MINISTERUL AFACERILOR INTERNE

INSPECTORATUL GENERAL AL POLIŢIEI ROMÂNE

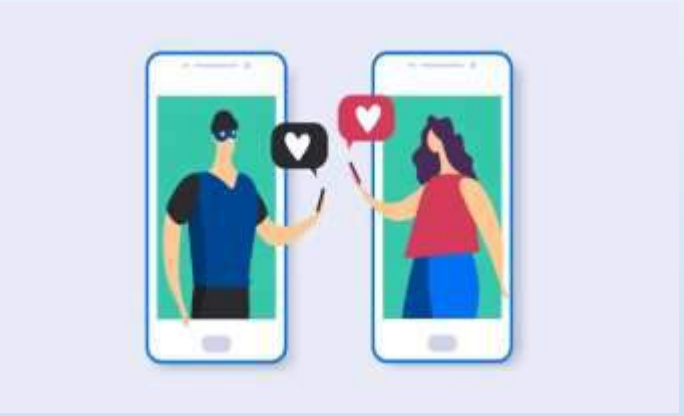
INSPECTORATUL DE POLIŢIE AL JUDEŢULUI SATU MARE

Compartimentul Analiza și Prevenirea Criminalității

CAMPANIE DE PREVENIRE A FRAUDELOR INFORMATICE

Cele mai întâlnite tipuri de fraude în mediul online

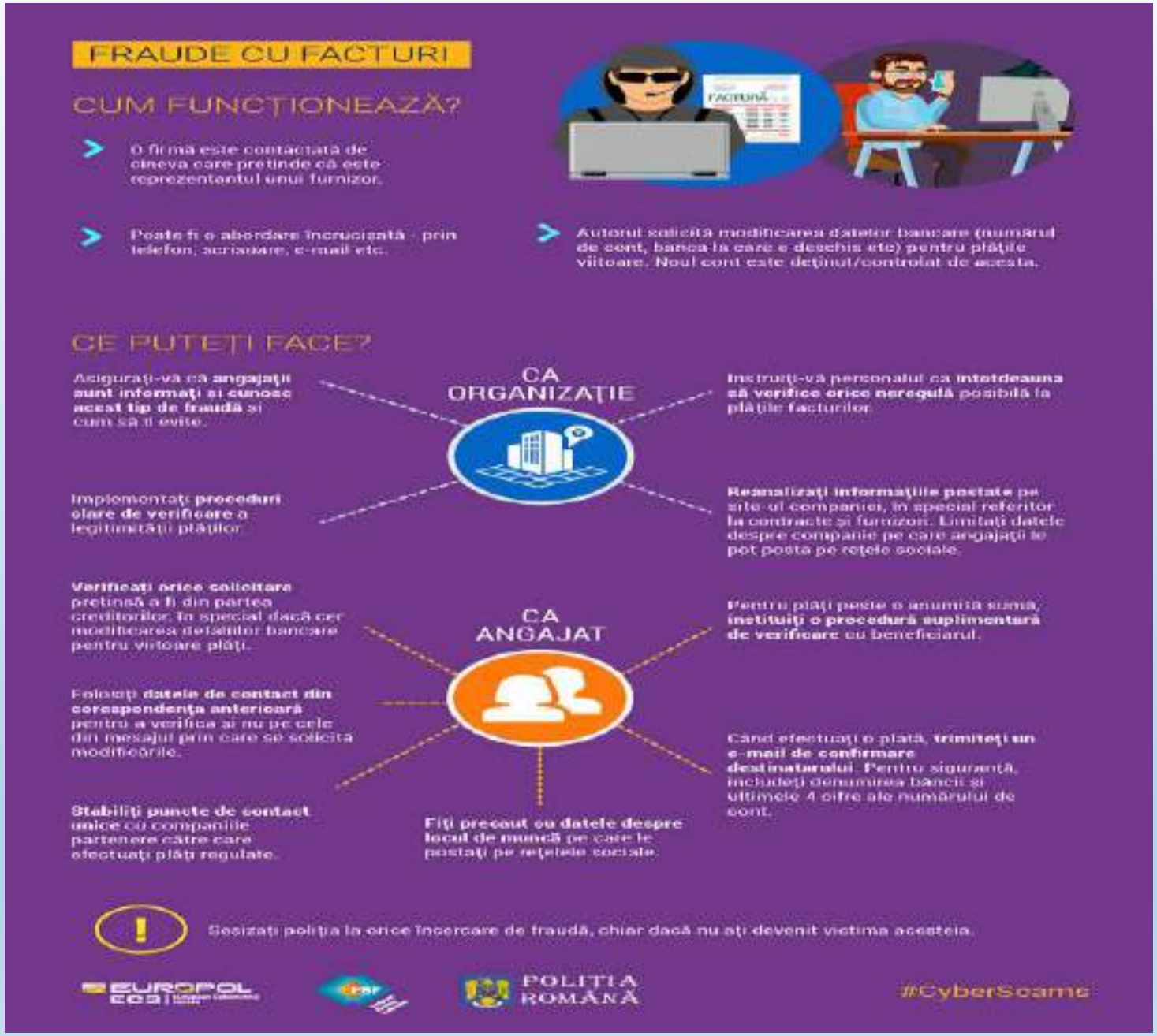
- **Frauda ”Mesaj de la șef”**
- **Fraude cu facturi**
- **Frauda care se ascunde în spatele unei probleme tehnice**
- **Phishing/Smishing/Vishing**: autorii te apelează telefonic, îți trimit un mesaj text (SMS) ori un e-mail
- **Website-uri bancare contrafăcute**



- **Iubire prefacută**
- **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.



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 sa 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.

Avertisment

G **Google Assistance <GoogleAssistance@gmail.com>** Oct 11, 2021, 4:03 AM (5 hours ago)
to me

Avertisment

Sistemele noastre au detectat funcționarea incorectă a contului tău de e-mail. Este posibil să fi fost victima unei tentative de hacking. Sună gratuit la 07558256632 și un consultant te va îndruma pentru a-ți rezolva problema sau intră pe AsistentaGmail și urmează pașii pentru rezolvare.

Echipa Google

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.

E-MAIL-URI TIP PHISHING

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

CUM FUNCȚIONEAZĂ?

Aceste e-mail-uri:

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

imită logo-ul și designul mesajelor reale.

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

utilizează un limbaj care sugerează urgența.

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?

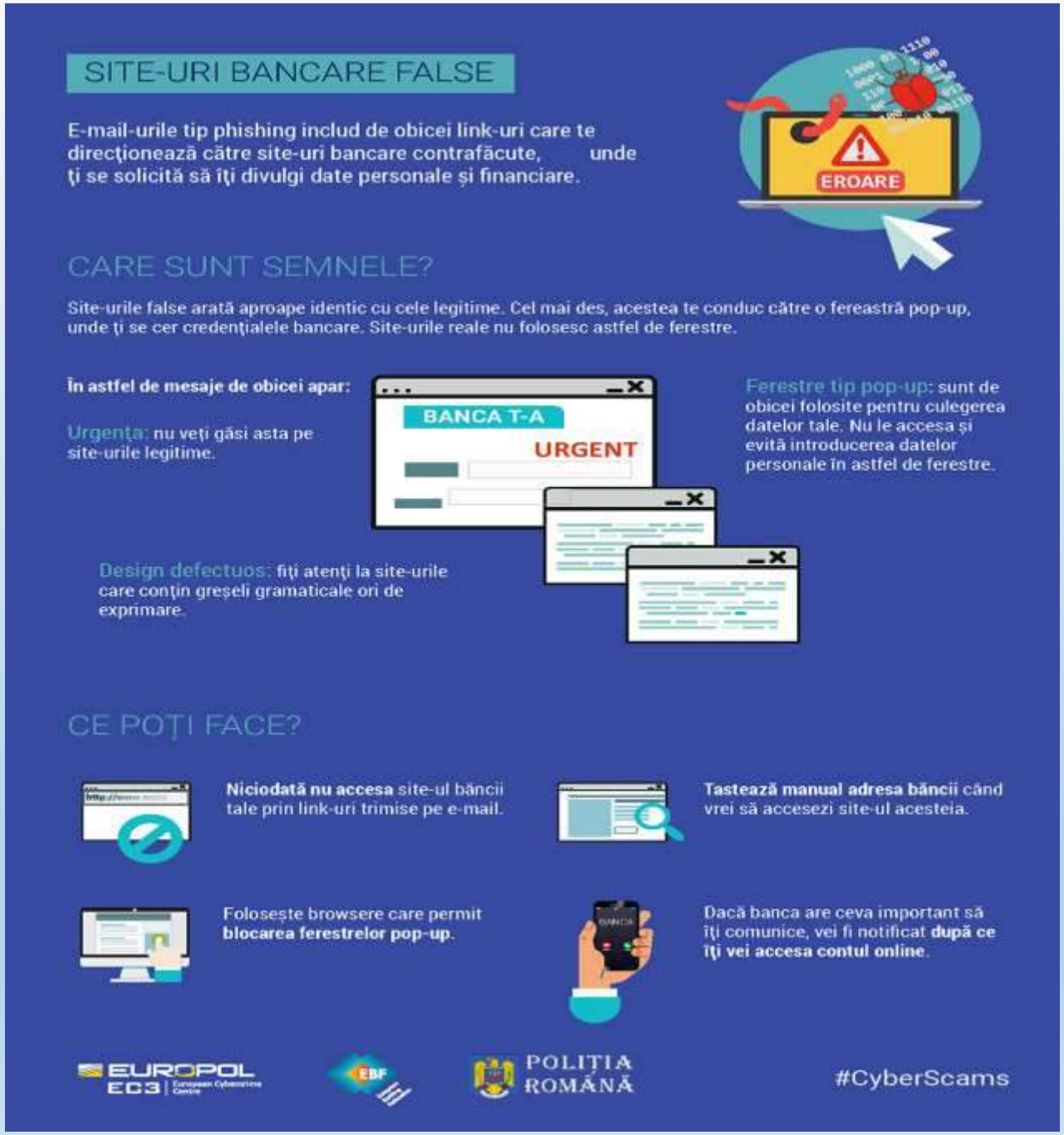
- **Actualizează permanent programele** calculatorului, inclusiv sistemul de operare.
- Fii **extrem de atent** dacă primești mesaje "din partea băncii" prin care ți se solicită date sensibile (date despre cont, parole etc.).
- **Citește cu atenție mesajele** - compară adresa expeditorului cu cea din 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

EUROPOL EC3 | European Cybercrime Centre

EBF

POLIȚIA ROMÂNĂ

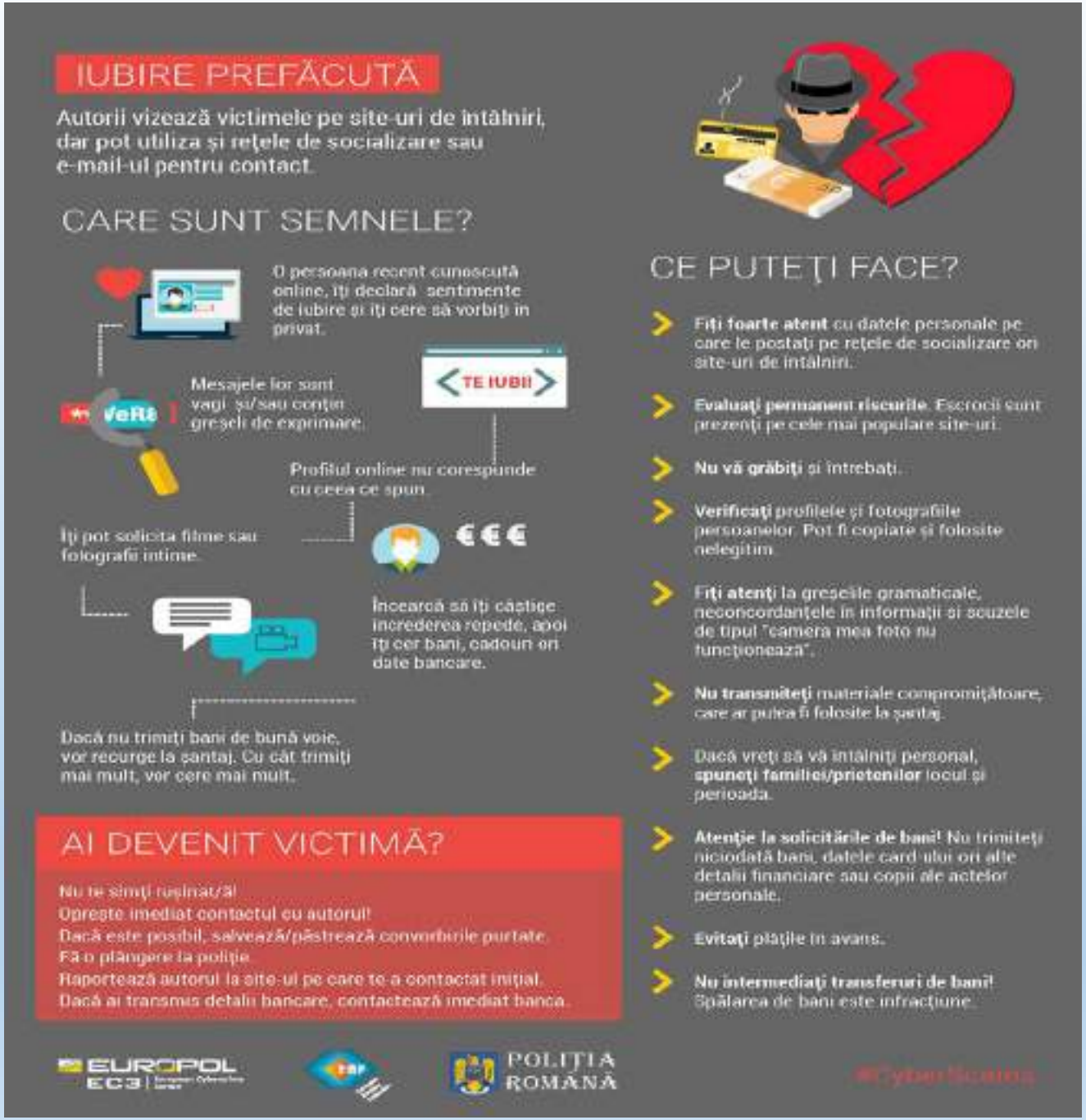


Website-uri bancare contrafăcute (Spoofed bank website fraud)

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 prefacută (Romance scam)

Autorii pretind că sunt îndragostiți 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.



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**.

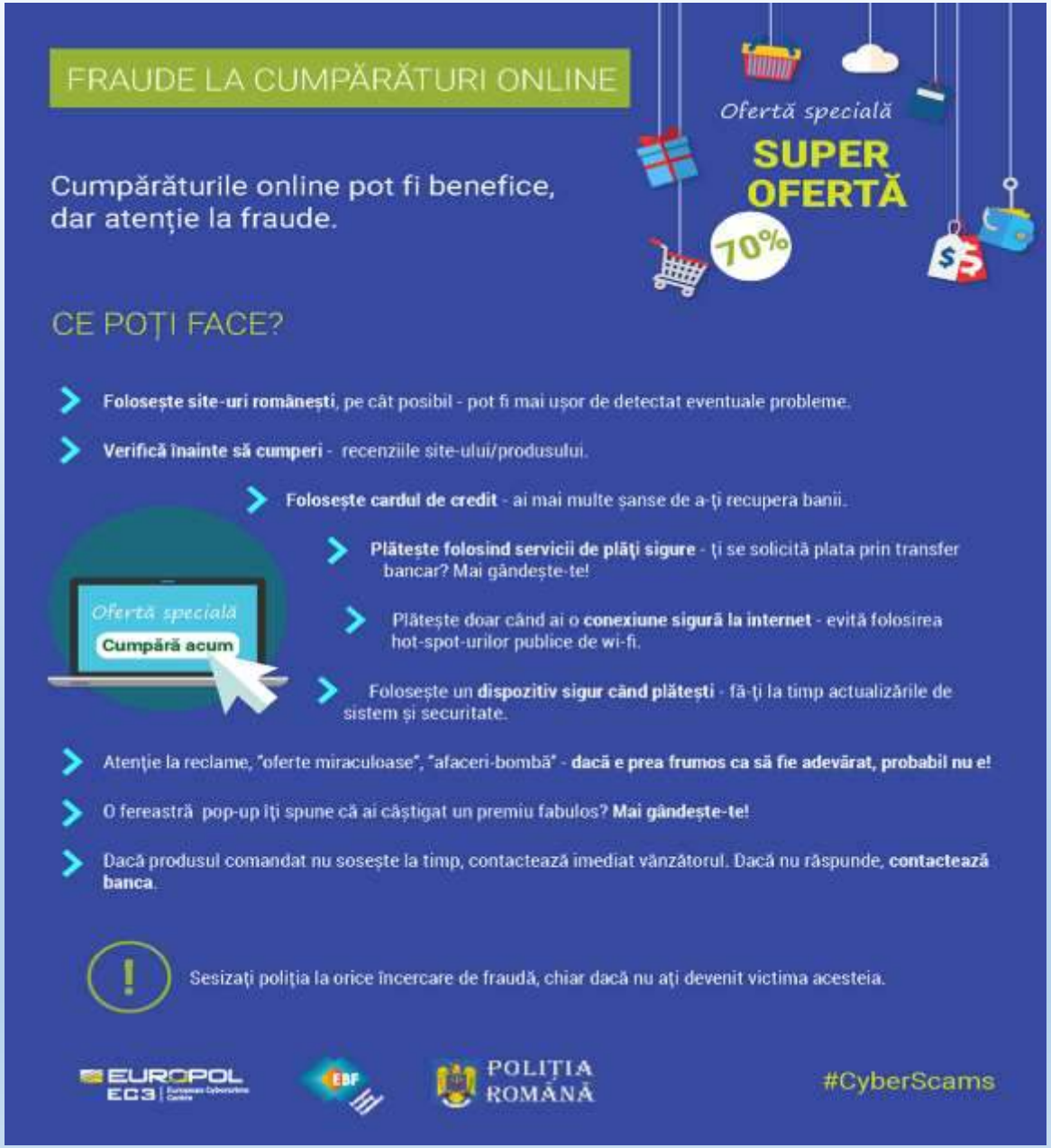
Spoofing-ul numărului de telefon

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.



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 investiţie** cu un câștig mare de la persoane necunoscute.
- Ai grijă la mesajele prin care **ţi se oferă câştiguri uşoare, 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, **anunţă imediat banca la care ai conturile şi 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 asigurat 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 peroană 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.

EUROPOL EC3 | European Cybercrime Centre

EBF

POLIȚIA ROMÂNĂ

#CyberScams

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.

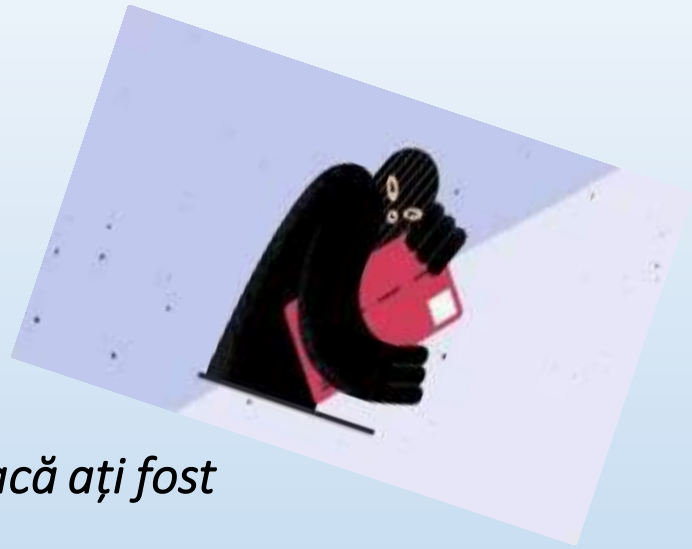
- **Citește cu atenție**, înainte de a deschide orice mesaj sau un fișier care pare a fi transmis de la banca ta sau de alte persoane/instituții. Mesajele false conțin, de multe ori, formule de adresare impersonale, greșeli gramaticale sau de exprimare.

- **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.
- **Sfătuiește-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.