Poliția Română, Directoratul Național de Securitate Cibernetică și Asociația Română a Băncilor avertizează asupra riscului de fraudă prin apeluri telefonice false (spoofed)

Poliția Română, Directoratul Național de Securitate Cibernetică (DNSC) și Asociația Română a Băncilor (ARB) atrag atenția, prin intermediul proiectului național de conștientizare **#SigurantaOnline**, asupra creșterii fraudelor prin apeluri telefonice false (spoofed) în ultima perioadă. Concret, infractorii se prezintă ca funcționari bancari și utilizează în fals numere de telefon ale băncilor sau similare, folosind un discurs inedit, persuasiv și înșelător.

Spoofing-ul numărului de telefon este o tehnică de înșelăciune prin care un atacator își modifică numărul de telefon, astfel încât să apară pe ecranul persoanei apelate un alt număr decât cel real. Această metodă este utilizată pentru a induce în eroare victima, determinând-o să creadă că interlocutorul reprezintă o entitate legitimă, cum ar fi o bancă sau o altă instituție, fiind folosită pentru a obține informații personale sau bancare sensibile.

În ultimele zile este activă o campanie care se folosește de numele unor bănci pentru apeluri false (spoofed) în care atacatorii apelează potențiale victime și se prezintă drept angajați ai acestora.

În actuala variantă de campanie frauduloasă, persoana apelată telefonic este anunțată că i s-a aprobat creditul solicitat. Primul instinct este acela de a reacționa rapid și de a efectua demersurile necesare pentru anularea acestei acțiuni. Atacatorii mizează pe acest aspect încă de la început, și anume pe activarea rapidă a emoției, pentru a evita ca interlocutorul să acționeze cu calm la telefon și să pună întrebările logice în acest caz, ori să facă verificări suplimentare, pe un alt canal de comunicare cu banca sau cu autoritățile.

Din momentul în care persoana apelată anunță că nu a efectuat vreo cerere pentru acordarea unui credit, atacatorii îi spun că în acel caz este cel mai probabil vorba despre o „fraudă" și că vor avea nevoie de anumite date personale, date de autentificare, respectiv date bancare, pentru a face demersurile necesare raportării presupusei „fraude" și pentru a recupera eventualele sume pierdute. Acesta este un scenariu înșelător în care sunt folosite extrem de bine tehnici de inginerie socială, iar atacatorii sunt foarte bine antrenați în a fi convingători și amabili.

Recomandări pentru evitarea atacurilor prin apeluri telefonice false (spoofed):

- **Verificați întotdeauna sursa/autenticitatea apelurilor telefonice primite printr-un canal de comunicare oficial alternativ, înainte de a oferi orice informații personale.**
- **Refuzați apelurile care vi se par suspecte, chiar dacă pretind că provin de la bănci sau alte autorități și apar numere de telefon ale acestora sau asemănătoare.**
- **Nu furnizați date personale la telefon și nici date bancare! Băncile nu vor cere niciodată informații privind parole de acces la contul bancar și nici date de pe cardurile bancare. Nu răspundeți la astfel de solicitări și încheiați apelul imediat.**
- **Nu discutați despre credite și bani la telefon! O bancă nu va apela niciodată telefonic utilizatorii pentru a anula credite sau a le promite recuperarea unor sume de bani.**
- **Raportați apelurile suspecte. Dacă primiți un apel care vi se pare dubios, informați imediat banca/instituția în numele căreia se pretinde că a fost efectuat apelul pentru a ajuta la identificarea rapidă a tentativelor de fraudă.**
- **Notificați autoritățile dacă ați fost victima fraudelor. Dacă ați divulgat accidental date personale sau ale cardului, contactați imediat banca pentru a bloca accesul la conturi și raportați incidentul la Poliție și la Directoratul Național de Securitate Cibernetică.**
- **Spuneți prietenilor și familiei despre atacurile care folosesc instrumente pentru a realiza apeluri spoofed. Astfel ajutați direct la conștientizarea noilor amenințări din mediul online și la reducerea numărului potențial de victime ale acestor atacuri. Contribuiți la răspândirea**

acestor avertizări prin detalii asupra discursului inedit și înșelător folosit de atacatori pentru a reduce șansele ca astfel de tentative de fraudă să aibă succes.

Dacă v-ați divulgat datele cardului bancar, este important să contactați imediat banca pentru a bloca orice tranzacții neautorizate. În cazul în care constatați că ați suferit pierderi financiare ca urmare a unui incident de tip spoofing, depuneți o plângere oficială la Poliție. De asemenea, informați Directoratul Național de Securitate Cibernetică fie telefonic la numărul 1911, fie prin e-mail la alerts@dnsc.ro, pentru a contribui la prevenirea unor astfel de incidente în viitor.

Proiectul național de educație digitală **#SigurantaOnline** este menit să ofere cele mai bune practici de securitate cibernetică, prin accesarea platformei sigurantaonline.ro, pentru a evita ca utilizatori din România să devină victime ale fraudelor informatice. **#SigurantaOnline** este o inițiativă a Poliției Române, Directoratului Național de Securitate Cibernetică și Asociației Române a Băncilor, la care s-au raliat și alte entități public-private.