

FII ÎN SIGURANȚĂ ONLINE!

*Cum ne protejăm de
escrocheriile digitale
cu impact financiar?*

CE SUNT ESCROCHERIILE PRIN TEHNOLOGIILE INFORMAȚIONALE?

Escrocheriile online sunt tentative de înșelăciune realizate prin mijloace electronice – cum ar fi e-mailul, telefonul mobil, rețelele sociale sau site-urile web – prin care infractorii cibernetici încearcă să obțină **date personale sau financiare**, ori să te determine să faci **plăți nejustificate**.



TIPURI FRECVENTE DE ESCROCHERII DIGITALE

PHISHING



Escrocherii prin e-mail sau mesaje instant care imită companii de încredere (bănci, instituții publice, platforme de servicii), cu scopul de a te face să dezvălui:

- date de acces la conturi bancare,
- parole,
- informații personale.

Exemplu: Un e-mail care pare a fi de la banca ta, îți cere urgent să-ți „reactualizezi” datele accesând un link – dar linkul duce la un site fals.

SMISHING (SMS + PHISHING)



Escrocherie prin mesaje text SMS, care:

- pretind livrări eșuate,
- notificări bancare false,
- sau premii câștigate.

Pericolul: Linkuri incluse în SMS-uri care duc la site-uri frauduloase unde îți se cer date personale.

VISHING (VOCE + PHISHING)



Infractorii te sună și:

- se prezintă ca angajați bancari sau oficiali,
- îți cer coduri PIN, numărul cardului, CVC2, coduri de securitate,
- te sperie cu tranzacții suspecte sau actualizări urgente de date.

Regulă de aur: Băncile **nu cer niciodată date sensibile prin telefon!**



ALTE FORME DE ÎNȘELĂCIUNE ONLINE

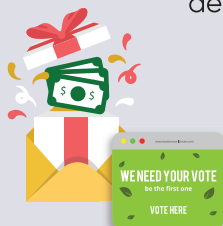


Anunțuri false: Produse fictive
vândute online, cerere de plată în avans.

„Romance scam”: Înșelăciune
emoțională prin site-uri de dating, urmată
de cereri de bani.



Rețele sociale: Conturi false,
concursuri fictive, mesaje de ajutor
suspecte.



Ransomware: Fișiere blocate de un
virus și deblocare doar contra
răscumpărării.



SEMNE CĂ E O ESCROCHERIE:

Mesaje sau
apeluri
neasteptate
cu cereri
urgente

Solicitări de date
sensibile pe
canale neoficiale



Linkuri sau
adrese de
e-mail
suspecte

Premii mari
sau moșteniri
dubioase



Greșeli
gramaticale
în comunicare



CUM TE PROTEJEZI?



Verifică sursa înainte de a accesa linkuri sau de a da curs solicitărilor



Nu furniza date personale prin telefon, e-mail sau SMS



Activează autentificarea cu doi factori (2FA)



Actualizează softul și folosește antivirus



Folosește parole complexe și diferite pentru fiecare cont



Evită rețelele Wi-Fi publice pentru tranzacții financiare



CE FACI DACĂ AI FOST VICTIMA UNEI ESCROCHERII?



1 Deconectează-te de la internet și schimbă parolele

2 Informează banca sau instituția implicată



3 Raportează la poliție



4 Cere ajutor de la specialiști în securitate cibernetică



Această publicație a fost realizată cu sprijin financiar din partea Norvegiei. Conținutul acestei publicații este responsabilitatea exclusivă a Asociației Presei Independente (API) și nu poate fi în niciun caz considerat că reflectă punctele de vedere ale Guvernului Norvegiei.