

## Atenție la fraudele prin apeluri telefonice / mesaje false

În ultima perioadă s-a intensificat numărul de tentative de fraudă prin tipologia de spoofing - o metodă prin care atacatorii falsifică numărul de telefon sau identitatea afișată, astfel încât apelul sau mesajul să pară că vine de la contrapartide de încredere:

- Bancă
- instituții publice (Poliție, BNR, ANAF etc. )
- firme cunoscute
- persoane de încredere.

### Important de știut:

Chiar dacă pe ecran apare un număr real sau un nume cunoscut, apelul poate fi unul fals și care încearcă impersonarea unei contrapartide de încredere.

### Cum încearcă acești fraudatori să vă păcălească:

- vă solicită date personale (CNP, coduri, parole)
- vă solicită coduri SMS sau aprobări să acceseze aplicația bancară
- creează presiune ("cont blocat", "tranzacție suspectă", "urgență", "bani de primit")
- vă solicită plăți rapide sau transferuri

### Care sunt măsurile de aplicat pentru a vă proteja de acest gen de fraude:

- Nu oferiți date personale sau bancare la telefon
- Nu comunicați coduri primite prin SMS
- Nu instalați aplicații la cererea unui apelant
- Nu accesați linkuri din mesaje suspecte sau primite via WhatsUp, SMS, e-mail etc.

### Ce trebuie să faceți dacă primiți un astfel de apel:

- Închideți apelul imediat.
- Sunați la numărul oficial (de pe site-ul Băncii sau numărul de spatele cardului, nu din mesaj, la numerele oficiale publicate pe website-urilor instituțiilor publice), respectiv la datele de contact deținute ale contrapartidelor dvs. pentru a valida autenticitatea apelului.
- Raportați imediat tentativă (Bancă, Poliție - dacă e cazul).

### Banca NU vă solicita niciodată:

- parole
- PIN-uri
- coduri de autentificare
- aprobare de plăți la telefon.

Dacă ați constatat suspiciuni privind autenticitatea unei comunicări / apel telefonic, contactează-ne prin canalele oficiale ale Băncii.