

Comunitatea bancara recomanda clientilor sa manifeste vigilenta sporita în cazul platilor efectuate online

Comunitatea bancara recomanda clientilor sa manifeste vigilenta sporita în cazul platilor efectuate online întrucât, în situatia unei fraude, conform normelor europene, bancile nu pot recupera banii pentru clienti daca tranzactiile sunt realizate cu autentificarea stricta a acestora, potrivit unui comunicat al Asociatiei Române a Bancilor (ARB).

Conform sursei citate, sistemul bancar continua campania de constientizare asupra fraudelor din mediul online si avertizeaza ca tranzactiile în care sunt completate toate elementele de siguranta ale cardului si sunt autorizate de clienti, prin canalele convenite anterior cu emitentul, nu sunt considerate frauduloase.

Elementele de securitate ale cardului sunt numarul cardului, data de expirare si CVV2/CVC2, iar aprobarea tranzactiei se realizeaza de regula în aplicatia de internet banking/aplicatia de autorizare a semnaturii sau prin validarea unei parole si trimiterea unui cod unic primit de titularul cardului pentru autorizarea fiecărei plati. Astfel, autentificarea stricta a clientului înseamna folosirea a doua elemente din urmatoarele categorii: ceva ce clientul cunoaste (codul PIN, parola), ceva ce clientul detine (telefonul mobil, verificat prin parola transmisa prin SMS) si ceva ce clientul este (amprenta, recunoasterea faciala).

Pentru tranzactiile efectuate cu autentificarea stricta a clientilor, reglementate conform noii Directive Europene privind Serviciile de Plati - PSD2, transpusa în legislatia româna în Legea 209/2019, coroborat cu prevederile regasite în reglementarile organizatiilor de carduri, bancile nu pot initia dispute pe motiv de fraudă, iar sansele sa recupereze sumele pentru clientii lor sunt aproape nule.

Potrivit organizatiei, 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 si mesaje în social media. În multe cazuri, aceste date sunt furnizate direct de detinatorii de carduri.

În mod frecvent, modelul de atac vizeaza contexte reale, ca de exemplu contactarea utilizatorilor care au postat anunturi pe platforme de vânzare-cumparare sau care au plasat comenzi pe site-uri din strainatate. Tentativele de fraudă sunt directionate atât catre cumparatori, cât si catre vânzatori.

Astfel, sub pretextul platii produsului postat spre vânzare sau a achitarii unor eventuale taxe (de transport sau vamale, în cazul comenzilor externe), cumparatorii primesc un link catre o pagina de internet falsa, care imita pagina oficiala a comerciantilor sau a companiilor. Pe aceste pagini false, clientii își introduc datele cardului si/sau credentialele de autentificare în internet banking sau soldul disponibil existent pe card.

Dupa introducerea datelor bancare, clientii aproba tranzactiile prin autorizarea acestora pe canalele convenite cu banca. În acest mod, atacatorii obtin toate datele cardului si în cele mai multe cazuri folosesc aplicatii pentru transferul instant al banilor, iar bancile emitente nu pot stopa astfel de operatiuni.

Comunitatea bancara are o serie de recomandari pentru securitatea contului.

"Pentru a se proteja împotriva fraudelor, este necesar ca toti utilizatorii de carduri sa fie vigilenți si sa respecte urmatoarele recomandari: datele bancare sunt confidentiale si nu trebuie furnizate; nu furnizati niciodata datele cardului daca aveti produse de vânzare postate pe diferite site-uri sau aplicatii. Nu introduceti datele cardului pe paginile primite si nu le oferiti altor persoane. Cardul bancar are doar rolul de plata, niciodata de încasare. În cazul în care trebuie sa primiti bani, puteti trimite doar codul IBAN. Un mesaj cu cod de autorizare nu va veni niciodata

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 linkuri 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.)", se menționează în comunicat.

În cazul în care a fost achiziționat un produs de pe un site extern/intern și ulterior se primesc mesaje în care sunt solicitate datele de card pentru plata unor taxe de vamă sau de curierat trebuie luată 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 reținut 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. Pastrați întreaga corespondență purtată cu autorul fraudei și depuneți o sesizare la Poliția Română", se mai spune în comunicat.