută și răspândită metodă de inginerie socială este „phishing”-ul. Dacă termenul englez fishing înseamnă pescuit propriu-zis, atunci phishig (cu „p”) este noțiunea utilizată pentru a desemna „pescuit”-ul fraudulos de parole, informații personale, coduri OTP (One Time Password) etc pentru a facilita accesul la mijloacele financiare ale victimei.

În funcție de instrumentele utilizate pentru un astfel de pescuit fraudulos distingem foarte multe tipuri de escrocherii. Printre acestea, cele mai frecvente escrocherii cu implicarea telefoniei ca și vehicul de perpetuare a fraudei sunt:

- Vishing (voice phishing) escrocii utilizează comunicarea telefonică prin intermediul căreia încearcă să persuadeze victima prin exploatarea fricii, stresului, respectului față de autorități, să întreprindă acțiuni pe care în alte circumstanțe nu le-ar fi întreprins.
- CLI Spoofing este o tehnologie prin care escrocii falsifică identitatea sau numărul de telefon pentru a părea o persoană, companie/număr de încredere. Prin intermediul caller ID spoofing, infractorii pot afișa pe dispozitivul victimei un număr legitim (numărul băncii, al soției sau copilului), dar în esență, este un număr fals și victima fără să-și dea seama discută cu un infractor.
- Smishing are loc atunci când escrocul trimite un mesaj scurt prin care încearcă să determine victima să acceseze un link, să instaleze o aplicație, să completeze un formular, să apeleze un număr de telefon controlat de escroci etc.
- Telephone Oriented Attack Delivery (TOAD) cunoscut prescurtat ca și (callback phishing), victima primește un mesaj aparent inofensiv, prin care i se comunică că ratează o oportunitate sau a apărut o problemă ce-l vizează și este îndemnat să apeleze un număr de

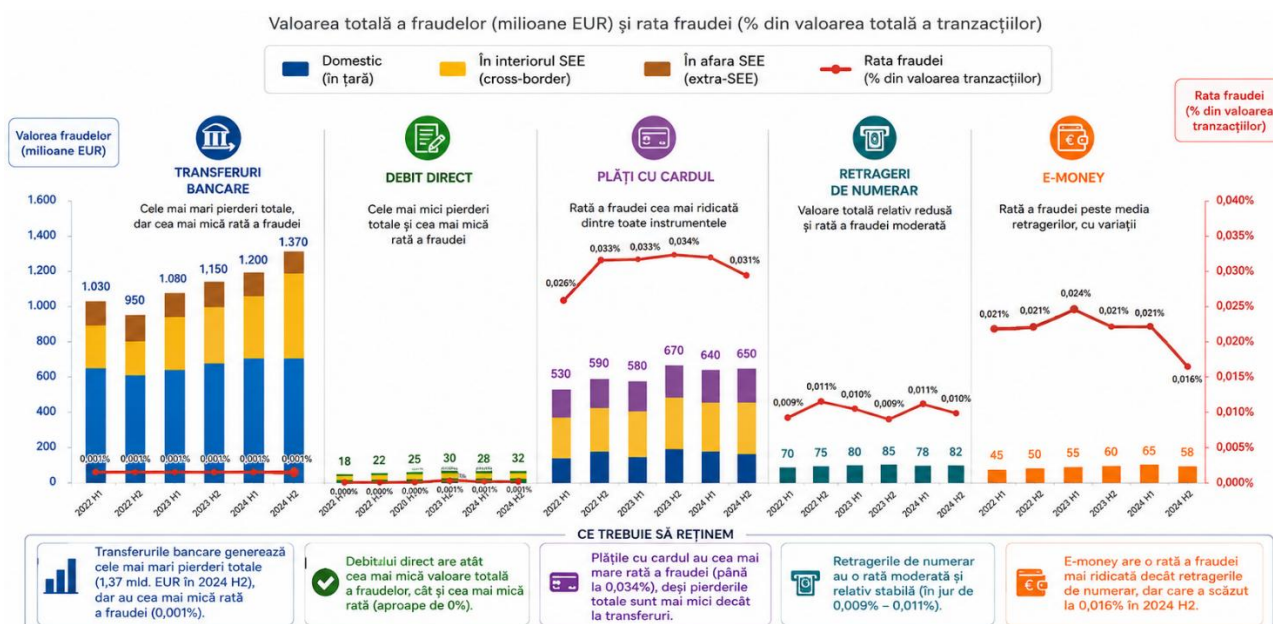
² ENISA [Threat Landscape 2025](#). European Union Agency for Cybersecurity, Oct. 2025, pag 11

³ Europol, [The evolving threat landscape. How encryption, proxies and AI are expanding cybercrime – Internet Organised Crime Threat Assessment](#) (IOCTA) 2026, Publications Office of the European Union, Luxembourg, pag 21

telefon, iar la celălalt capăt al firului se află, de fapt, un angajat al callcentrului ilegal, care, prin scenarii bine puse la punct îl deposează de mijloacele ce-i aparțin.

În conformitate cu Raportul Autorității Bancare Europene, volumul și tehnicile fraudelor financiare diferă în funcție de instrumentul de plată utilizat. Astfel, deși cele mai mari pierderi financiare sunt generate de fraudele asociate transferurilor și ordinilor de plată, ponderea acestora în totalul tranzacțiilor este relativ redusă datorită volumului foarte mare de transferuri efectuate zilnic prin acest instrument. În schimb, plățile cu cardul și instrumentele de plată electronice, precum portofelele electronice, înregistrează o rată a fraudelor mai ridicată raportată la valoarea totală a tranzacțiilor efectuate prin aceste instrumente⁴.

Figura nr. 1 Evoluția fraudelor după tipul instrumentelor de plată (semestru 1 2022 -semestrul 2 2024).



Sursa: elaborat cu IA în baza EBA Report on Payment Fraud.

În conformitate cu datele din același Raport, între 60% în 2022 și 80% în 2024 din valoarea fraudelor care implică transferul ca și instrument de plată au fost realizate prin metode de inginerie socială și manipularea plătitorului, în timp ce între 40% în 2022 și 20% în 2024 din valoarea fraudelor aferente acestui instrument de plată vizează inițierea unui ordin de plată de către escroc prin manipularea accesului la cheile de autentificare ale victimei. Raportul dintre aceste 2 tipuri de fraudă sunt de 10% la 90% în cazul cardurilor și 13% la 87% în cazul instrumentelor de plată electronice (portofele electronice).

Când victima este manipulată să autorizeze tranzacțiile sugerate de escroci (așa-numitul Authorised Push Payment fraud), într-o astfel de situație, vorbim despre un consimțământ viciat. În marea majoritate a fraudelor care implică ingineria socială, tranzacția este autorizată de către victimă printr-un astfel de acord viciat de a efectua o anumită tranzacție. Cu toate acestea, dacă au fost respectate și satisfăcute toate condițiile pentru inițierea și efectuarea plății, atunci banca sau

⁴ European Banking Authority, & European Central Bank. (2025). 2025 Report on payment fraud (EBA/REP/2025/40), pag 11

operatorul instrumentului de plată, execută „indicația” clientului și autorizează plata sau transferul. În consecință chiar dacă consințământul este viciat, dar dacă sunt satisfăcute condițiile necesare pentru autorizarea plății, atunci aceasta se realizează, iar operatorul instrumentului de plată se

Studiu de caz:

Un locuitor din Briceni primește un SMS, aparent trimis de bancă (numărul scurt este identificat de telefonul mobil drept fiind numărul unei bănci comerciale). Prin mesaj victima este informată că pe contul său a fost detectată o tranzacție suspectă și că dacă nu a inițiat el tranzacția, trebuie să telefoneze urgent la numărul indicat pentru „blocarea fraudei”. Mesajul reprezintă un caz de smishing pentru că acesta vine, aparent, de la un număr de telefon autentic (numărul băncii) și TOAD (callback phishing), deoarece victima este îndemnată să inițieze singură apelul către un alt număr controlat de escroci.

După apelare, victima discută cu un pretins „operator bancar” care vorbește profesionist și afirmă că banii riscă să fie furați de o grupare criminală. În timpul conversației, fraudatorul exploatează stresul, frica și respectul față de autoritate pentru a determina victima să acționeze rapid fără a analiza critic situația. Aceasta reprezintă componenta de vishing.

Ulterior, victima este convinsă să instaleze o aplicație de acces la distanță „pentru securizarea contului” și să comunice codurile OTP primite prin SMS. În alte cazuri similare întâlnite recent în Republica Moldova, victimele sunt convinse să transfere banii într-un „cont sigur” sau chiar să retragă numerar și să-l transmită unor „curieri ai băncii” (money mule). După obținerea accesului și a codurilor de autentificare, escrocii efectuează transferuri frauduloase și golesc conturile victimei.

consideră că și-a onorat obligațiunea contractuală.

Responsabilitatea pentru prevenirea fraudelor de tip phishing este una partajată

Deși este clar că în cazul unei fraude organul competent este poliția, iar pentru transferul mijloacelor către escroci s-ar face vinovată persoana care s-a lăsat fraudată, în realitate lucrurile nu sunt chiar atât de simple.

Datorită gradului de sofisticare a schemelor frauduloase, care prin implicare inteligenței artificiale și a agenților IA pot fi extrem de dificil de identificat, responsabilitatea pentru identificarea și prevenirea fraudelor devine una tot mai partajată între diferite autorități responsabile.

Poliția Republicii Moldova

Conform prevederilor legale, poliția este responsabilă de constatarea infracțiunilor, identificarea și urmărirea autorilor, acumularea probelor, destructurarea grupărilor criminale și cooperarea internațională în investigarea fraudelor transfrontaliere.

În practică, poliția intervine, de regulă, după producerea fraudei și a prejudiciului, în special în cazurile de escrocherie, acces ilegal la sisteme informatice, fraude cu instrumente de plată, spălare de bani și utilizarea conturilor „money mule” (cont căraș de bani, folosit pentru intermedierea transferurilor fondurilor ilicite cu scopul de a ascunde originea ilicită a mijloacelor și identitatea infractorului). Totodată, poliția desfășoară activități de prevenire și informare publică privind noile

scheme de fraudă și cooperează cu băncile, operatorii de telecomunicații și alte instituții în procesul de investigare.

Conform bunelor practici internaționale, rolul poliției în combaterea fraudelor bazate pe inginerie socială poate deveni mult mai proactiv și orientat spre prevenție. Poliția ar putea dezvolta unități specializate dedicate fraudelor ce implică consimțământ viciat (APP) și fraudelor digitale, precum și programe de identificare și blocare a rețelelor de „money mules”.

Complementar, bunele practici europene presupun integrarea poliției în mecanisme de schimb rapid de date și „fraud intelligence” împreună cu băncile, operatorii de rețele de telecomunicații, STISC și autoritățile de reglementare, astfel încât conturile, numerele telefonice și infrastructurile utilizate în fraude să poată fi identificate și blocate aproape în timp real. Suplimentar, [Platforma națională de raportare a crimelor cibernetice](#) poate fi adaptată și popularizată și pentru raportarea potențialelor fraude financiare și de inginerie socială sau fraudelor cu active virtuale, devenind astfel platformă națională de raportare a crimelor cibernetice și fraudelor financiare.

BNM

Banca Națională setează regulile de activitate atât pentru bănci, cât și pentru operatorii sistemelor de plăți și aprobă standardele privind securitatea plăților și funcționarea infrastructurii financiare. În ultimii ani, BNM a consolidat semnificativ cadrul normativ aferent securității plăților și prevenirii fraudelor digitale. Spre exemplu, au fost instituite cerințe privind aplicarea autentificării stricte a clienților (Strong Customer Authentication – SCA), protejarea confidențialității, integrității și autenticității elementelor de securitate personalizate ale utilizatorilor serviciilor de plată, precum și implementarea unor standarde sigure de comunicare între prestatorii serviciilor de plată⁵. Complementar, BNM a consolidat cadrul de monitorizare și supraveghere a infrastructurilor și participanților implicați în procesarea plăților, stabilind inclusiv cerințe pentru emitenții instrumentelor de plată și pentru prestatorii de servicii de plată care accesează scheme internaționale de plăți și remiteri de bani⁶. Aceste măsuri ar trebui să contribuie la creșterea securității infrastructurii financiare și reducerea riscurilor asociate fraudelor digitale și accesului neautorizat la instrumentele de plată. Astfel, BNM este autoritatea cheie care poate verifica dacă instituțiile implementează autentificarea strictă a clienților (SCA); dacă elementele de securitate sunt protejate adecvat; dacă există mecanisme de gestionare a incidentelor și fraudelor; dacă infrastructura de plăți respectă standardele operaționale și de securitate; dacă participanții gestionează corespunzător riscurile operaționale și online. Totuși, în lipsa unor informații publice referitoare la controalele și rezultatele controalelor BNM pentru verificarea respectării acestor standarde și referitoare la incidentele și vulnerabilitățile identificate este dificil să înțelegem care este nivelul efectiv de conformare a entităților supravegheate. De cealaltă parte, BNM este responsabilă de elaborarea și implementarea politicilor de educație și incluziune financiară prin intermediul cărora poate capacita consumatorii de servicii de plată și să-i facă mai imuni la fraudele de inginerie socială.

⁵ [Hotărârea BNM nr. 12/2024](#) pentru aprobarea Regulamentului cu privire la autentificarea strictă a clienților și standardul deschis, comun și sigur de comunicare între prestatorii de servicii de plată

⁶ [Hotărârea BNM nr. 289/2024](#) privind monitorizarea infrastructurilor pieței financiare, schemelor, aranjamentelor și a instrumentelor de plată

În context, BNM ar putea intensifica supravegherea respectării cadrului normativ aferent securității plăților și prevenirii fraudelor digitale. Iar în conformitate cu bunele practici, BNM ar putea crește standardele de operare pentru băncile comerciale și operatorii sistemelor de plată astfel încât aceștia să devină proactivi în identificarea și combaterea fraudelor financiare. BNM poate cere băncilor și operatorilor sistemelor de plăți implementarea instrumentelor de monitorizare, în timp real, a mișcărilor în contul clienților pentru identificarea și blocarea automată a tranzacțiilor atipice. Complementar, conform bunelor practici UE, BNM ar putea solicita confirmarea beneficiarului (Confirmation/Verification of Payee (CoP/VoP)). În cazul în care nu coincide titularul contului declarat de plătitor cu cel real din registrele băncilor, tranzacția nu se autorizează de către entitatea bancară sau operatorul sistemului de plăți etc.

Băncile comerciale și operatorii sistemelor de plăți și monedă electronică

Băncile comerciale și operatorii sistemelor de plăți, reprezintă prima linie de apărare împotriva fraudelor financiare, deoarece aceștia gestionează infrastructura prin care sunt realizate transferurile inclusiv și tranzacțiile frauduloase. În prezent, băncile implementează mecanisme de autentificare multifactor (MFA) și campanii de informare privind fraudele.

Totuși, conform bunelor practici, instituțiile bancare și operatorii sistemelor de plăți pot avea un rol mult mai activ în prevenirea fraudelor cu implicarea tehnicilor de inginerie socială. Astfel, acești actori pot implementa un sistem de identificare automată a tranzacțiilor atipice și introducerea unor avertizări dinamice atunci când clientul efectuează transferuri cu risc ridicat. Complementar, băncile pot contribui la combaterea fraudelor prin schimb rapid de informații privind conturile suspecte și dezvoltarea unor mecanisme de verificare a beneficiarului plății (Confirmation/Verification of Payee) sau blocarea conturilor care sunt suspectate a fi conectate la activități de fraude financiare. Bunele practici denotă o schimbare majoră de abordare, băncile și operatorii sistemelor de plăți nu mai percep problema consimțământului viciat ca pe o problemă doar a victimei. În era inteligenței artificiale și a schemelor de fraudă tot mai sofisticate, băncile și operatorii sistemelor de plăți depun eforturi consolidate semnificative pentru identificarea și curmarea potențialelor fraude financiare.

Agencia națională pentru reglementare în comunicații - ARCOM

Deși Agenția Națională pentru Reglementare în Comunicații nu are competențe directe de investigare a fraudelor financiare, instituția joacă un rol foarte important în prevenirea și combaterea fraudelor de tip vishing, smishing și CLI spoofing, deoarece acestea utilizează infrastructura comunicațiilor electronice. În 2025–2026, ARCOM a consolidat cadrul de reglementare în acest domeniu și l-a structurat pe două niveluri.

Primul nivel (opțional) este dat de Ghidul de recomandări pentru detectarea și combaterea CLI spoofing⁷, care le propune operatorilor patru modalități tehnice de combatere a fenomenului de

⁷ Hotărârea Consiliului de Administrație al ARCOM nr. [33 din 23.09.2025](#), prin care a fost aprobat „[Ghidul de recomandări pentru detectarea și combaterea CLI Spoofing](#)”; modificată prin Hotărârea nr. [5 din 29.01.2026](#).

afișare frauduloasă a identității apelantului: i) liste DNO, numere care nu inițiază niciodată apeluri (precum 112 sau numărul de pe reversul cardului bancar); ii) liste dinamice de permitere și blocare a apelurilor; iii) sistem de validare a apelurilor mobile de intrare folosind un server proxy) și iv) soluția GSMA Open Gateway (Number Verification API), prin care operatorii își confirmă reciproc autenticitatea numărului afișat. Având în vedere caracterul de recomandare al Ghidului, implementarea acestor metode rămâne, în principiu, la latitudinea furnizorilor, cu condiția respectării obligațiilor instituite prin condițiile de licență⁸.

Al doilea nivel (obligatoriu) îl reprezintă noile condiții generale de licență pentru utilizarea resurselor de numerotație⁹, care obligă operatorii de servicii de comunicații să blocheze apelurile recepționate pe trunchiurile internaționale în următoarele situații: (i) apelurile care afișează numere din Planul Național de Numerotație al Republicii Moldova care, potrivit destinației acestora, nu pot fi utilizate pentru inițierea apelurilor; (ii) apelurile care afișează numere nongeografice (formatul numărului nu este legat de localizarea geografică a utilizatorului) destinate serviciilor mobile, care nu sunt atribuite prin licență sau pentru care licența de utilizare a resurselor de numerotație a fost suspendată, retrasă ori a expirat; (iii) apelurile care afișează numere geografice, numere naționale scurte sau numere utilizate pentru servicii independente de locație, cu excepția apelurilor legitime de roaming internațional identificate prin Mobile Station Roaming Number (MSRN - număr temporar alocat de rețeaua gazdă unui abonat aflat în roaming); și (iv) apelurile recepționate fără identificatorul liniei apelante (CLI). Aceste obligații sunt aliniate tendințelor recente de reglementare existente la nivel european. Spre exemplu, de în România, ANCOM a impus, prin decizii individuale adresate furnizorilor cu interconectare internațională, blocarea, începând cu 7 iulie 2025, a apelurilor din străinătate care afișează numere românești din alte domenii decât cele mobile ori numere cu structură nevalidă, cu aceleași excepții pentru utilizările legitime¹⁰ (ex: în roaming).

Efectul măsurilor întreprinse de ARCOM în Republica Moldova este unul de rezonanță: peste 1 milion de apeluri frauduloase au fost blocate doar în primul trimestru al anului 2026, potrivit datelor raportate, deocamdată opțional, de furnizori¹¹ și comunicate public de ARCOM.

În pofida noilor condiții de licențiere care cer operatorilor combaterea fenomenului de CLI spoofing, nivelul obligator al cadrului autohton rămâne destul de limitat.

⁸ Ghid, pct. 25 și pct. 51: Ghidul își declară caracterul orientativ, implementarea metodelor rămânând la discreția furnizorilor, respectiv opțională.

⁹ Hotărârea Consiliului de Administrație al ARCOM [nr. 46 din 17.11.2025](#) privind aprobarea Condițiilor generale de licență pentru utilizarea resurselor de numerotație din Planul național de numerotație al Republicii Moldova (în continuare CGLPURNPNN); în vigoare de la 01.01.2026, potrivit pct. 4 al hotărârii.

¹⁰ [„ANCOM ia măsuri împotriva fraudelor comise prin apelurile efectuate în numele unor instituții publice, bănci sau companii de stat”](#), ANCOM, comunicat de presă, 4 iunie 2025.

¹¹ Anexa Ghidului (pag. 18), nota la poziția 4, introdusă prin Hotărârea nr. 5/2026: raportarea volumelor de apeluri blocate „se realizează în mod opțional de către furnizori”.

Pentru obligațiile anti-spoofing incluse în condițiile noi de licențiere nu s-a prevăzut nicio perioadă tranzitorie, ceea ce înseamnă implementarea deplină a acestor prevederi cu începere de la 1 ianuarie 2026. Intervalul de circa șase săptămâni dintre adoptare și intrarea în vigoare, a fost, la modul practic, termen de conformare, comparabil ca durată cu cel acordat de ANCOM operatorilor români. Cu toate acestea, potrivit punctului 67 din condițiile generale de licență (CGLPURNPNN), pentru satisfacerea responsabilității de combatere a fenomenului de CLI spoofing, operatorii pot agreea cel puțin o singură metodă din Ghid ¹². Această formulare poate fi interpretată, în practică, drept o condiție suficientă de conformare. De cealaltă parte, o singură metodă din cele 4 reflectate în Ghid, nu poate însă acoperi standardele cumulative ale pct. 66 din CGLPURNPNN privind detectarea și filtrarea, în timp real, la punctele de interconectare și de intrare în rețea, plus blocarea traficului abuziv. Ambiguitatea acestor formulări, le oferă operatorilor un argument în eventualele proceduri de sancționare, „cel puțin una” rămânând singurul reper cuantificat al întregului cadru metodologic.

Totodată, noile condiții de licențiere nu stabilesc rigori clare de raportare privind tehnologia utilizată, apelurile blocate pe tehnologie, incidentele de blocare eronată (fals pozitive) etc. Obligația titularilor de licență se limitează la furnizarea informațiilor necesare verificării de către agenție¹³, iar raportarea statistică trimestrială a apelurilor frauduloase, deși formulată imperativ (transmitere până la data de 20 a lunii următoare trimestrului)¹⁴, este reflectată într-un document cu caracter de recomandare, totodată, indicatorul-cheie: apelurile blocate, rămâne, explicit opțional¹⁵. Astfel, atestăm un decalaj între obligația formală și conformarea demonstrată. Dovada implementării nivelului obligatoriu al cadrului autohton de combatere a fenomenului de CLI spoofing se sprijină, deocamdată, pe declarațiile operatorilor și oficialilor ARCOM, nu pe date de conformare verificabile.

Limita structurală, valabilă atât în Republica Moldova, cât și în unele state membre ale UE (de exemplu, România), constă în faptul că apelurile internaționale care afișează numere mobile naționale nu pot fi blocate în totalitate în mod automat. Deși apelurile internaționale care prezintă fraudulos numere naționale sunt, ca regulă, blocate, o excepție o constituie apelurile cu identificatorul unei linii mobile naționale aparținând altui furnizor (off-net), care pot proveni în mod legitim de la abonați aflați în roaming internațional. În lipsa unui mecanism interoperator de verificare în timp real a autenticității CLI și a statutului de roaming, aceste apeluri nu pot fi diferențiate cu certitudine de cele frauduloase fără riscul blocării comunicațiilor legitime.

¹² CGLPURNPNN , pct. 67: furnizorii „pot agreea, de comun acord, cel puțin una din metodele” prevăzute de Ghid – document calificat de același punct drept unul de bune practici, cu caracter de recomandare; tot pct. 67 permite Agenției să emită reglementări sau instrucțiuni suplimentare.

¹³ CGLPURNPNN , pct. 64–65: Agenția monitorizează, supraveghează și controlează respectarea condițiilor, iar titularii au obligația de a furniza „toate informațiile necesare pentru a verifica respectarea” acestora.

¹⁴ [Ghid](#), pct. 80 (în redacția Hotărârii nr. 5/2026), coroborat cu pct. 79, care ancorează obligativitatea furnizării informațiilor solicitate în art. 25 alin. (16) pct. 7) din Legea nr. 241/2007 și în art. 26 alin. (1) lit. a) și art. 35 alin. (2) din Legea nr. 72/2025.

¹⁵ Anxa la Ghid.

În contextul actual, ARCOM ar putea continua eforturile de combatere a fenomenului de fraude telefonice pe, cel puțin, trei dimensiuni.

Pe dimensiunea standardelor și a conformării, ARCOM ar putea să: i) precizeze prin instrucțiunile pe care conform pct. 67 din condițiile de licență le poate emite, că implementarea uneia sau mai multor metode din Ghid nu constituie, prin ea însăși, dovada conformării cu pct. 66 (CGLURNPNN), conformitatea urmând a fi evaluată prin acoperirea tuturor punctelor de interconectare internațională cu detectarea și filtrarea, în timp real, capacitatea de blocare pentru categoriile de la pct. 25 și implementarea unui mecanism de verificare, în timp real, a autenticității CLI și a statutului de roaming al numerelor mobile naționale; ii) stabilească, prin aceleași instrucțiuni, termene și jaloane verificabile pentru agrearea de către operatori a metodelor de combatere a fenomenului de CLI spoofing și pentru operaționalizarea obligației generale de securitate, dublate de obligația titularilor de licență de a atesta formal implementarea măsurilor de blocare deja exigibile și metodele agreate; iii) instituie, o raportare periodică de conformare distinctă de statistica apelurilor, verificată prin control și reflectată într-un tablou public, pe fiecare operator separat și pe metodă de combaterea a fenomenului de CLI spoofing, prin publicarea periodică a unor indicatori agregați sau individualizați, în condițiile legii.; iv) și să consolideze raportarea statistică, transferând raportarea trimestrială din Ghid într-un act cu forță juridică obligatorie.

Totodată, ARCOM poate continua consolidarea cadrului de reglementare prin implementarea mecanismelor interoperatorii obligatorii de verificare a autenticității CLI, inclusiv prin operaționalizarea soluției bazate pe Number Verification API. De asemenea, poate să operaționalizeze baza de date națională DNO, a cărei creare s-a angajat să o analizeze¹⁶; și să aplice mecanismul asumat prin Ghid: revenirea cu reglementări obligatorii dacă statisticile arată că fenomenul nu scade¹⁷.

Pe cea de-a 3-a dimensiune, a eforturilor de combatere a fraudelor telefonice, ARCOM ar putea să extindă eforturile, pentru a acoperi și SMS-urile frauduloase (smishing), pe care actualul ghid, dedicat exclusiv apelurilor vocale, nu le acoperă¹⁸ pentru că voce și SMS-urile circulă prin stive tehnologice diferite. În context, ARCOM ar putea și să întărească cerințele de identificare la portarea numerelor și la înlocuirea cartei SIM (împotriva fraudelor de tip SIM swap). Totodată, autoritatea ar putea și să faciliteze schimbul rapid de informații cu băncile, STISC și organele de drept privind numerele și infrastructurile utilizate în fraude.

¹⁶ [Ghid](#), secțiunea 5.3 lit. a), nota: Agenția va analiza posibilitatea creării unei baze de date naționale a numerelor DNO, accesibilă furnizorilor pentru verificarea și blocarea în timp real a apelurilor.

¹⁷ [Ghid](#), pct. 79.

¹⁸ [Ghid](#), pct 1 subpunct 7., pag 4 „Cu toate acestea, prezentul ghid vizează în principal examinarea și evaluarea inițiativelor de reglementare și a soluțiilor tehnice **destinate combaterii falsificării CLI, exclusiv în contextul apelurilor vocale.**”

Centrul Național pentru Protecția Datelor cu Caracter Personal (CNPDPCP)

Deși protecția datelor cu caracter personal nu vizează direct investigarea fraudelor, datele personale reprezintă una dintre principalele resurse utilizate în atacurile de tip phishing și fraudele de inginerie socială. Informațiile despre numărul de telefon, nume, prenume, rude, tranzacții sau locul de muncă permit escrocilor să construiască scenarii credibile și să manipuleze mult mai ușor victimele. În acest context, autoritatea responsabilă de protecția datelor cu caracter personal poate contribui la diminuarea fraudelor prin supravegherea modului în care operatorii gestionează și securizează datele personale, prin investigarea scurgerilor de date și promovarea unor standarde mai ridicate privind protecția datelor cu caracter personal.

În contextul intensificării comerțului la distanță și incidența tot mai mare a situațiilor când platformele online colectează multe date cu caracter personal despre clienți precum: număr de telefon, nume, prenume, adrese de livrare etc, devine foarte importantă intensificarea acțiunilor de informare și educare a societății asupra importanței protecției datelor cu caracter personal, ghidarea operatorilor de date cu caracter personal referitor la modul în care aceștia pot asigura aplicarea corectă a legislației în acest domeniu, dar și intensificarea controalelor pe bază de risc.

CNPF

CNPF, prin mandatul de protecție a consumatorilor, contribuie la diminuarea riscurilor asociate fraudelor financiare realizate cu utilizarea conturilor de plăți, prin supravegherea conduitei prestatorilor de servicii de plată, precum și prin activități de informare și educație financiară.

În materie de activitate de supraveghere, CNPF verifică modul în care prestatorii își respectă obligațiile legale față de consumatori în cazurile efectuării unor operațiuni frauduloase cu utilizarea instrumentelor de plată, precum și cazurile de pierdere, furt, sau utilizare fără drept a acestora. Astfel, CNPF poate verifica dacă prestatorul a informat consumatorul cu privire la drepturile și obligațiile sale, dacă a pus la dispoziție canale de notificare, dacă a întreprins măsuri de blocare sau securizare a instrumentelor de plată după notificarea consumatorului și dacă a aplicat corect regimul legal privind corectarea sau restituirea sumelor aferente operațiunilor neautorizate ori executate necorespunzător.

În materie de educație financiară, autoritatea se concentrează pe creșterea gradului de conștientizare a consumatorilor cu privire la riscurile de fraudă, precum și cunoașterea pașilor de urmat în cazul pierderii, furtului, compromiterii sau utilizării neautorizate a instrumentului de plată.

CNPF poate continua efortul de comunicare, informare și educare a consumatorului, intensificând, în același timp, și eforturile de supraveghere a conduitei prestatorilor de servicii de plată.

Agenții economici

Companiile private joacă și ele un rol extrem de important în reducerea riscurilor asociate phishing-ului și fraudelor de inginerie socială, în special în contextul fraudelor cu facturi false și Business Email Compromise (BEC). Totodată, datele pe care le colectează agenții economici despre clienții lor, dacă nu sunt gestionate cu diligență și ajung pe mâna escrocilor, vor fi utilizate pentru regizarea fraudelor de inginerie socială.

În acest context, agenții economici pot contribui la prevenirea fraudelor prin implementarea autentificării multifactor, instruirea periodică a personalului privind phishing-ul și fraudele de inginerie socială. Conform bunelor practici internaționale, companiile ar trebui să trateze phishing-ul nu doar ca pe o problemă IT, ci ca pe un risc operațional și financiar major. Complementar, mediul de afaceri trebuie să manifeste maximă prudență atunci când intră în posesia și prelucrează datele cu caracter personal ale clienților, pentru a nu admite ca aceste date să ajung pe mâna escrocilor.

În căutarea compromisului dintre securitate, cost și libertate

Combaterea fraudelor digitale și a phishing-ului presupune identificarea permanentă a unui compromis între securitate, costuri, comoditate, libertate și intimitate personală. Astfel, deși operatorii de plăți ar putea implementa sisteme sofisticate de monitorizare a tranzacțiilor pentru identificarea și blocarea tranzacțiilor atipice, costurile implementării acestor soluții vor fi transferate către consumatori prin comisioane de administrare. De cealaltă parte, monitorizarea comportamentului atipic înseamnă, de de-o parte, reducerea libertății individuale din cauza creșterii supravegherii tranzacțiilor. De cealaltă parte, dacă unele tranzacții ar putea fi interpretate de către aceste sisteme de monitorizare drept fiind suspecte fără ca acestea să fie neapărat ilicite, aceasta ar implica necesitatea unei intervenții din partea plătitorului pentru deblocarea contului sau a tranzacției înghețate etc ceea ce poate reprezenta un disconfort major pentru consumatori.

Introducerea tehnologiilor de contracarare a fenomenelor de CLI spoofing și smishing vor duce și ele la o diminuare considerabilă a intimității consumatorilor de servicii de telefonie mobilă, dar și transferul către aceștia a costurilor implementării tehnologiilor specializate.

Implementarea standardelor avansate de securitate, audit, criptare și conformare în ceea ce privește operarea datelor cu caracter personal, presupune investiții considerabile în infrastructură și expertiză tehnică, care poate afecta grav și disproporționat agenții economici, mai cu seamă pe cei mici, care ar putea să nu-și poată permite aceste cheltuieli. În astfel de circumstanțe, costurile conformării pot deveni chiar și prohibitive, afectând sustenabilitatea activității companiei.

În context, trebuie să înțelegem că implementarea măsurilor moderne de combatere a fraudelor și a phishing-ului implică atât costuri financiare directe, cât și costuri indirecte legate de reducerea comodității, creșterea supravegherii și diminuarea nivelului de intimitate de care utilizatorii se pot bucura. Din acest motiv, politicile antifraudă eficiente trebuie să urmărească un echilibru rezonabil între nivelul de securitate dorit și costurile economice și sociale pe care suntem dispuși să le acceptăm.

Acțiuni imediate pe care le putem întreprinde pentru a ne proteja de fraudele de inginerie socială

Deși astfel de fraude devin tot mai sofisticate și mai periculoase, există acțiuni pe care le putem întreprinde imediat pentru a ne proteja și a diminua riscul asociat acestora.

- Opriți imediat conversația și informați banca / prestatorul de servicii de plată nebanca, cu privire la fraudă, însușirea frauduloasă a instrumentului de plată sau de orice altă utilizare

neautorizată a acestuia. Unii prestatori oferă posibilitatea de blocare a oricăror operațiuni direct în aplicații. Sesizați poliția și autoritățile dacă: i) cineva vă telefonează și pretinde că este reprezentantul băncii, poliției, serviciului fiscal, rude, reprezentantul companiei mobile etc și vă solicită să-i comunicați codul OTP, parole, mutarea banilor pe "un cont sigur", instalarea urgentă a diferitor aplicații pe dispozitivele dvs etc; ii) interlocutorii dvs. încearcă să creeze: panică; urgență; frică; impresia unei autorități legitime; sentimentul că trebuie să acționați imediat.

- Nu aveți încredere în numărul afișat pe ecran! Acesta poate fi falsificat prin tehnici de CLI spoofing. Chiar dacă pe telefon apare denumirea băncii sau un număr aparent legitim (bancă, poliție, furnizor etc), la celălalt capăt al firului poate fi un infractor. Astfel, dacă vă încearcă un sentiment că parcă nu este ceva în regulă închideți imediat telefonul și încercați dvs să luați legătura cu reprezentanții băncii sau instituției apelante pentru a clarifica situația dar folosiți doar numărul oficial, afișat pe pagina acestora.
- Dacă vedeți afișat numărul rudelor, prietenilor, dar la celălalt capăt al firului vorbește sau bănuiți că vorbește o altă persoană, închideți apelul și telefonați dvs. ruda sau prietenul. Prin spoofing se poate falsifica afișarea numărului, dar nu și preluarea unui număr legitim.
- Nu accesați link-uri primite prin SMS sau aplicații de mesagerie dacă acestea creează: panică; presiune; promisiuni financiare; urgență etc.
- Fiți foarte atenți la ce coduri QR scanați cu dispozitivul dvs quishing-ul (phishing prin coduri QR) vă poate manipula să credeți că ați nimerit pe o pagină legitimă a băncii dvs, sau să declanșeze instalarea unei aplicații care vă poate fura identitatea sau accesul la dispozitiv.
- Nu publicați excesiv informații personale online. Escrocii folosesc: rețelele sociale; informațiile de pe platformele de angajare/recrutare; sau informații publice pentru ași identifica potențialele victime și a alege mai bine strategia de inginerie socială. Cu cât atacatorul știe mai multe despre dumneavoastră, cu atât manipularea devine mai eficientă.
- Verificați atent orice solicitare privind schimbarea unui IBAN sau efectuarea unor plăți neobișnuite.
- Dacă suspectați că ați devenit victima unei fraude: contactați imediat banca; solicitați blocarea contului și/sau cardului; anunțați poliția; păstrați mesajele, numerele și capturile de ecran, informați poliția și partajați experiența dvs cu alții pentru ca și ceilalți să fie informați despre riscul de fraudă. În fraudele digitale, viteza reacției este extrem de importantă. Primele minute după transfer pot face diferența între recuperarea și pierderea definitivă a banilor.

Pentru a afla mai multe despre fraudele de inginerie socială sau despre fraudele cu activele virtuale și cum ne protejăm de acestea, puteți interacționa cu [asistentul virtual IA](#) dezvoltat în acest scop.

Campania națională de informare a consumatorilor



Acest material a fost produs cu suportul financiar al Uniunii Europene și al Fundației Soros Moldova. Conținutul acestuia reprezintă responsabilitatea exclusivă a proiectului „Consolidarea cadrului de protecție a consumatorului în Republica Moldova”, implementat de către Centrul Analitic Independent „Expert-Grup” în calitate de lider de consorțiu, în parteneriat cu Institutul pentru Politici și Reforme Europene, și finanțat de către Uniunea Europeană și Fundația Soros Moldova.