

ATENȚIE LA APELURILE FALSE!

Spoofing – înșelăciunea prin mascarea identității reale a numărului de telefon

Spoofingul este o metodă prin care **infractorii sună de pe un număr fals**, care pare să fie de **încredere**, cum ar fi cel al unei instituții cunoscute (Poliție, bancă, DNSC etc.). Scopul lor este să vă păcălească pentru a obține **informații personale sau date bancare**.

Aceștia folosesc o **tehnologie** numită VoIP (apel prin internet) care le permite să afișeze pe **telefonul dumneavoastră un alt număr** decât cel real. De exemplu, puteți primi un apel care pare să vină de la Poliție, dar în realitate vine de la un escroc.

Q Cum funcționează această înșelăciune:

- Persoana care vă sună **nu folosește un telefon obișnuit**, ci un program care face apeluri prin internet.
- Acest program poate **schimba numărul care apare pe ecranul dumneavoastră**.
- Astfel, **pare că sunteți sunat de o instituție cunoscută**, deși este un număr fals.
- Infractorii vă pot cere:
 - **date bancare**
 - **coduri PIN sau parole**
 - **să faceți o plată urgentă** sau un „transfer de siguranță”, deseori prin utilizarea unor bancomate de criptomonede

★ Ce trebuie să faceți pentru a vă proteja:

- ✓ **Nu aveți încredere în orice apel, chiar dacă numărul pare cunoscut.**
- ✓ **Nu dați niciodată datele cardului, parole sau coduri PIN prin telefon.**
- ✓ **Închideți apelul și sunați direct instituția respectivă folosind numărul oficial** de pe site-ul lor.
- ✓ **Dacă vi se pare ceva suspect, cereți ajutorul unui membru al familiei sau sunați la Poliție.**

! Important:

Nu vă lăsați păcăliți de numere care par oficiale. Infractorii pot copia orice număr. Dacă aveți dubii, **nu vorbiți cu persoana, nu urmați instrucțiunile și verificați din surse sigure.**

✗ SEMNE CLARE CĂ ESTE O ȚEAPĂ:

- ◆ Vi se promite că vă **îmbogățiți repede, cu bani puțini**
- ◆ Vi se spune că oferta este „numai azi” sau „pe timp limitat”, sau pentru „un număr limitat de persoane”
- ◆ Nu vi se oferă detalii clare despre companie
- ◆ Vi se cere să instalați aplicații necunoscute
- ◆ Vi se cere să trimiteți bani sau criptomonede în conturi străine

✓ CUM VĂ PROTEJAȚI:

1. **Fiți prudenți cu ofertele de investiții online.**
Dacă pare prea frumos să fie adevărat, mai mult ca sigur este o înșelătorie!
2. **Nu trimiteți bani necunoscuților!**
Nici prin transfer bancar, nici prin criptomonede!
3. **Nu instalați aplicații la cererea unor persoane necunoscute!**
Ele pot da acestora acces total la telefonul sau calculatorul dvs.
4. **Nu dați datele dvs. personale sau bancare pe site-uri pe care nu le cunoașteți.**
5. **Cereți sfatul unui membru al familiei sau unui prieten dacă nu sunteți siguri de o ofertă.**
6. **Verificați dacă firma este autorizată în România – consultați site-ul la Autorității de Supraveghere Financiară (ASF).**
7. **Nu cedați presiunii!**
Infractorii vor să luați decizii rapide, fără să verificați.
8. **Citiți documentele cu atenție.**
Orice ofertă serioasă trebuie să aibă informații clare, în scris.

📢 Ce să faceți dacă ați fost păcălit:

- Nu mai trimiteți bani!
 - Nu mai vorbiți cu escrocii!
 - Dacă ați efectuat tranzacții cu cardul, anunțați imediat banca!
 - Anunțați imediat Poliția și Directoratul Național de Securitate Cibernetică (DNSC)
-

RECOMANDĂRI PENTRU A EVITA ÎNȘELĂCIUNILE PRIN MESAJERIE (WhatsApp)

Informații importante oferite de Poliția Română

Atenție! În ultima perioadă, au apărut înșelăciuni pe WhatsApp și alte aplicații de mesaje. Infractorii trimit mesaje false, ca să vă fure contul și să ceară bani de la prietenii dumneavoastră.

Cum acționează infractorii:

1. **Trimit un mesaj fals**, ca fiind din partea unui cunoscut, din lista dvs. de contacte. Exemplu: „Bună! Te rog să o votezi pe fiica unor prieteni într-un concurs. Mulțumesc!”. Mesajul are un **link** ce trebuie accesat pentru a vota, **dar linkul este periculos**.
2. Dacă apăsați pe link, se deschide o **pagină falsă**, prin care vi se cere să urmați niște pași.
3. Pe fondul confuziei, **infractorii încep să vă copieze contul WhatsApp** pe alt dispozitiv – laptop sau calculator.
4. Vi se cere să **introduceți un cod PIN pe care îl primiți prin SMS** și vi se spune că e pentru confirmarea votului dar, de fapt, este codul prin care ei **preiau controlul asupra contului dvs. WhatsApp**.
5. Infractorii trimit apoi **mesaje către prietenii dumneavoastră, cerând bani în numele dumneavoastră**. Pot spune că aveți o urgență, că v-a fost blocat contul bancar etc.
6. **Astfel, autorii vă folosesc contul WhatsApp pentru a păcăli și alte persoane.**

Cum vă puteți proteja:

- ✓ **Nu deschideți link-uri primite prin mesaje**, chiar dacă par de la prieteni. Sunați persoana care v-a trimis mesajul și întrebați-o dacă e real.
- ✓ **Nu introduceți niciodată coduri PIN primite de la alte persoane.**
- ✓ **Evitați să reacționați în grabă**, mai ales dacă mesajul cere *ajutor urgent*.
- ✓ **Instalați un program antivirus din surse legitime.**
- ✓ **Activați „autentificarea în doi pași” în aplicația WhatsApp**. Este o măsură de siguranță suplimentară.
- ✓ **Fiți atenți la orice mesaj care vi se pare suspect**. Nu e nicio rușine să cereți părerea unui membru al familiei/prieten.

Ce faceți dacă ați fost păcălit?

- Nu dezinstalați aplicația WhatsApp.
- Intrați în setările aplicației și deconectați orice alt dispozitiv necunoscut.
- Anunțați imediat prietenii că mesajele trimise din contul dumneavoastră nu sunt reale.
- Raportați incidentul autorităților:

☎ **Poliția Română** – accesați site-ul oficial la secțiunea „Contact/Trimite o petiție online” [Poliția Română - Poliția Română](#)

☎ **Directoratul Național de Securitate Cibernetică (DNSC)** – sunați la 1911 sau intrați pe site-ul DNSC și apăsați butonul „**Raportează un incident**” [DNSC | PNRISC](#)

ATENȚIE LA ÎNȘELĂCIUNILE CU INVESTIȚII ONLINE!

Cum să vă protejați de fraude legate de acțiuni și criptomonede

Ce se întâmplă?

Tot mai multe persoane, inclusiv în România, au fost păcălite să investească bani în platforme online **false** de acțiuni sau monede virtuale.

Infractorii promit *câștiguri rapide, cu investiții mici*, dar **totul este o înșelătorie**. Scopul lor este să vă fure banii și datele personale.

Cum acționează infractorii:

1. **Postează reclame false pe Facebook sau alte rețele sociale**, cu titluri precum:
„Investește acum în companii românești”
„Afacerea care îți poate dubla banii”
Folosesc **imagini false cu persoane cunoscute** (președintele țării, prezentatori TV, firme mari).
2. Dacă dați clic pe reclamă, vi se cere: numele, telefonul și adresa de e-mail. Cu aceste informații, vă vor contacta rapid.
3. Sunteți sunați de persoane necunoscute (uneori vorbesc limba română cu accent străin). Ele vă conving să „investiți” o sumă mică, care va aduce rapid **profituri mari**.
4. Vi se cere să instalați o aplicație „de ajutor”. Aceasta le oferă acces complet la telefonul sau calculatorul dvs.
Așa pot fura parole, date bancare, documente.
5. Vi se arată un cont fals cu „profituri mari”, ca să fiți încurajați să trimiteți mai mulți bani. În realitate, **nu există nicio investiție. Totul este o păcăleală.**
6. După ce descoperiți fraudă, există posibilitatea de a fi din nou contactați de **alți escroci**, care pretind că sunt „de la autorități” și vă pot ajuta să recuperați banii – **dar cer o „garanție”**.
Aceasta este o a doua înșelătorie!