

FRAUDA "MESAJ DE LA ȘEF"

Frauda "Mesaj de la șef" vizează angajații autorizați să 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 că 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".



Deseori, 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.

Se referă la o situație sensibilă (ex. control autorități, achiziții etc.).

CARE SUNT SEMNELE?

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

CE POȚI FACE?

CA ORGANIZAȚIE

Conștientizați riscul și asigurați-vă că **angajații sunt informați permanent**.

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.



Sesizați 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 nici un pas procedural și rezistați presiunilor.**

Verificați cu atenție adresele de e-mail când primiți solicitări de informații sensibile/transferuri de bani.

Dacă aveți dubii în cazul unui transfer de bani, **consultați un coleg.**

Niciodată nu deschideți link-uri sau atașamente dubioase 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.

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 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.



SERVICIUL
TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ

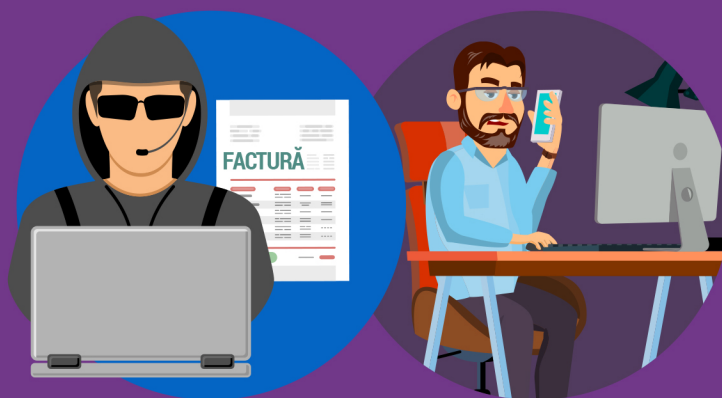


EUROPOL
EC3 | European Cybercrime
Centre

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 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 pretinsă a fi din partea creditorilor, în special dacă cer modificarea detaliilor 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.

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

CA ANGAJAT



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

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

Fiți precaut cu datele despre locul de muncă pe care le postați pe rețelele sociale.



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

FRAUDE LA CUMPĂRĂTURI ONLINE

Cumpărăturile online pot fi benefice, dar atenție la fraude.

Ofertă specială

**SUPER
OFERTĂ**

70%

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-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.**



SERVICIUL
TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ



EUROPOL
EC3 | European Cybercrime
Centre

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 primești de la bancă.

imită logo-ul și designul mesajelor reale.

EROARE

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.



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



SERVICIUL
TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ



EUROPOL
EC3 | European Cybercrime
Centre



#CyberScams

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?



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.



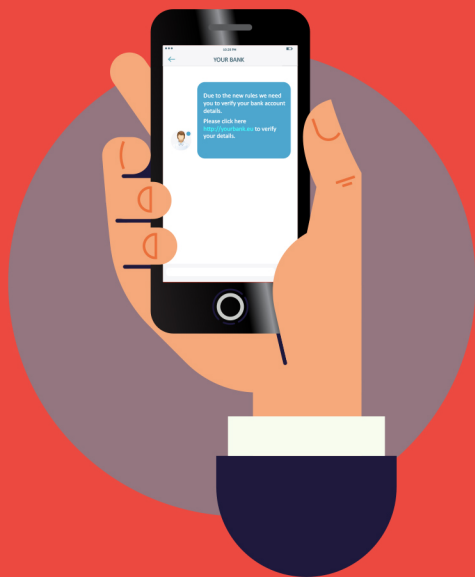
SERVICIUL
TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ



EUROPOL
EC3 | European Cybercrime
Centre

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 "îți verifici, actualizezi, reactivezi" contul. Dar...în realitate ești direcționat 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 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.



SERVICIUL
TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ



EUROPOL
EC3 | European Cybercrime
Centre

SITE-URI BANCARE FALSE

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

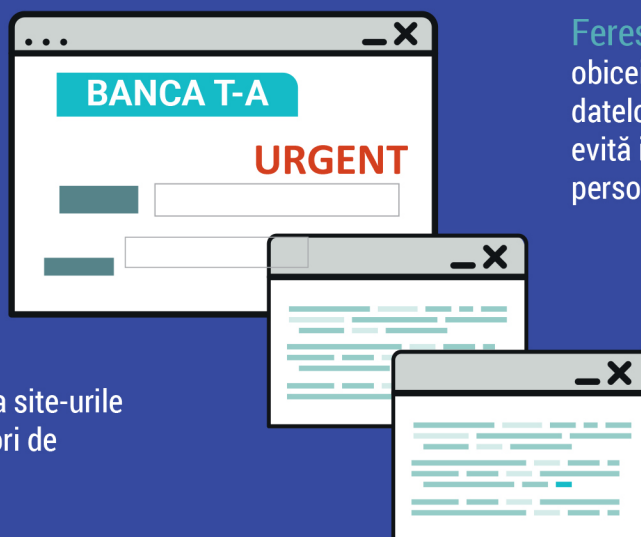


CARE SUNT SEMNELE?

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

În astfel de mesaje de obicei apar:

Urgența: nu vei 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.



SERVICIUL
TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ



EUROPOL
EC3 | European Cybercrime
Centre

APELURI TELEFONICE TIP PHISHING

Vishing (combinație 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.

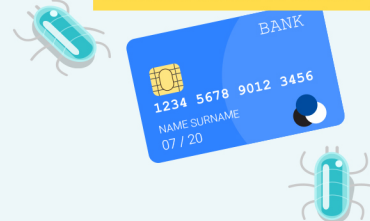


CE POȚI FACE?

- **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.**



BANK ACCOUNT HACKING



SERVICIUL
TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ



EUROPOL
EC3 | European Cybercrime
Centre