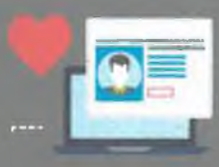
IUBIRE PREFĂCUTĂ

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 persoana recent cunoscută online, îți declară sentimente de iubire și îți cere să vorbiți 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 rușinat/ă!
Oprește imediat contactul cu autorul!
Dacă este posibil, salvează/păstrează convorbirile 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 atent** cu datele personale pe care le postați pe rețele de socializare ori site-uri de întâlniri.
- **Evaluați permanent riscurile.** Escrocii 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, **spuneți 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

EBF

POLIȚIA ROMÂNĂ

#CyberScams

FRAUDE LA CUMPĂRĂTURI ONLINE

Cumpărăturile online pot fi benefice, dar atenție la fraude.

CE POȚI 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-ţi recupera banii.
- **Plătește folosind servicii de plăţi sigure** - ţi 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-ţi la timp actualizările de sistem și securitate.

- Atenţie la reclame, "oferte miraculoase", "afaceri-bombă" - **dacă e prea frumos ca să fie adevărat, probabil nu e!**
- O fereastră pop-up îţi 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**.

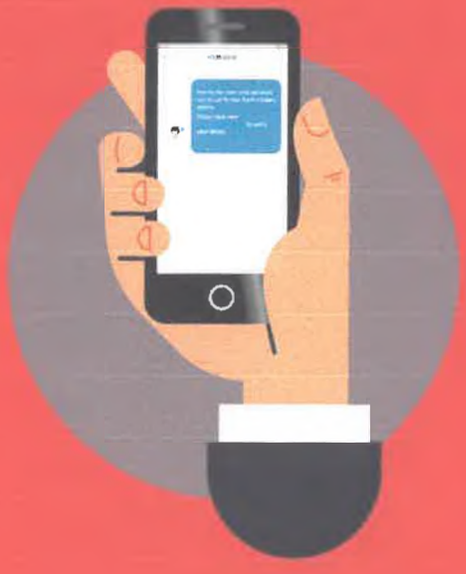
Sesizaţi poliţia la orice încercare de fraudă, chiar dacă nu aţi devenit victima acesteia.

EUROPOL EC3 | EBF | POLIȚIA ROMÂNĂ

#CyberScams

PHISHING PRIN SMS

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



CUM FUNCȚIONEAZĂ?

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

CE POȚI FACE?

- **Nu accesa link-uri, atașamente sau imagini nesolicitate**, primite prin SMS de la persoane necunoscute.
- **Nu acţiona în grabă**. Ia-ţi timp și verifică informaţiile înainte de a trimite un eventual răspuns.
- **Niciodată nu răspunde unui SMS** prin care ţi se solicită codul PIN, parole de acces la contul de online banking ori alte credenţiale de siguranţă.
- **Contactează imediat banca**, dacă stii că ai răspuns unui astfel de mesaj și ai furnizat detalii bancare în aceste condiţii.

EUROPOL EC3 | EBF | POLIȚIA ROMÂNĂ

#CyberScams

APELURI TELEFONICE TIP PHISHING

Vishing (combinaţie de cuvinte între "Phishing" și "voce") este o fraudă în care autorii, apelând telefonic victima și folosind diverse pretexte, o conving să divulge date personale și/sau financiare ori să le transfere bani.

CE POȚI FACE?

- **Fii prudent** cu privire la apelurile telefonice primite de la necunoscuți.
- **Cere numărul apelantului** și spune-i că revii tu cu un apel.
- Pentru verificarea identității acestuia, **apelează organizația în numele căreia pretind că sună**.
- **Chiar dacă îți transmit un număr la care îi poți contacta,** nu considera asta ca formă de verificare a realității expuse.
- Autorii pot găsi informații despre tine în mediul online, în special pe rețele sociale. **Nu lua de bun orice telefon,** doar pentru că apelantul știe câte ceva despre tine.
- **Nu transmite prin telefon codul PIN ori parola** de la contul de Internet Banking. Niciodată banca nu ți le va solicita în acest mod.
- **Nu transfera bani** către necunoscuți care îți solicită asta.
- Dacă ai bănuieli, **contactează banca**.

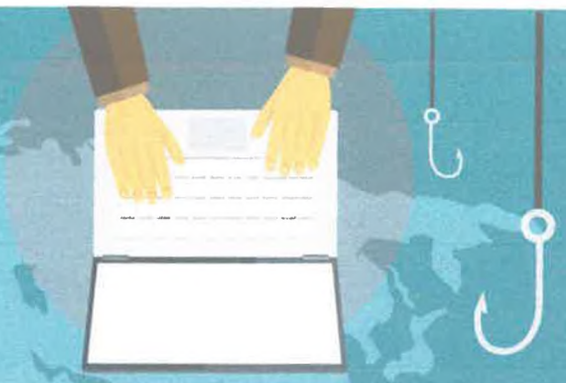
EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLIȚIA ROMÂNĂ

#CyberScams

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.

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**.

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

#CyberScams

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

EUROPOL EC3 European Cybercrime Centre

EBF

POLIȚIA ROMÂNĂ