FRAUDA ”MESAJ DE LA ȘEF”

Frauda ”Mesaj de la șef” vizează angajaţii autorizaţi să efectueze plăţi, care, prin inducere în eroare, sunt determinaţi să plătească o factură falsă ori să efectueze un transfer.

CUM FUNCȚIONEAZĂ?

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

De obicei este bine informat cu privire la organizaţie.

Solicită efectuarea urgentă a unei plăţi.

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

Se referă la o situaţie sensibilă (ex. control autorităţi, achiziţii etc.).

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

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

Angajatul transferă banii într-un cont al autorului.

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

CARE SUNT SEMNELE?

- E-mail sau apel telefonic nesolicitat.
- Contact cu un oficial cu care nu ești în legătură directă, în mod normal.
- Solicitare de confidenţialitate.
- Presiune sub semnul presupusei urgenţe.
- Solicitare neobișnuită, ieșită din tiparele procedurilor interne.
- Ameninţări sau promisiuni neobișnuite, flatare.

CE POȚI FACE?

CA ORGANIZAŢIE

Conștientizaţi riscul și asiguraţi-vă că **angajaţii sunt informaţi permanent**.

Instruiţi-vă staff-ul să manifeste **atenţie maximă la efectuarea plăţilor**.

Implementaţi proceduri interne stricte referitoare la plăţi.

Implementaţi proceduri de verificare a legitimităţii plăţilor solicitate prin e-mail.

Stabiliţi reguli de raportare a tentativelor de fraudă.

Verificaţi datele publicate pe site-ul companiei, **restricţionaţi accesul la datele importante** și fiţi atenţi la reţelele sociale.

Actualizaţi soluţiile tehnice de securitate.

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

CA ANGAJAT

Respectaţi cu strictețe procedurile de securitate în cazul plăţilor și achiziţiilor. **Nu săriţi nici un pas procedural și rezistaţi presiunilor.**

Verificaţi cu atenţie adresele de e-mail când primiţi solicitări de informaţii sensibile/transferuri de bani.

Dacă aveţi dubii în cazul unui transfer de bani, **consultaţi un coleg.**

Niciodată nu deschideţi link-uri sau atașamente dubioase primite prin e-mail. Fiţi foarte atenţi când verificaţi mail-ul personal pe calculatorul de serviciu.

Manifestaţi precauţie și restricţionaţi informaţiile de pe reţelele sociale.

Evitaţi publicarea de date despre conducerea, securitatea sau procedurile firmei.

Dacă primiţi un e-mail suspect, informaţi imediat departamentul IT.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLIȚIA ROMÂNĂ

#CyberScams

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

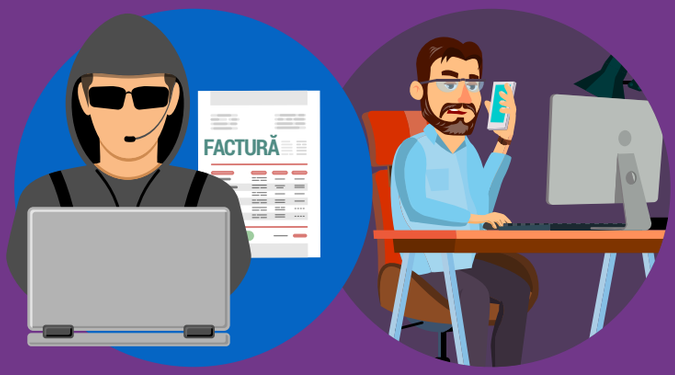
EBF European Banking Federation

POLIȚIA ROMÂNĂ

#CyberScams

FRAUDE CU FACTURI

CUM FUNCȚIONEAZĂ?



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

CE PUTEȚI FACE?

CA ORGANIZAŢIE

Asiguraţi-vă că **angajaţii sunt informaţi și cunosc acest tip de fraudă** și cum să îl evite.

Instruiţi-vă personalul ca **întotdeauna să verifice orice neregulă** posibilă la plăţile facturilor.

Implementaţi **proceduri clare de verificare** a legitimităţii plăţilor.

Reanalizaţi informaţiile postate pe site-ul companiei, în special referitor la contracte și furnizori. Limitaţi datele despre companie pe care angajaţii le pot posta pe reţele sociale.

CA ANGAJAT

Verificaţi orice solicitare pretinsă a fi din partea creditorilor, în special dacă cer modificarea detaliilor bancare pentru viitoare plăţi.

Pentru plăţi peste o anumită sumă, **instituiţi o procedură suplimentară de verificare** cu beneficiarul.

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

Când efectuaţi o plată, **trimiteţi un e-mail de confirmare destinatarului**. Pentru siguranţă, includeţi denumirea băncii și ultimele 4 cifre ale numărului de cont.

Stabiliţi puncte de contact unice cu companiile partenere către care efectuaţi plăţi regulate.

Fiţi precaut cu datele despre locul de muncă pe care le postaţi pe reţelele sociale.

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

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | 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 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 primiţi de la bancă.

imită logo-ul și designul mesajelor reale.

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

utilizează un limbaj care sugerează urgenţa.

CE POȚI FACE?

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

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

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

#CyberScams

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLIȚIA ROMÂNĂ

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.

TE IUBI!

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.

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.

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.

EUROPOL EC3 European Cybercrime Centre

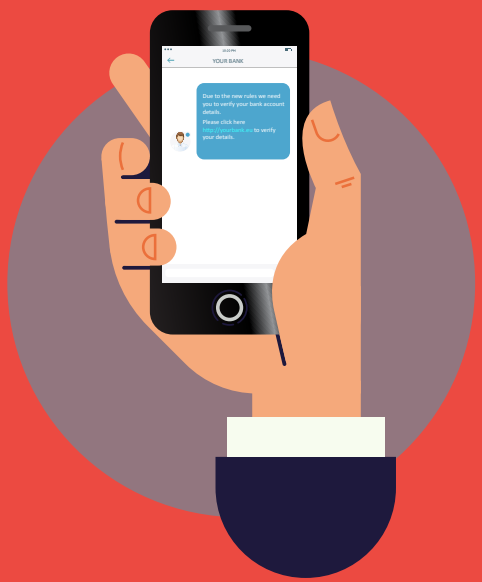
EBF European Banking Federation

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 știi că ai răspuns unui astfel de mesaj și ai furnizat detalii bancare în aceste condiţii.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLIȚIA ROMÂNĂ

#CyberScams

SITE-URI BANCARE FALSE

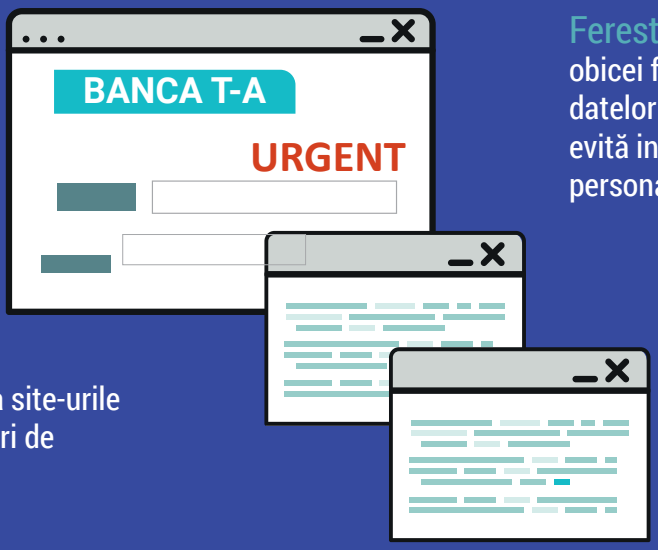
E-mail-urile tip phishing includd de obicei link-uri care te direcţionează către site-uri bancare contrafăcute, unde ţi se solicită să îţi divulgi date personale și financiare.

CARE SUNT SEMNELE?

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

În astfel de mesaje de obicei apar:

Urgenţa: 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: fiţi atenţi la site-urile care conţin 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 îţi comunice, vei fi notificat **după ce îţi vei accesa contul online**.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

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 necunoscuţi.
- **Cere numărul apelantului** și spune-i că revii tu cu un apel.
- Pentru verificarea identităţii acestuia, **apelează organizaţia în numele căreia pretind că sună**.
- **Chiar dacă îţi transmit un număr la care îi poţi contacta**, nu considera asta ca formă de verificare a realităţii expuse.
- Autorii pot găsi informaţii despre tine în mediul online, în special pe reţele 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 ţi le va solicita în acest mod.
- **Nu transfera bani** către necunoscuţi care îţi solicită asta.
- Dacă ai bănuieli, **contactează banca**.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLIȚIA ROMÂNĂ

#CyberScams