

Stimați clienți,

Vă reamintim că, pentru evitarea fraudelor prin instrumente electronice de plată, elementele de securitate personalizate - care sunt confidențiale - trebuie păstrate în condiții de siguranță, aceasta constituind și o obligație legală.

Pentru informarea dumneavoastră vă supunem atenției cel mai recent comunicat de presă al Băncii Naționale a României referitor la atenționarea utilizatorilor de servicii de plată cu privire la păstrarea în siguranță a elementelor de securitate personalizate ale instrumentelor de plată:

„BNR este autoritatea națională competentă, responsabilă cu urmărirea respectării de către prestatorii de servicii de plată a cerințelor operaționale și de securitate aplicabile serviciilor de plată. BNR monitorizează pe bază continuă evoluțiile din acest domeniu.

În ultima perioadă, pe fondul creșterii gradului de utilizare a mijloacelor moderne de plată în contextul digitalizării accelerate a economiei și a dezvoltării comerțului online, inclusiv ca urmare a restricțiilor sanitare și a contextului epidemiologic actual, a devenit tot mai preocupantă evoluția fraudelor prin instrumente electronice de tip card, internet banking sau mobile banking.

O mare parte a acestor fraude se bazează pe inginerii sociale (*phishing*), utilizatorii serviciilor de plată fiind manipulați de către atacatori și determinați, sub diverse pretexte înșelătoare, să le comunice acestora elementele de securitate ale instrumentelor de plată pe care le dețin (datele cardului, codurile PIN, codurile de activare ale aplicațiilor de internet/mobile banking, parole statice sau dinamice, coduri de înrolare ale cardurilor în aplicații de tip portofel electronic), ce sunt folosite ulterior pentru accesarea conturilor clienților și sustragerea fondurilor din conturile acestora.

BNR atrage atenția utilizatorilor de servicii de plată asupra faptului că elementele de securitate personalizate aferente instrumentelor de plată trebuie păstrate în condiții de siguranță, aceasta constituind și o obligație legală. Aceste elemente sunt confidențiale și nu sunt niciodată solicitate de către emitentul instrumentului de plată sau de către o altă autoritate prin e-mail, SMS sau printr-o pagină web. Divulgarea acestor informații poate permite unor potențiali atacatori să acceseze conturile și să inițieze operațiuni de plată frauduloase.

BNR recomandă tuturor utilizatorilor de servicii de plată să acorde o atenție sporită următoarelor aspecte:

- i. atunci când accesează aplicațiile bancare disponibile online, să se asigure că s-au conectat la paginile web oficiale ale băncilor, care utilizează conexiuni securizate de tip <https://> și să verifice că denumirea paginii web care apare în bara de adrese reflectă fără dubii denumirea băncii;
- ii. să citească cu atenție mesajele de alertă primite prin SMS de la bancă, în special cele prin care sunt transmise parole, coduri de acces ori de validare, pentru a înțelege natura operațiunii pe care urmează să o inițieze/autorizeze.

În cazul în care suspectează că sunt victime ale unor astfel de înșelătorii, utilizatorii serviciilor de plată trebuie să contacteze în cel mai scurt timp posibil instituția care a emis instrumentul de plată, pentru a primi asistența tehnică specifică în vederea limitării pe cât posibil a pierderilor și să sesizeze organele de cercetare penală despre incident.”

Dacă suspectați că sunteți victime ale unor înșelătorii, vă rugăm să ne contactați la:

E-mail: e-ximsuport@eximbank.ro

Telefon: 021.405.31.78 (L-V, orele 9.00-17.30)

Vă mulțumim!