

MINISTERUL AFACERILOR INTERNE



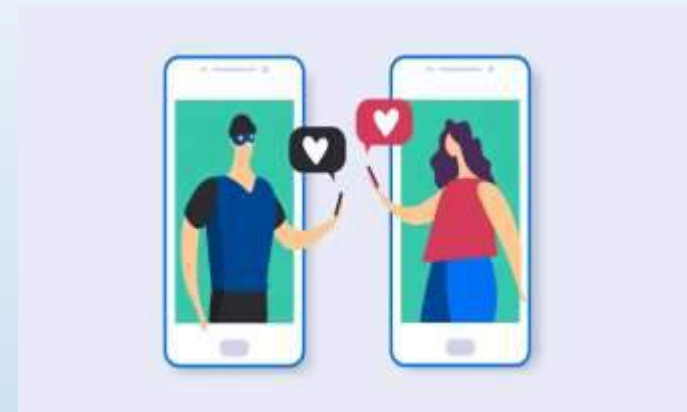
INSPECTORATUL GENERAL AL POLIȚIEI ROMÂNE
INSPECTORATUL DE POLIȚIE AL JUDEȚULUI SATU MARE
Compartimentul Analiza și Prevenirea Criminalității

CAMPANIE DE PREVENIRE A FRAUDELOR INFORMATICE



Cele mai întâlnite tipuri de fraude în mediul online

- Frauda "Mesaj de la șef"
- Fraude cu facturi
- Frauda care se ascunde în spatele unei probleme tehnice
- **Phishing/Smishing/Vishing**: autorii te apelează telefonic, îți trimit un mesaj text (SMS) ori un e-mail
- Website-uri bancare contrafăcute



- **Iubire prefăcută**
- Fraudă de tip loterie
- Frauda cu produse gratis sau foarte ieftine
- Furtul de date personale
- Spoofing-ul
- Fraude în domeniul cumpărăturilor online
- **Fraude cu investiții**

Frauda „Mesaj de la șef” CEO fraud

Vizând angajații autorizați să efectueze plăți, autorul sună sau trimite un e-mail, pretinzând că este unul din managerii de top din companie și îi determină să plătească o factură falsă ori să efectueze un transfer din contul firmei.

FRAUDA "MESAJ DE LA ȘEF"

Frauda "Mesaj de la șef" vizează angajații autorizați ca efectueze plăți, care, prin inducere în eroare, sunt determinați să plătească o factură falsă ori să efectueze un transfer.

CUM FUNCȚIONEAZĂ?

Un autor sună sau trimite un e-mail, pretinzând să este unul din managerii de top din companie.

De obicei este bine informat cu privire la organizație.

Solicită efectuarea urgentă a unei plăți.

Folosește un limbaj persuasiv, de tipul: "avem încredere în tine, rămâne între noi, eu sunt ocupat acum".

Se referă la o situație sensibilă (ca. control autorităț, audieri etc.).

Deeseori, solicită ca plata să se facă într-un cont din afara țării și chiar a Europei.

Angajatul transferă banii într-un cont al autorului.

Instrucțiuni complete pot fi trimise mai târziu, de către o persoană sau prin e-mail.

Angajatului i se cere să nu respecte procedura obișnuită de autorizare a plăților.

CARE SUNT SEMNELE?

- E-mail sau apel telefonic neobișnuit.
- Contact cu un oficial cu care nu ești în legătură directă, în mod normal.
- Solicitare de confidențialitate.
- Presiune sub semnul presupusei urgențe.
- Solicitare neobișnuită, scită din țipărele procedurilor interne.
- Amenințări sau promisiuni neobișnuite, fitate.

CE POTI FACE?

CA ORGANIZAȚIE

- Constituiți-vă un sistem și asigurați-vă că angajații au informații permanente.
- Instruiți-vă staff-ul să manifeste atenție maximă la efectuarea plăților.
- Implementați proceduri interne stricte referitoare la plăți.
- Implementați proceduri de verificare a legitimității plăților solicitate prin e-mail.
- Stabiliți reguli de raportare a tentativelor de fraudă.
- Verificați datele publicate pe site-ul companiei, restricționați accesul la datele importante și fiți atenți la rețelele sociale.
- Actualizați soluțiile tehnice de securitate.

☎ Solicitați poliția la orice încercare de fraudă, chiar dacă nu ați devenit victima acesteia.

CA ANGAJAT

- Respectați cu strictețe procedurile de securitate în cazul plăților și achizițiilor. Nu săriți nică să pas procedural și rezistați presiunilor.
- Verificați cu atenție adresele de e-mail când primiți solicitări de informații sensibile/transfereți de bani.
- Dacă aveți dubii în cazul unui transfer de bani, consultați un coleg.
- Niciodată nu deschideți link-uri sau atașamentele stufăscă primite prin e-mail. Fiți foarte atenți când verificați mail-ul personal pe calculatorul de serviciu.
- Manifestați precauție și restricționați informațiile de pe rețelele sociale.
- Evitați publicarea de date despre conducerea, securitatea sau procedurile firmei.

⚠ Dacă primiți un e-mail suspect, informați imediat departamentul IT.

EUROPOL
CO B I 2019

MI

POLIȚIA ROMÂNĂ

#CyberScam

FRAUDE CU FACTURI

CUM FUNCȚIONEAZĂ?

- > O firmă este contactată de cineva care pretinde că este reprezentantul unui furnizor.
- > Poate fi o abordare încrucizată - prin telefon, acțiune, e-mail etc.
- > Autorul solicită modificarea datelor bancare (numărul de cont, banca la care e deschis etc) pentru plățile viitoare. Noul cont este deținut/controlat de acesta.



CE PUTEȚI FACE?

Asigurați-vă că angajații sunt informați și cunosc acest tip de fraudă și cum să îl evite.

Implementați proceduri clare de verificare a legitimității plăților.

Verificați orice solicitare preținsă a fi, din partea creditorilor. În special dacă cer modificarea datelor bancare pentru viitoare plăți.

Folosiți datele de contact din corespondența anterioară pentru a verifica și nu pe cele din mesajul prin care se solicită modificările.

Stabiliți puncte de contact unice cu companiile partenere către care efectuați plăți regulate.

CA ORGANIZAȚIE



Instruiți-vă personalul ca întotdeauna să verifice orice neregulă posibilă la plățile facturilor.

Realizați informațiile postate pe site-ul companiei, în special referitor la contracte și furnizori. Limitați datele despre companie pe care angajații le pot posta pe rețelele sociale.

Pentru plăți peste o anumită sumă, instituiți o procedură suplimentară de verificare cu beneficiarul.

CA ANGAJAT



Fii precaut cu datele despre locul de muncă pe care le postezi pe rețelele sociale.

Când efectuați o plată, trimiteți un e-mail de confirmare destinatarului. Pentru siguranță, includeți denumirea bancii și ultimele 4 cifre ale numărului de cont.



Sesizați poliția la orice încercare de fraudă, chiar dacă nu ați devenit victima acesteia.

Fraude cu facturi Invoice fraud

O firmă este contactată de cineva care pretinde că este reprezentantul unui furnizor de bunuri/servicii legitim. Angajații cu atribuții de efectuare de plăți sunt determinați să plătească, pe viitor, facturi false în conturile autorilor.

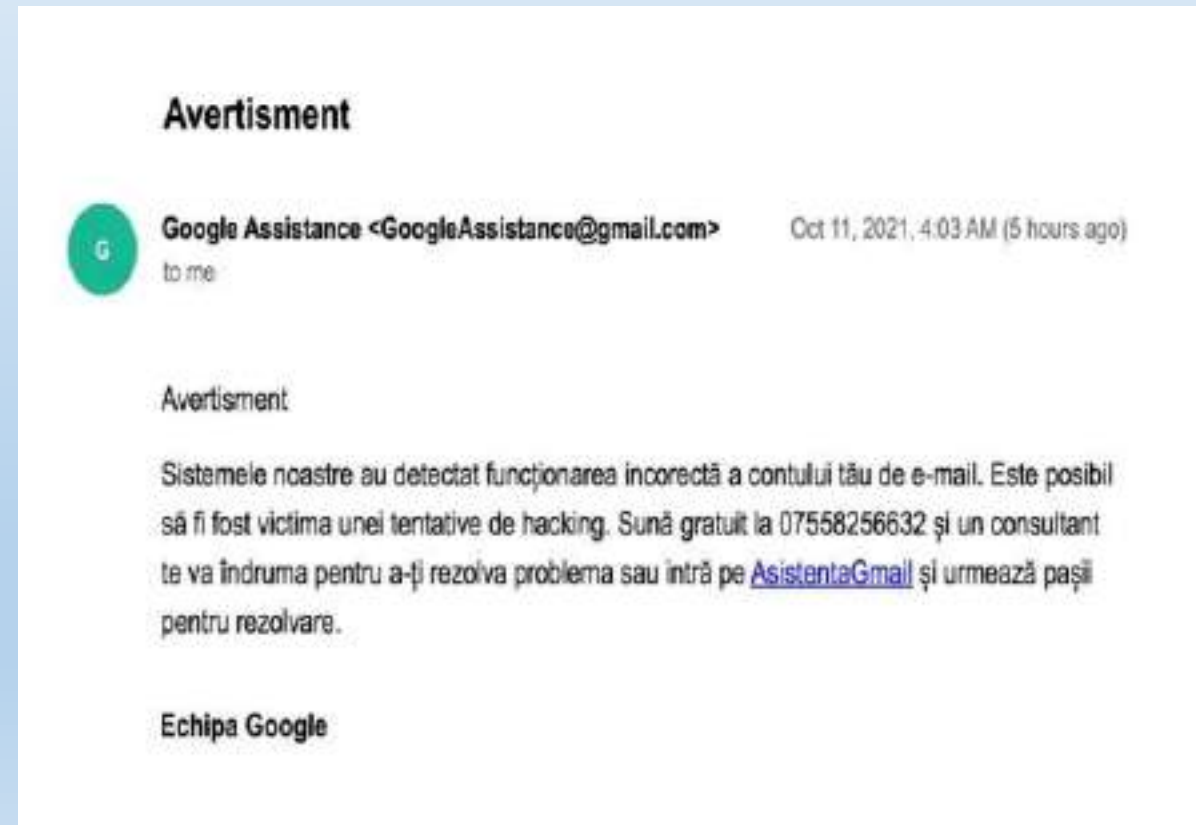
Frauda care se ascunde în spatele unei „probleme tehnice”

Escrocheriile de tipul asistență tehnică încep cu un **avertisment pop-up cu privire la o anumită problemă** a computerului sau a conturilor tale online (ex. email).

Fereastra pop-up îți oferă un număr de telefon la care să apelezi sau un link de reply.

Un fals angajat Microsoft sau Apple răspunde la telefon și te convinge să le dai acces la computerul tău, astfel încât să poată rezolva problema.

Apoi, fie îți accesează banca prin computer, fie solicită o plată pentru reparațiile menționate.



Phishing/ Smishing / Vishing

Autorii te apelează telefonic, îți trimit un mesaj text (SMS) ori un e-mail, prin care te induc în eroare, pentru a-ți divulga date personale, financiare ori de securitate.

PHISHING PRIN SMS

Smishing (combinație de cuvinte dintre SMS și Phishing) este încercarea de inducere în eroare prin mesaje text, pentru obținerea de date personale, bancare ori de securitate.



CUM FUNCȚIONEAZĂ?

Prin mesajul text (SMS), autorii, de obicei, îți solicită să apelezi un număr de telefon sau să accesezi un link prin care "ți verifici, actualizezi, reactivezi" contul. Dar... în realitate ești direcționat către un site fals sau un operator complice, pretinzând reprezentant al băncii.

CE POTI FACE?

- Nu accesa link-uri, atașamente sau imagini nesolicitate, primite prin SMS de la persoane necunoscute.
- Nu acționa în grabă. Ia-ți timp și verifică informațiile înainte de a trimite un eventual răspuns.
- Niciodată nu răspunde unui SMS prin care ți se solicită codul PIN, parole de acces la contul de online banking ori alte credențiale de siguranță.
- Contactează imediat banca, dacă știi că ai răspuns unui astfel de mesaj și ai furnizat detalii bancare în aceste condiții.

E-MAIL-URI TIP PHISHING

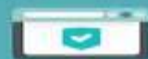
Phishing se referă la mesaje false care induc în eroare destinatarul, pentru a-și divulga date personale, financiare ori de securitate.

CUM FUNCȚIONEAZĂ?

Aceste e-mail-uri:

pot arăta identic cu acelea pe care le primești de la bancă.

imită logo-ul și designul mesajelor reale.



utilizează un limbaj care sugerează urgența.



ți solicită să descarci un atașament sau să deschizi un link.



Infractorii informatici se bazează pe faptul că oamenii sunt ocupați; la prima vedere, aceste e-mail-uri par legitime.



Atenție la folosirea dispozitivelor mobile. Poate fi mai dificil de depistat o încercare de phishing pe telefonul mobil sau pe tabletă.

CE POȚI FACE?

- Actualizează permanent programele calculatorului, inclusiv sistemul de operare.
- Fii extrem de atent dacă primești mesaje "din partea băncii" prin care ți se solicită date sensibile (date despre cont, parole etc.).
- Citește cu atenție mesajele - compară adresa expeditorului cu cea din corespondențele anterioare. Verifică eventuale greșeli de exprimare.
- Nu răspunde la mesaje dubioase. Eventual, le poți retransmite băncii tale, scriind adresa.
- Nu deschide link-urile și nu descărca atașamentele din astfel de mesaje.
- Dacă ai dubii cu privire la o tranzacție, efectuează verificări suplimentare.

#CyberScams



SITE-URI BANCARE FALSE

E-mail-urile tip phishing includ de obicei link-uri care te direcționează către site-uri bancare contrafăcute, unde îți se solicită să îți divulgi date personale și financiare.



CARE SUNT SEMNELE?

Site-urile false arată aproape identic cu cele legitime. Cel mai des, acestea te conduc către o fereastră pop-up, unde îți se cer credențialele bancare. Site-urile reale nu folosesc astfel de ferestre.

În astfel de mesaje de obicei apar:

Urgența: nu veți găsi asta pe site-urile legitime.



Ferestre tip pop-up: sunt de obicei folosite pentru culegerea datelor tale. Nu le accesa și evită introducerea datelor personale în astfel de ferestre.

Design defectuos: fiți atenți la site-urile care conțin greșeli gramaticale ori de exprimare.

CE POȚI FACE?



Niciodată nu accesa site-ul băncii tale prin link-uri trimise pe e-mail.



Tastează manual adresa băncii când vrei să accesezi site-ul acesteia.



Folosește browsere care permit blocarea ferestrelor pop-up.



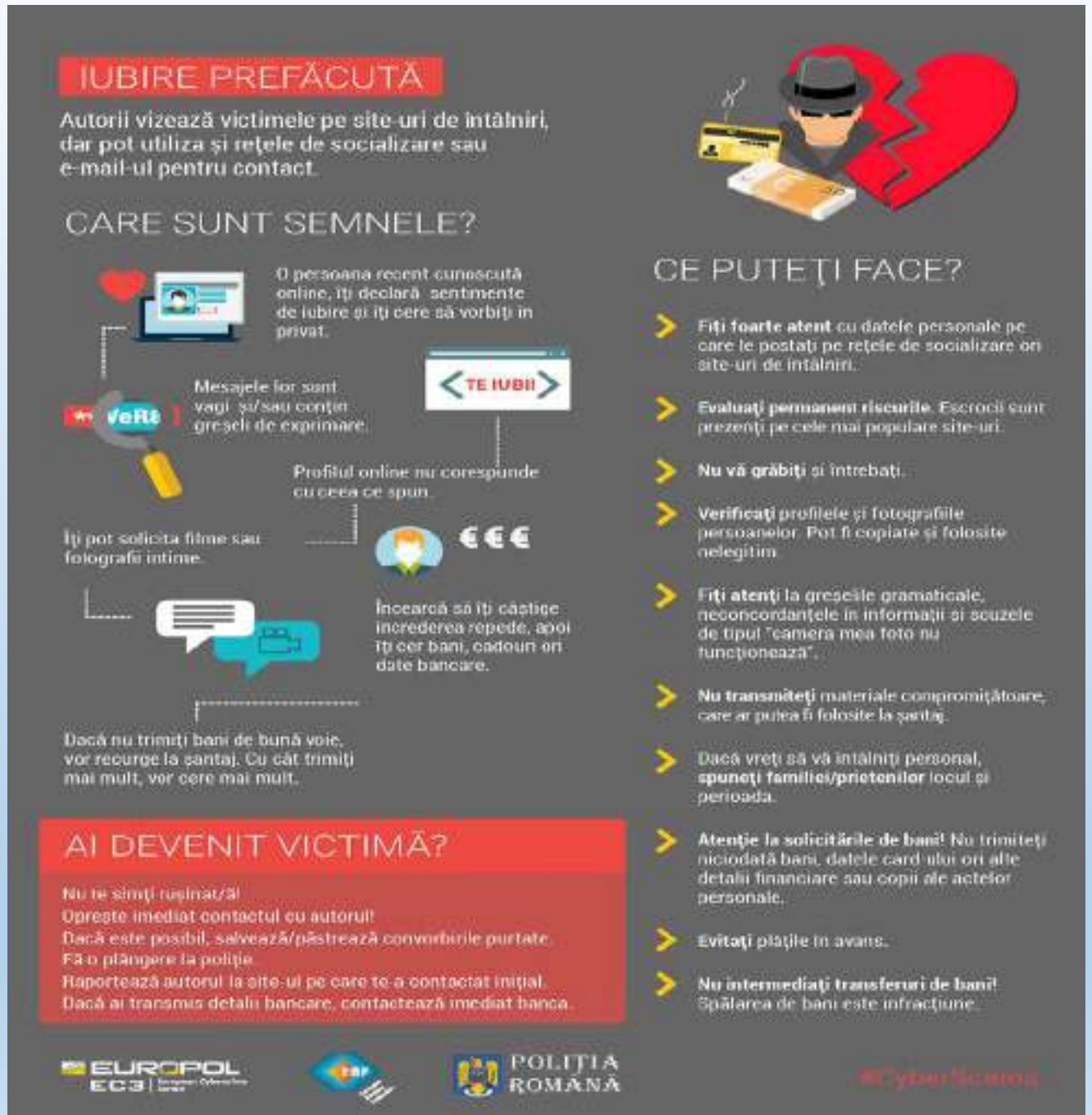
Dacă banca are ceva important să îți comunice, vei fi notificat după ce îți vei accesa contul online.

Website-uri bancare contrafăcute (Spoofed bank website fraud)

Autorii folosesc mesaje de tip "phishing" cu link-uri către site-uri bancare false. Odată ce ai accesat link-ul, prin metode diverse, și se colectează ilegal datele personale și/sau bancare. Site-ul contrafăcut va arăta precum cel legitim pe care îl imită, cu foarte mici diferențe, deseori greu sesizabile.

Iubire prefăcută (Romance scam)

Autorii pretind că sunt îndrăgostiți și își doresc o relație cu potențiala victimă. Deși debutează pe site-uri de întâlniri, sunt folosite conturi false de e-mail sau pe rețele sociale pentru menținerea contactului, câștigarea și exploatarea încrederii.



IUBIRE PREFĂCUTĂ

Autorii vizează victimele pe site-uri de întâlniri, dar pot utiliza și rețele de socializare sau e-mail-ul pentru contact.

CARE SUNT SEMNELE?

- O persoană recent cunoscută online, îți declară sentimente de iubire și îți cere să vorbești în privat.
- Mesajele lor sunt vagi și/sau conțin greșeli de exprimare.
- Profilul online nu corespunde cu ceea ce spun.
- Îți pot solicita filme sau fotografii intime.
- Încearcă să îți câștige încrederea repede, apoi îți cer bani, cadouri ori date bancare.
- Dacă nu trimiți bani de bună voie, vor recurge la șantaj. Cu cât trimiți mai mult, vor cere mai mult.

AI DEVENIT VICTIMĂ?

Nu te simți rănit/a!
Oprește imediat contactul cu autorul!
Dacă este posibil, salvează/păstrează conversațiile purtate.
Fă o plângere la poliție.
Raportează autorul la site-ul pe care te-a contactat inițial.
Dacă ai transmis detalii bancare, contactează imediat banca.

CE PUTEȚI FACE?

- Fiți foarte atenți cu datele personale pe care le postați pe rețele de socializare ori site-uri de întâlniri.
- Evaluati permanent riscurile. Escroci sunt prezenți pe cele mai populare site-uri.
- Nu vă grăbiți și întrebați.
- Verificați profilele și fotografiile persoanelor. Pot fi copiate și folosite nelegitim.
- Fiți atenți la greșelile gramaticale, neconcordanțele în informații și scuzele de tipul "camera mea foto nu funcționează".
- Nu transmiteți materiale compromițătoare, care ar putea fi folosite la șantaj.
- Dacă vreți să vă întâlniți personal, sunați familiei/prietenilor locul și perioada.
- Atenție la solicitările de bani! Nu trimiteți niciodată bani, datele card-ului ori alte detalii financiare sau copii ale actelor personale.
- Evitați plățile în avans.
- Nu intermediați transferuri de bani! Spălarea de bani este infracțiune.

EUROPOL EC3 | European Cybercrime Centre

POLIȚIA ROMÂNĂ

© CyberScam.ro



Frauda de tip loterie

- O înșelătorie la loterie poate fi un banner colorat pe un site web care spune că ești vizitatorul norocos care a câștigat o sumă de bani sau poate fi un e-mail care spune că ai câștigat la o tombolă. Indiferent de situație, **infractorul va cere informații personale și bancare pentru a trimite „câștigul”**. Odată furnizate aceste date, economiile tale pot fi cu ușurință furate.
- **Cum să eviți o înșelătorie la loterie:**
 - Amintește-ți că nu poți câștiga la o loterie la care nu ai participat niciodată
 - Reține că nimeni nu dă bani gratuit.
 - Nu oferi niciodată informațiile tale bancare unui necunoscut.

Frauda cu produse gratis, foarte ieftine sau contrafăcute

- Înșelătoria cu produse ar putea fi **un anunț** pentru produse ieftine sau chiar gratuite (plus taxe) de vânzare. După ce introduci **informațiile bancare** pentru a cumpăra sau a primi gratuit produsul, acești escroci îți vor lua banii.
- Într-o altă situație, poți întâlni un produs cosmetic fals care te scăpa de riduri. S-a constatat că aceste **produse contrafăcute** conțin ingrediente cancerigene, cum ar fi arsenic, beriliu sau cadmiu. Acești escroci îți iau banii și te lasă cu probleme de sănătate.



Cum să eviți o înșelătorie cu produse:

- **Ferește-te** de produsele cu „formule secrete” sau „ingrediente revoluționare”.
- **Nu da click** pe bannere cu oferte care par prea atractive pentru a fi adevărate.



Furtul de date personale (Personal data theft)

Autorii îți colectează nelegitim **datele personale de pe rețele de socializare**.
Datele tale pot fi **vândute** altor infractori sau folosite pentru a-ți accesa **conturile bancare, contracta împrumuturi ori derula afaceri ilegale în numele tau**.



Spoofing-ul numărului de telefon



ATENȚIE LA APELURILE FALSE!

Cum să nu cazi în capcana spoofing-ului



Ai grijă să nu devii victimă!

Infraactorii apelează potențiale victime și se prezintă drept angajați ai unor bănci din România ce îl anunță despre un credit făcut în numele lor.



Banca nu va apele niciodată utilizatorii pentru a le promite oportunitatea de recuperare a sumelor pierdute.



Banca nu va cere niciodată utilizatorilor să furnizeze telefonic date cu caracter sensibil (date personale, de autentificare, sau de carduri bancare), în urma unor apeluri efectuate de companie. Evitați furnizarea de date la telefon!



Verificați întotdeauna autenticitatea apelurilor de la o autoritate sau companie, printr-un canal de comunicare separat, în special dacă vi se solicită date cu caracter sensibil.



Raportați astfel de apeluri către organizația în numele căreia s-a efectuat apelul, pentru a atrage atenția cât mai rapid asupra noilor scenarii folosite de atacatori.



În cazul în care ați furnizat date de card, sesizați imediat banca, iar dacă ați fost păgubit, depuneți o plângere la Poliție și notificați DNSC (telefon 1911 sau alerts@dnsc.ro).



Nu în ultimul rând, contribuiți la răspândirea acestor avertizări și către alți utilizatori, pentru a reduce șansele ca astfel de tentative de fraudă să aibă succes!

O inițiativă



Este o tehnică de înșelăciune prin care **un atacator își modifică numărul de telefon**, astfel încât să apară pe ecranul persoanei apelate un alt număr decât cel real.

Această metodă este utilizată pentru a induce în eroare victima și a obține informații personale sau bancare sensibile.

Fraude în domeniul cumpărăturilor online (Online shopping scams)

Autorii îți oferă oportunitați „speciale” de investiții cu profituri rapide... sau îți prezintă „oferte-bombă” de „chilipiruri” în mediul online.



FRAUDE LA CUMPĂRĂTURI ONLINE

Cumpărăturile online pot fi benefice, dar atenție la fraude.

CE POTI FACE?

- > Folosește site-uri românești, pe cât posibil - pot fi mai ușor de detectat eventuale probleme.
- > Verifică înainte să cumperi - recenziile site-ului/produsului.
- > Folosește cardul de credit - ai mai multe șanse de a-ți recupera banii.
- > Plătește folosind servicii de plăți sigure - ți se solicită plata prin transfer bancar? Mai gândește-te!
- > Plătește doar când ai o conexiune sigură la internet - evită folosirea hot-spot-urilor publice de wi-fi.
- > Folosește un dispozitiv sigur când plătești - fă-ți la timp actualizările de sistem și securitate.
- > Atenție la reclame, „oferte miraculoase”, „afaceri-bombă” - dacă e prea frumos ca să fie adevărat, probabil nu e!
- > O fereastră pop-up îți spune că ai câștigat un premiu fabulos? Mai gândește-te!
- > Dacă produsul comandat nu sosește la timp, contactează imediat vânzătorul. Dacă nu răspunde, **contactează banca.**

 Sesizați poliția la orice încercare de fraudă, chiar dacă nu ați devenit victima acesteia.

 #CyberScams

Fraudele care au ca mod de operare investițiile online



- Prin acest tip de fraudă sunt solicitate datele bancare cu **promisiunea falsă de obținere de câștiguri** din investiții financiare în: **criptomonede, petrol, aur, etc.**
- Potențialele victime sunt contactate prin **diverse canale de comunicare** de către persoane care pretind că sunt reprezentanți ai unor companii sau platforme de investiții.
- În schimbul promisiunilor false de câștiguri mari, fraudatorii conving persoanele vizate să furnizeze **datele de acces la serviciile bancare online** (Internet/ Mobile Banking), **datele cardului bancar** (număr card, codul de securitate de pe spatele cardului) și **coduri SMS** sau se solicită o sumă inițială de aproximativ 1200/ 1250 RON, urmând să fie cerute ulterior și alte sume de bani sub pretextul că profitul va fi din ce în ce mai mare.
- De asemenea, persoanele sunt determinate să-și instaleze **aplicații prin care se permite accesul persoanelor neautorizate la telefon de la distanță**. Astfel, atacatorii ajung să aibă acces la conturile bancare, fapt ce determină posibilitatea efectuării de operațiuni.
- În unele cazuri, pentru a crea **o aparență de credibilitate**, demersurile sunt prezentate ca fiind promovate de **o personalitate publică** sau cu experiență în domeniul financiar.
- **Persoanele dornice de câștiguri substanțiale, ușoare și rapide** riscă să nu poată retrage sumele investite dacă fac vreun transfer de bani sau să fie victime ale fraudelor prin divulgarea datelor contului sau cardului bancar.
- După ce au pierdut diferite sume de bani, **victimele pot fi resunate** de către infractori sub pretextul că sunt polițiști sau reprezentanți ai băncii și li se pretind accesul la cont sau anumite comisioane „pentru a li se returna sumele pierdute inițial”.

Metode de a te proteja de fraudele legate de investiții

- Verifică din mai multe surse orice **propunere de investiție** cu un câștig mare de la persoane necunoscute.
- Ai grijă la mesajele prin care **ți se oferă câștiguri ușoare, rapide sau mari**. Nu accesa link-urile de pe platformele de socializare care promit câștiguri mari de bani într-un termen scurt de timp;
- Nu instala **aplicații pe telefon/calculator** decât din surse oficiale;



- Asigură-te că ești singura persoană care are acces la **aplicațiile/site-urile de investiții**, nu și persoana care ți-a vorbit de investiții;
- Nu furniza niciodată altor persoane **datele personale sau bancare** (cont, user, parola Mobile/Internet banking, numărul cardului, codul de securitate de pe spatele cardului etc.);
- Dacă crezi că ai fost înșelat sau ai furnizat datele bancare altor persoane, **anunță imediat banca la care ai conturile și poliția**.

FRAUDE CU INVESTIȚII

Fraudele obișnuite cu investiții pot include "oportunități" de investiții în acțiuni, obligațiuni, criptomonedă, metale prețioase, imobiliare în străinătate sau energii alternative.

CARE SUNT SEMNELE?



> Ești sigurat că afacerea e sigură și îți recuperezi foarte repede investiția.

> Oferta este limitată în timp.

> Primești un apel nesolicitat, în mod repetat.

> Oferta este doar pentru tine și nu trebuie să o divulgi altcuiva.

CE POȚI FACE?

- > **Întotdeauna cere sfaturi financiare de la o persoană imparțială**, înainte de orice investiție ori plată.
- > **Refuză orice apel necunoscut** legat de așa zise oportunități de investiții.
- > **Fii precaut** la ofertele care promit investiții "sigure", recuperare garantată ori câștiguri mari.
- > **Atenție la tentativele viitoare.** Dacă ai fost victima unei fraude, foarte probabil autorii te vor ținti din nou sau îți vor vinde datele altor infractori.
- > **Contactează poliția** dacă ai suspiciuni.



Cum să te protejezi de fraudele din mediul online

- **Evită să accesezi** link-uri, primite din surse necunoscute pe mail sau prin SMS, prin intermediul comunicărilor de pe social media, ori prin intermediul platformelor de tip chat (WhatsApp, Signal, Telegram, etc.) și **nu completa datele tale personale sau bancare** pe acestea.
- **Nu da click** atunci când ai fost etichetat într-o postare din social media care îți promite câștiguri mari, cu siguranță este vorba despre o înșelătorie.
- **Fii atent** la mesajele care par să vină din partea băncilor! Băncile nu solicită niciodată date confidențiale cum ar fi datele cardurilor, parole de acces, coduri PIN, nici telefonic, nici prin SMS, nici prin e-mail și nici prin completarea acestora pe website.
- **Citește cu atenție**, înainte de a deschide orice mesaj sau un fișier care pare a fi transmis de la banca ta sau de alte persoane/instituții. Mesajele false conțin, de multe ori, formule de adresare impersonale, greșeli gramaticale sau de exprimare.
- **Ca regulă**, nu efectua transferuri și nu procesa operațiuni doar în baza unui e-mail sau a unei solicitări telefonice urgente, fără a face o verificare a autenticității mesajului.



Cum să te protejezi de fraudele din mediul online



- **Nu furniza niciodată** altor persoane datele de autentificare la conturi (username, parola, cod suplimentar de autentificare sau cod de back-up);
- **Nu dezvălui** datele de pe cardul personal: nume, număr, data de expirare, CVV2/CVC (numărul de trei cifre de pe spatele cardului) și nici PIN-ul. Nu introduce codul PIN pe site-uri de internet și nu-l divulga telefonic!
- **Dacă trebuie să primești bani**, dă IBAN-ul tău (numărul de cont, format din 24 de caractere, litere și cifre), nu datele de pe card! Solicitarea datelor cardului de către alte persoane este o capcană.
 - Folosește mereu **parole** cu un nivel de complexitate ridicat. Evită folosirea termenilor uzuali și schimbă periodic parolele.
 - Instalează cele mai recente **actualizări** ale sistemului de operare și antivirus.
 - **Asigură-te** că ai mereu copii de rezervă ale datelor tale pentru a-ți proteja datele împotriva atacatorilor.
 - **Sfătuieste-te** cu familia și cu alți cunoscuți înainte de a lua o decizie cu privire la orice ofertă primită în mediul online.





În cazul în care ați introdus date financiare **sesizați imediat banca**, iar dacă ați fost păgubit, **depuneți o plângere la Poliția Română și notificați Directoratul Național de Securitate Cibernetică** (telefon 1911 sau alerts@dnsc.ro)

Nu în ultimul rând, **contribuiți la răspândirea acestor avertizări și către alți utilizatori**, pentru a reduce șansele ca astfel de tentative de fraudă să aibă o rată de succes mulțumitoare pentru infractori.