E-MAIL-URI TIP PHISHING

Phishing-ul 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.

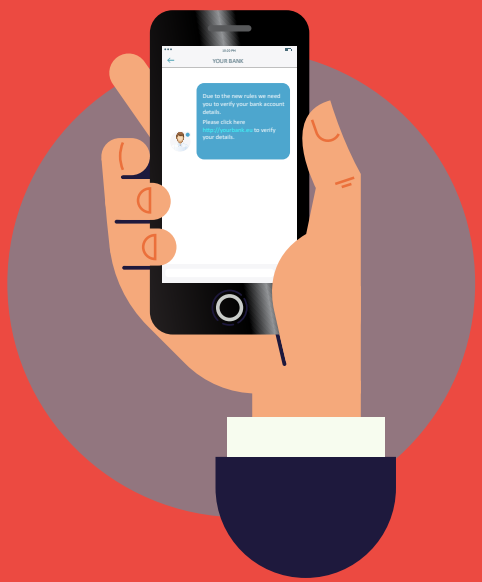
#CyberScams

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 European Banking Federation | GUVERNUL ROMÂNIEI | DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

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.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

GUVERNUL ROMÂNIEI

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

#CyberScams

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**.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | GUVERNUL ROMÂNIEI | DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

#CyberScams