

**#Dreptullabanking: Clienții băncilor sunt invitați să acorde
atenție sporită mesajelor antifraudă**

Băncile din România au implementat măsuri tehnice și desfășoară campanii ample, consistente și susținute pentru reducerea riscului de fraudă în mediul online cu care se pot confrunta clienții lor, preocuparea fiind creșterea competențelor utilizatorilor pentru prevenirea acestora. Asociația Română a Băncilor dezvoltă, în numele băncilor, proiectul național Siguranțaonline, împreună cu Poliția Română și Directoratul Național de Securitate Cibernetică, prin intermediul căruia mesajele au fost distribuite către peste 10 milioane de utilizatori. Cetățenii se pot informa inclusiv pe www.siguranțaonline.ro despre principalele riscuri și amenințări cu care se pot confrunta în interacțiunea cu canalele online, printre care phishing, propunerile false de investiții care includ și clipuri alterate cu tehnologia deepfake, spoofing etc.

Clienții băncilor sunt invitați să acorde atenție sporită mesajelor informative antifraudă provenite de la instituțiile de credit prin Internet/Mobile banking, website, newsletter, social media, podcast și prin intermediul campaniilor și conferințelor desfășurate pentru a crește nivelul de siguranță online.

Instituțiile de credit transmit utilizatorilor mesaje în aplicațiile de Internet/Mobile banking pentru revizuirea și actualizarea periodică a setărilor de securitate și sunt postate bannere antifraudă în aceste aplicații. Băncile diseminează newslettere dedicate siguranței online, care prezintă cele mai frecvente practici de tip scam, cu exemple concrete și care subliniază importanța parolelor puternice, autentificării în doi pași și a altor practici de securitate.

În campaniile antifraudă care se desfășoară în mass-media și social media sunt oferite informații ample despre aplicațiile pe care să nu le instaleze pe telefon și în ce context reprezintă un pericol pentru siguranța datelor bancare, despre propunerile false de investiții, tentativele de fraudă legate de investiții în criptomonede sau prin apeluri false.

Pentru siguranța lor, utilizatorii sunt rugați:

- Să nu furnizeze datele de pe cardul bancar în nicio situație: nume, număr, data de expirare, codul de securitate de pe spatele cardului format din trei cifre. Aceste date se folosesc doar de către utilizator pentru plata online pe site-uri securizate și nu atunci când este conectat la o rețea Wi-Fi publică, ci trebuie să fie securizată.
- Să se informeze că băncile nu vor cere niciodată informații privind parolele de acces la contul bancar și nici datele de pe cardurile bancare. În situația în care datele le-au fost solicitate telefonic de către orice persoană, recomandarea pentru clienți este să încheie apelul imediat.
- Să nu furnizeze niciodată datele personale de utilizare a contului bancar (username și parola de acces la contul bancar) altor persoane;
- Să furnizeze IBAN-ul, nu datele de pe card, dacă trebuie să primească bani;
- Să nu introducă codul PIN de la cardul bancar pe site-uri de internet și să nu-l divulge;
- Să nu creadă promisiunile nerealiste legate de investiții și să păstreze un simț critic. Dacă sună prea bine pentru a fi adevărat, este posibil să fie o fraudă. Să fie sceptici față de promisiunile de câștiguri imense și rapide, dar și față de anunțuri care se prezintă ca oferte pe termen limitat. Investițiile financiare presupun riscuri și nu sunt garantate;
- Să nu instaleze aplicații, la solicitarea unor persoane pe motiv că sunt aplicații de investiții, prin care pot fi vulnerabilizați în fața tentativelor de fraudă;
- Să contacteze imediat banca și să notifice autoritățile dacă au fost victima fraudelor.

