MESAJ DE INFORMARE

cu privire la riscurile de securitate

Banca Cooperatistă Istrița Buzău recunoaște importanța securității tranzacțiilor bancare și oferă câteva exemple și sfaturi pentru a vă ajuta să identificați și să preveniți situațiile de fraudă.

Cele mai utilizate tehnici pentru fraudarea consumatorilor sunt vishingul și **phishingul** Utilizând aceste tehnici, fraudatorii profită de consumatori, în special de cei vulnerabili, și de lipsa lor de cunoștințe și de conștientizare cu privire la siguranța digitală. Cei mai expuși fraudelor de la distanță sunt persoanele în vârstă și clienții băncilor care nu sunt familiarizați cu plățile digitale cu amănuntul.

Pentru protecția dumneavoastră, Banca Cooperatistă Istrița Buzău vă prezintă cele mai relevante exemple utilizate de fraudatori, astfel încât dumneavoastră să puteți recunoaște astfel de încercări și să vă puteți apăra.

Atacurile de vishing sunt cele mai frecvente atacuri îndreptate către persoanele fizice și se produc prin convorbiri telefonice.

Exemple de atacuri de vishing:

1. Vishing prin apel telefonic:

- Atacatorii pretind a fi reprezentanți ai unor companii cunoscute (BNR, Bursa de valori București BVB, bănci etc.) și încearcă să obțină informații sensibile legate de conturi sau de carduri.
- Exemple:
  - "Sunt de la banca dumneavoastră. Există o activitate suspectă pe contul dumneavoastră."
  - "Sunt de la Microsoft. Computerul dumneavoastră a fost infectat cu virus."
  - ”Sunt inspector la Direcția de Combatere a Fraudelor Cibernetice. Datele dumneavoastră bancare au fost compromise și urmează să fie efectuate transferuri neautorizate din conturile dumneavoastră. O să trimit pe WhatsApp un link pentru a instala aplicația oficială de securitate a Poliției Române și trebuie să dați click pe link.” Deoarece linkul este fraudulos, după ce clientul dă click pe link, fraudatorul va obține control total asupra telefonului și a contului bancar al victimei și poate transfera orice sume de bani.

2. Atacuri de falsificare prin telefon (Spoofing):

- Atacatorii afișează un număr de telefon fals pe ecranul victimei, astfel încât poate părea că apelul provine de la o companie cunoscută
- Exemple:
  - Numărul de telefon afișat este cel al băncii dumneavoastră sau numărul de telefon afișat este cel al companiei de electricitate

Deoarece veți crede că ați fost sunat de la o sursă de încredere, este posibil să oferiți atacatorului informații confidențiale pe care acesta să le folosească pentru a frauda. Este important să nu dați nici un fel de informații personale sau legate de conturi prin telefon.

3. Presiunea psihologică:

- Atacatorii utilizează tactici de intimidare și alarmă și încearcă să determine victima să acționeze rapid, fără a se gândi
- Exemple:
  - "Contul dumneavoastră va fi blocat dacă nu ne furnizați imediat parola."
  - "Trebuie să plătiți imediat această factură pentru a evita deconectarea."

4. Atacuri de falsificare combinate cu presiunea psihologică:

- Atacatorii utilizează tactici de intimidare și alarmă și, în același timp, poate părea că apelul provine de la un număr de telefon cunoscut
- Exemplu:
  - Numărul de telefon afișat este al unei rude apropiate și se cer bani pentru că, de exemplu, a avut loc un accident și ruda nu poate vorbi sau se inventează tot felul de motive. Datorită tonului alertant pe care îl folosește fraudatorul, victima se sperie și nu mai gândește limpede, astfel încât satisface cerințele fraudatorului.

5. Inginerie socială:

- Atacatorii construiesc o relație de încredere cu victima și obțin astfel informații sensibile prin conversație
- Exemple:
  - Atacatorul se preface că este un prieten sau un membru al familiei
  - Atacatorul pretinde că are nevoie de ajutor pentru a rezolva o problemă

Atacurile de phishing sunt acele atacuri care vin pe cale scrisă (e-mail, sms, WhatsApp)

Exemple de atacuri de phishing:

1. Emailuri frauduloase:

- Simulează mesaje de la entități de încredere (BNR, Bursa de valori București BVB, bănci etc.)
- Conțin linkuri malițioase sau atașamente infectate
- Utilizează un ton alarmant sau urgent pentru a grăbi victima
- Exemple:
  - "Contul tău a fost suspendat! Click aici pentru a-l reactiva."
  - "Ai primit o nouă factură. Descarcă atașamentul pentru a o vizualiza."

Dacă veți da click sau veți descărca atașamentul, fraudatorul va obține control total asupra computerului sau telefonului și a chiar a contului bancar și va putea transfera sumele de bani aflate în cont.

2. Phishing prin SMS:

- Este similar cu phishingul prin email, dar utilizează mesaje text. Linkurile pe care vi se cere să dați click, vă pot redirecționa către site-uri web false, care par de încredere și de pe care vi se pot cere informații legate de conturi sau carduri. Dacă le veți oferi, atacatorul va putea dispune de banii dumneavoastră.
- Exemple:
  - "Ai câștigat un premiu! Click pe link pentru a-l revendica."
  - "Există o problemă cu contul tău. Trimite-ne parola pentru a o verifica."
  - ”Ai primit un colet la Poșta Română. Click aici pentru a plăti taxe vamale.”

<u>Măsuri de protecție pe care le puteți lua:</u>

- Fiți atenți la mesajele nesolicitate, fie că vin prin email, SMS sau telefon și nu răspundeți la ele;
- Fiți atent la mesajele generice – mesajele frauduloase sunt, de multe ori, impersonale și cu greșeli gramaticale, sau cu greșeli de exprimare;
- NU faceți click pe linkuri care vin pe e-mail sau pe telefon (WhatsApp, SMS) și NU deschideți atașamente din surse necunoscute care vin pe aceste canale;
- NU furnizați niciodată informații personale sau legate de cont (inclusiv parole) prin telefon sau email;
- NU comunicați niciodată date aferente cardurilor tale (ex. codul PIN, codul CVV2/CVC – reprezentat de ultimele 3 cifre de pe spatele cardului);
- Contactați direct banca, instituția sau compania de la care a primit mesaj sau telefon, pe adrese de e-mail sau pe numere de telefon oficiale, pentru a verifica veridicitatea mesajului;
- Utilizați un software antivirus actualizat;
- Fiți informat și acordați atenție comunicărilor transmise de bancă cu privire la avertizări de securitate sau cu privire la cele mai noi tehnici de phishing și vishing. Consultați informațiile de securitate de pe site-ul băncii **Cooperatiste Istrița Buzău** la adresa bancaistrita.ro/securitate/

Vă reamintim că Banca Cooperatistă Istrița Buzău nu vă va solicita, in nicio situație, prin niciun mijloc de comunicație (verbal direct, telefonic, SMS, e-mail etc.**) informații confidențiale (**user/ parolă, număr de card, data expirării acestuia, codul PIN**) sau accesarea unor adrese URL sau link-uri către site-uri unde vă este solicitat să introduceți informații confidențiale.** De asemenea**, <u>informații precum parola și codul PIN</u> <u>nu trebuie divulgate sub niciun motiv</u>, <u>nimănui și nici chiar Băncii</u>. Daca ați primit o astfel de solicitare, vă rugăm să ne contactați imediat!**

Am luat la cunoștință, Nume, prenume și semnătura

Data ……... ……