PREVENIREA FRAUDELOR FINANCIARE

Reguli de bază

GHID PRACTIC

Banca Națională a Moldovei

Tentativele de fraudă financiară au devenit tot mai diverse, mai convingătoare și mai greu de recunoscut la prima vedere. Escrocii folosesc apeluri telefonice, SMS-uri, e-mailuri, aplicații de mesagerie, pagini web false sau chiar numere de telefon care par oficiale, pentru a obține bani, date bancare, parole, coduri OTP sau acces la conturi.

Ghidul aduce în atenție principalele forme de fraudă întâlnite în prezent și câteva reguli simple care pot preveni pierderile financiare.

Nicio instituție publică, Banca Națională a Moldovei și nicio bancă licențiată nu vă cer datele cardului, parole, coduri OTP sau transferul banilor într-un „cont sigur” - nici prin telefon, nici prin mesaje prin SMS, Viber, WatsApp, Telegram etc.

! Regula de bază

PRINCIPALELE TIPURI DE FRAUDĂ

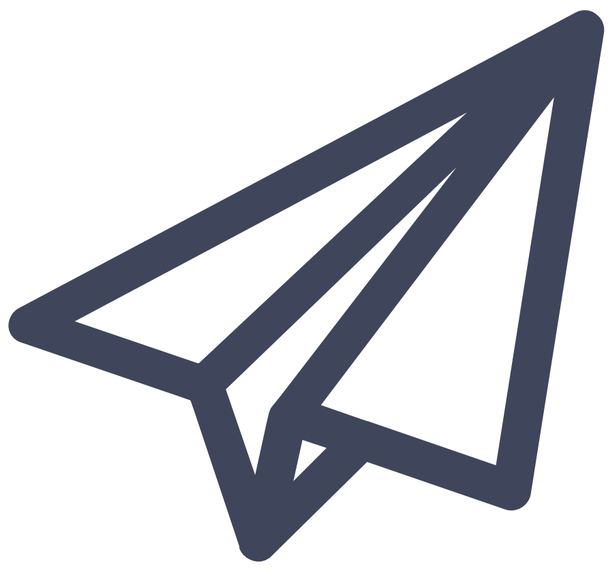
1. IMPERSONAREA BĂNCILOR, POLIȚIEI, INSTITUȚIILOR PUBLICE

! NU transmiteți date bancare și nu efectuați transferuri la solicitarea persoanelor care vă contactează telefonic.

Escrocii pot pretinde că sunt reprezentanți ai unei bănci, ai poliției, SIS, procuraturii sau ai altor instituții. De regulă, încearcă să sperie victima, spunând că banii sunt în pericol, că există o anchetă sau că trebuie luate măsuri urgente.

2. FRAUDE PRIN APLICAȚII DE MESAGERIE ETC.

! NU dați curs solicitărilor financiare primite prin aplicații de mesagerie.
Verificați întotdeauna informația prin canale oficiale.



Persoane necunoscute pot contacta cetățenii prin aplicații de mesagerie (Telegram, Viber, WatsApp etc.) și pot pretinde că reprezintă instituții publice, bănci licențiate, companii sau chiar rude apropiate.

3. PHISING ȘI SMISHING

! NU accesați linkuri primite prin SMS sau e-mail de la surse necunoscute sau neverificate. Informați-vă doar din surse oficiale.

Victima primește e-mailuri sau SMS-uri false, cu linkuri care imită pagini oficiale ale băncilor, instituțiilor publice, companiilor de curierat sau altor organizații cunoscute.

4. APELURI TELEFONICE FRAUDULOASE - VISHING

! NU comunicați niciodată coduri OTP, parole sau date de autentificare prin telefon.

Escrocii telefonează și încearcă să obțină coduri OTP, parole, date de card sau confirmarea unor tranzacții.

5. FRAUDE CU OTP ȘI CREDITE ONLINE

! Codurile OTP sunt strict personale. Nu le transmiteți nimănui, indiferent de motivul invocat.

Escrocii pot obține codurile OTP expediate prin SMS și le pot folosi pentru contractarea unor credite online sau pentru autorizarea unor operațiuni în numele victimei.

6. LINKURI ȘI PAGINI FALSE

! NU introduceți datele cardului pe pagini neverificate.
Verificați atent adresa site-ului și utilizați doar site-urile oficiale.

Victima este direcționată către pagini web false/clonate, unde i se cere să introducă datele cardului, parole, coduri de securitate sau informații personale etc.

7. FRAUDE INVESTIȚIONALE

! NU investiți bani în platforme neverificate și nu luați decizii financiare la recomandarea persoanelor necunoscute.

Escrocii promit câștiguri rapide și sigure din criptomonede, acțiuni, platforme de tranzacționare sau alte produse financiare fictive.

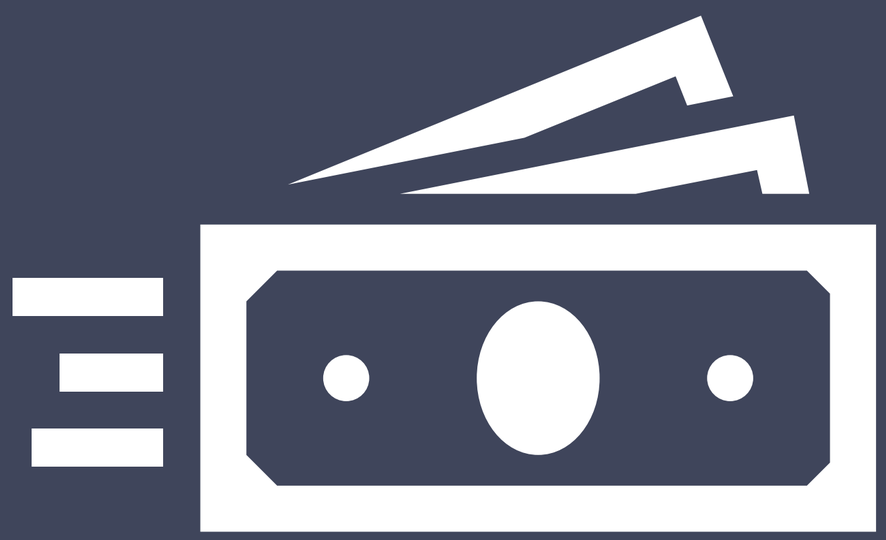
8. „CONTURI SIGURE”

! NU transferați bani în „conturi sigure”. Acesta este un semnal clasic de fraudă.

Victimei i se spune că banii săi sunt în pericol și că trebuie transferați urgent într-un „cont sigur”.

9. CONTURI FOLOSITE PENTRU TRANSFERUL BANILOR PROVENIȚI DIN FRAUDE

! NU acceptați să primiți sau să transferați bani pentru persoane necunoscute.



Unele persoane sunt convinse să ofere acces la conturile lor sau să transfere bani pentru alte persoane, contra unei recompense.
În acest mod, acestea pot deveni implicate în scheme ilegale.

10. FALSIFICAREA NUMĂRULUI DE TELEFON - SPOOFING CALLER ID

! NU aveți încredere doar în numărul afișat pe telefon. Închideți apelul și sunați direct instituția, folosind numărul de pe site-ul oficial.

Escrocii pot falsifica numărul afișat pe ecran, astfel încât apelul să pară că vine de la o bancă, instituție publică sau altă organizație oficială.

11. FRAUDE PRIN APLICAȚII DE ACCES LA DISTANȚĂ

! NU instalați aplicații la solicitarea persoanelor necunoscute și nu permiteți accesul la distanță asupra dispozitivelor personale.

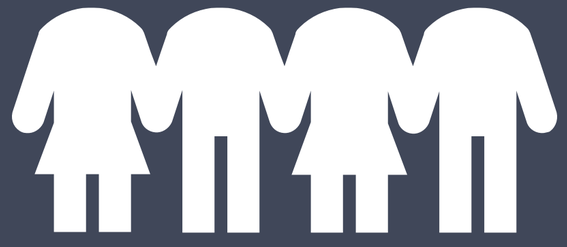
Escrocii vă pot convinge să instalați aplicații prin care obțin acces de la distanță la telefon, tabletă, laptop sau calculator, precum și la datele stocate pe aceste dispozitive.

12. FRAUDE PRIN CURIERI, COLETE, TAXE SAU AMENZI FALSE

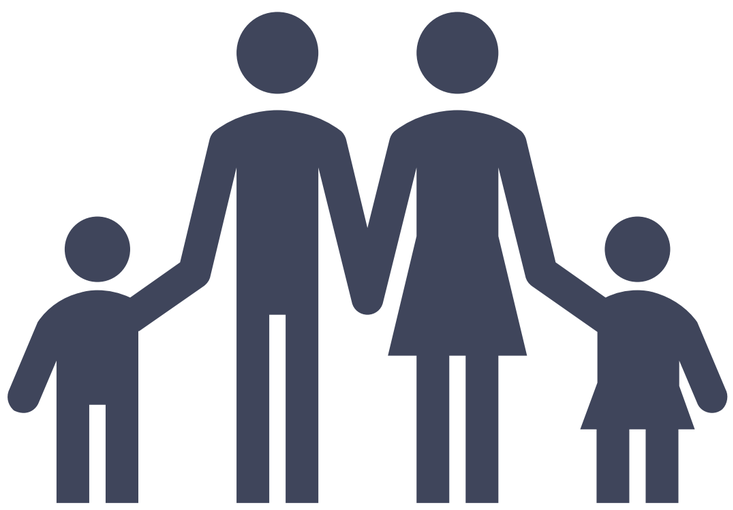
! Nu efectuați plăți accesând linkuri primite prin SMS sau aplicații de mesagerie.

Verificați direct informația pe site-ul oficial al instituției sau companiei.

Escrocii transmit mesaje privind colete, livrări, taxe, amenzi sau plăți urgente și direcționează victima către pagini false de plată.



TRANSMITEȚI ACESTE INFORMAȚII ȘI CELOR APROPIAȚI!



Prevenirea fraudelor începe cu fiecare dintre noi, dar și prin grija față de familie și comunitate.

Discutați despre aceste riscuri cu părinții, bunicii, copiii, rudele și cu toți cei care vă sunt în preajmă.

O CONVERSAȚIE SIMPLĂ POATE PREVENI O PIERDERE FINANCIARĂ ENORMĂ!

! Mesaj-cheie de retinut

- **NU oferiți date bancare nimănui**
- **NU transmiteți coduri OTP**
- **NU transferați bani**
- **NU acceptați bani**

la solicitarea persoanelor care vă contactează telefonic sau prin mesaje. Verificați întotdeauna informația prin canale oficiale și persoana care vă apelează.

În cazul unei situații suspecte:

1. **Nu vă grăbiți.** Escrocii mizează pe panică și presiune psihologică.
2. **Nu comunicați date bancare, parole sau coduri OTP.**
3. **Nu accesați linkuri suspecte și nu instalați aplicații indicate de persoane necunoscute.**
4. **Închideți apelul și verificați informația prin canale oficiale.**
5. **Contactați direct banca sau instituția vizată**, folosind datele de contact publicate pe site-ul oficial.
6. **Apelați 112** și informați autoritățile.
7. **Discutați cu rudele și apropiații** despre aceste riscuri, pentru a preveni manipularea și pierderile financiare.

MESAJE GENERICE

„ATENȚIE la mesajele și apelurile care cer bani, date personale sau confirmări urgente. Verifică sursa și nu trimite informații bancare către necunoscuți.”

„NU oferi date bancare, parole sau coduri și verifică orice apel sau mesaj care promite câștiguri rapide. Contactează direct banca sau instituția pe canalele oficiale.”

MESAJE GENERICE

18–25 ani

„Ai primit un link despre un «câștig rapid» sau investiții garantate? Verifică sursa înainte să introduci datele cardului. Fraudele online pot goli contul în câteva minute.”

„Nu trimite codurile primite prin SMS nimănui - nici măcar dacă persoana pretinde că este de la bancă. Banca NU cere parole sau coduri de confirmare.”

MESAJE GENERICE

26–45 ani

„Atenție la apelurile urgente despre conturi blocate sau tranzacții suspecte! Închide apelul și contactează direct banca folosind numărul oficial.”

„Verifică de două ori IBAN-ul și destinatarul înainte de orice transfer. Escrocii folosesc conturi false și mesaje care par reale.”

MESAJE GENERICE

46+ ani
„Nu oferi date personale sau bancare prin telefon persoanelor necunoscute. Dacă ai dubii, cere ajutorul unui membru al familiei sau contactează banca direct.”

„Mesajele despre premii, moșteniri sau investiții «fără risc» pot ascunde fraude. Dacă oferta pare prea bună ca să fie adevărată, probabil este falsă.”

Banca Națională
a Moldovei

35 ani

www.bnm.md