#Dreptullabanking: Comunitatea bancară recomandă clienților să manifeste vigilență sporită în cazul plăților efectuate on line

București, 14 iunie 2021- Comunitatea bancară recomandă clienților să manifeste vigilență sporită în cazul plăților efectuate on line întrucât, în situația unei fraude, conform normelor europene, băncile nu pot recupera banii pentru clienți dacă tranzacțiile sunt realizate cu autentificarea strictă a acestora.

Sistemul bancar continuă campania de conștientizare asupra fraudelor din mediul online și avertizează că tranzacțiile în care sunt completate toate elementele de siguranță ale cardului și sunt autorizate de către clienți, prin canalele convenite anterior cu emitentul, nu sunt considerate frauduloase.

Elementele de securitate ale cardului sunt numărul cardului, data de expirare și CVV2/CVC2, iar aprobarea tranzacției se realizează de regulă în aplicația de Internet Banking/aplicația de autorizare a semnăturii sau prin validarea unei parole și trimiterea unui cod unic primit de titularul cardului pentru autorizarea fiecărei plăți. Astfel, autentificarea strictă a clientului înseamnă folosirea a două elemente din următoarele categorii: ceva ce clientul cunoaște (codul PIN, parola), ceva ce clientul deține (telefonul mobil, verificat prin parola transmisă prin SMS) și ceva ce clientul este (amprenta, recunoașterea facială).

Pentru tranzacțiile efectuate cu autentificarea strictă a clienților, reglementate conform noii Directive Europene privind Serviciile de Plăți - PSD2, transpusă în legislația română în Legea 209 /2019, coroborat cu prevederile regăsite în reglementările organizațiilor de carduri, băncile nu pot iniția dispute pe motiv de fraudă, iar șansele să recupereze sumele pentru clienții lor sunt aproape nule.

În contextul pandemiei COVID-19, tentativele de fraudă în mediul online s-au amplificat, iar atacatorii au devenit mai abili în accesarea datelor personale ale utilizatorilor prin website-uri false, e-mail-uri, SMS-uri și mesaje în social media. În multe cazuri, aceste date sunt furnizate direct de către deținătorii de carduri.

În mod frecvent, modelul de atac vizează contexte reale, ca de exemplu contactarea utilizatorilor care au postat anunțuri pe platforme de vânzare-cumpărare sau care au plasat comenzi pe site-uri din străinătate. Tentativele de fraudă sunt direcționate atât către cumpărători, cât și către vânzători.

Astfel, sub pretextul plății produsului postat spre vânzare sau a achitării unor eventuale taxe (de transport sau vamale, în cazul comenzilor externe), cumpărătorii primesc un link către o pagină de internet falsă, care imită pagina oficială a comercianților sau a companiilor. Pe aceste pagini false, clienții își introduc datele cardului și/ sau credențialele de autentificare în Internet Banking sau soldul disponibil existent pe card.

După introducerea datelor bancare, clienții aprobă tranzacțiile prin autorizarea acestora pe canalele convenite cu banca. În acest mod, atacatorii obțin toate datele cardului și în cele mai multe cazuri, folosesc aplicații pentru transferul instant al banilor, iar băncile emitente nu pot stopa astfel de operațiuni.

<u>Recomandările comunității bancare pentru securitatea contului</u>

Pentru a se proteja împotriva fraudelor, este necesar ca toți utilizatorii de carduri să fie vigilenți și să respecte următoarele recomandări:

- Datele bancare sunt confidențiale și nu trebuie furnizate;

- Nu furnizați niciodată datele cardului dacă aveți produse de vânzare postate pe diferite site-uri sau aplicații. Nu introduceți datele cardului pe paginile primite și nu le oferiți altor persoane. Cardul bancar are doar rolul de plată, niciodată de încasare. În cazul în care trebuie să primiți bani, puteți trimite doar codul IBAN. Un mesaj cu cod de autorizare nu va veni niciodată când trebuie să primiți bani, iar trimiterea codului primit înseamnă autorizarea unei plăți.
- În cazul în care doriți să achiziționați produse de pe site-urile de vânzare, asigurați-vă că site-ul este cel corect. Cel mai sigur este să introduceți adresa website-ului în bara de navigare și să nu dați click pe link-uri necunoscute (primite pe SMS/ WhatsApp/ e-mail), deși acestea pot fi similare paginii platformei de vânzare. Aceste recomandări sunt valabile și în alte cazuri (site-urile companiilor de curierat, a celor care oferă pachete de vacanță etc.).
- În cazul în care ați achiziționat un produs de pe un site extern/ intern și ulterior, primiți mesaje în care vă sunt solicitate datele de card pentru plata unor taxe de vamale sau de curierat, luați legătura cu respectivul comerciant pentru a confirma autenticitatea acestora. În cazul achiziționării unui produs de pe un site extern, comerciantul menționează încă de la început valoarea acestuia și eventuale cheltuieli de livrare. Prin urmare, în majoritatea cazurilor, trebuie să rețineți că astfel de solicitări vin din partea atacatorilor.
- În cazul în care ați furnizat totuși datele de card și primiți o solicitare pentru autorizarea unei tranzacții, verificați cu atenție detaliile afișate și renunțați la efectuarea acesteia. Detaliile afișate sunt următoarele:
    - Faptul că se autorizează o plată;
    - Numele comerciantului la care se efectuează plata;
    - Valoarea tranzacției;
    - Data tranzacției;
    - Terminația numărului de card utilizat.
- Dacă ați efectuat totuși o astfel de tranzacție, blocați imediat cardul din aplicația de Internet Banking sau sunați banca emitentă la numărul de telefon de pe spatele cardului pentru blocarea de urgență a cardului. Anunțați întotdeauna banca dacă primiți mesaje suspecte. Păstrați întreaga corespondență purtată cu autorul fraudei și depuneți o sesizare la Poliția Română.

www.dreptullabanking.ro

Facebook @DreptulLaBanking