PREVENIREA FRAUDELOR ÎN MEDIUL ON-LINE

Internetul a devenit foarte atractiv pentru infractorii cibernetici. Autorii folosesc metode ingenioase și promisiuni în scopul de a obține bani sau informații financiare valoroase de la dumneavoastră.

Una dintre cele mai des folosite incidente de securitate cibernetică de tip fraudă este ***tentativa de fraudă pe platformele de vânzări online***.

Mecanismul utilizat de atacatori este unul dual, țintind atât cumpărătorii, cât și vânzătorii dintr-o platformă. Metoda de atac implică contactarea utilizatorilor și redirecționarea lor către alte soluții de tip chat, de regulă Whatsapp. Următorul pas este convingerea potențialei victime de a furniza datele de pe card, în urma accesării unui link nelegitim transmis de atacatori. Astfel, sunt obținute toate datele cardului, inclusiv parolele de securitate cu care efectuează o primă tranzacție de tip transfer (care va debita contul de card al vânzătorului), iar ulterior le utilizează pentru alte tranzacții frauduloase.

Persoanele care au postat anunțuri de vânzare pe site-uri sunt sfătuiți să nu comunice datele de pe card, acestea fiind confidențiale și folosite exclusiv pentru achiziții și nu pentru încasări.

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

- să nu comunice nimănui PIN-ul, datele înscrise pe card inclusiv codul CVV2/CVC2, date personale de identificare, orice alte informații de securitate aflate pe carduri sau parolele de securitate utilizate în tranzacționare; Angajații băncilor nu vor solicita niciodată divulgarea acestor informații indiferent prin ce mijloace se primește solicitarea - e-mail, SMS, apeluri telefonice sau la servicii financiare furnizate de bancă la distanță.
- să nu furnizeze niciodată datele de acces la Internet/Mobile Banking;
- datele înscrise pe card trebuie cunoscute exclusiv de titular și trebuie completate doar când acesta efectuează cumpărături online pe site-uri securizate;
- să nu deschidă atașamentele din e-mail-urile primite de la persoane necunoscute;
- să nu intre pe link-uri primite prin e-mail-uri necunoscute sau nesolicitate;
- să nu instaleze aplicații din surse necunoscute și programe necertificate descărcate de pe website-uri dubioase;
- să aibă instalat un program antivirus bun și actualizat și să actualizeze permanent sistemul de operare;

În situația în care este solicitată introducerea unor coduri suplimentare, să nu execute acest lucru și să anunțe imediat banca emitentă în cazul în care observa în browser următoarele:

- imagini suspecte care nu corespund cu cele din paginile web ale băncii,
- apariția unor ferestre „pop-up" care solicită introducerea de date confidențiale,
- că nu se pot autentifica în pagina de Login de la prima încercare, întrucât s-ar putea să devină victima unui atac informatic.

Sesizați Poliția la orice încercare de fraudă, chiar dacă nu ați devenit victima acesteia !