

Protecția cardurilor bancare de fraude cibernetice



Pe parcursul sărbătorilor de iarnă, când numărul tranzacțiilor efectuate prin intermediul cardurilor bancare crește, utilizatorii acestora sunt expuși unor riscuri semnificative și trebuie să cunoască un șir de măsuri importante pentru protejarea datelor bancare, atât în lumea reală, cât și în cea virtuală.

Pentru protecția de unele fraude cibernetice în timpul tranzacțiilor efectuate prin intermediul cardurilor bancare, Ministerul Afacerilor Interne vine cu următoarele recomandări către cetățeni:

- la retragerea banilor de pe card de la un ATM, în special când sunteți peste hotarele țării sau în altă localitate, trebuie să utilizați un terminal situat în locuri publice, din zonele centrale sau comerciale ale orașului. Preferabil ar fi un terminal din incinta unor bănci sau la sediile acestora;
- asigurați-vă că terminalul ATM nu a fost modificat. Trebuie verificate vizual fanta de acces a cardului, ecranul și tastatura. Dacă se observă urme de lipici, crăpături în plastic, folii lipite peste tastatură sau orice alt semn suspect, utilizatorii sunt sfătuiți să întrerupă tranzacția și să anunțe poliția și banca;
- asigurați-vă că absolut nimeni nu vede codul PIN pe care îl introduceți. Iar pentru prevenirea situației de aflare a codului dumneavoastră PIN, cu ajutorul unor dispozitive video instalate ilegal, acoperiți cu cealaltă mână tastatura în timpul introducerii codului;
- activați notificarea prin SMS pentru orice plăți făcute din contul de card, dacă banca oferă acest serviciu;
- după concedii și vacanțe, verificați extrasul de cont, iar în cazul depistării unor tranzacții suspecte, anunțați imediat banca, dacă este cazul. Tranzacția poate fi refuzată, în cazul existenței unor motive întemeiate, iar banca este obligată să ajute utilizatorul să-și recupereze banii;
- nu scăpați din vedere cardul și asigurați-vă că semnați un singur bon de plată când efectuați plăți în magazin, restaurant, benzinărie, hotel etc. Deseori, fraudatorii strecoară sub chitanță o altă foaie cu indigo, pe care este trecută o sumă mai mare de

bani;

- nu păstrați codul PIN împreună cu cardul, scris pe hârtie sau în telefonul mobil. Cel mai bine ar fi să-l memorizați.

Odată cu creșterea accelerată a comerțului online, utilizatorii s-au obișnuit să folosească și alte servicii care acceptă plata cu cardul - de la rezervări de vacanțe, la asigurări de mașini sau achiziții de produse. Comercianții implementează mecanismele necesare pentru prevenirea furtului și fraudei, însă există și o serie de măsuri recomandate, care merită reținute:

- protejați-vă calculatorul prin instalarea cel puțin a unei soluții antivirus actualizat și a unui firewall. De asemenea, este foarte important ca sistemul de operare și programele utilizate să fie cu update-urile curente;

- nu utilizați pentru plăți online calculatoare virusate sau care aparțin altor persoane;

- fiți atenți la ofertele speciale, în special la ofertele-șoc, care promovează produse la prețuri exagerat de mici, comparativ cu majoritatea comercianților. Pagina respectivă poate fi un site de phishing;

- fiți atenți la site-urile accesate. Infractorii cibernetici obișnuiesc să copie design-ul unor site-uri cunoscute și să creeze pagini web false, utilizate pentru colectarea datelor bancare și a datelor de autentificare;

- fiți atenți la introducerea datelor personale. La procurarea unui produs online este necesară introducerea datelor bancare și adresei de livrare, însă majoritatea site-urilor false cer acest lucru chiar din momentul accesării acestora, lucru care este inutil și suspect. Evitați astfel de magazine online;

- efectuați cumpărături numai de pe paginile criptate. Criptarea este esențială pentru magazinele online, iar cele care o folosesc vor afișa în bara de adresă a browser-ului o conexiune de tip https („s”-ul vine de la „secured”, este o conexiune http securizată). Indicii ale unei conexiuni criptate pot fi simbolul în formă de lacăt sau afișarea barei de adresă cu o culoare diferită;

- folosiți pentru cumpărături online un card separat, cu o limită scăzută de credit. Dacă datele acestui card sunt compromise, paguba este mult mai mică decât în cazul în care fraudă ar fi afectat cardul de economii sau cel de salariu;

- utilizați parole complexe, formate din litere, cifre și caractere speciale. Parolele de tip „123456” nu vor fi niciodată utile. De asemenea, este recomandat să aveți parole unice pentru fiecare serviciu online - parolă separată pentru e-mail, parolă separată pentru rețele sociale, parolă separată pentru contul online banking.

Urmând aceste sfaturi, fraudele bancare pot fi cu succes evitate, mai ales în perioadele aglomerate ale anului, când foarte mulți oameni folosesc cardurile pentru diverse tranzacții.

Direcția informare și relații cu publicul,
9 ianuarie 2013