

BNR: Daca titularul instrumentului de plata a transmis elementele de securitate personalizate unor terte persoane, prestatorul serviciilor nu poate fi obligat sa suporte eventualul prejudiciu

Banca Nationala a României atrage atentia utilizatorilor de servicii de plata ca elementele de securitate personalizate trebuie pastrate în conditii de siguranta, iar în cazul în care titularul instrumentului de plata a transmis elementele de securitate personalizate unor terte persoane acesta este în culpa în situatia producerii unei fraude, iar prestatorul serviciilor de plata nu poate fi obligat sa suporte eventualul prejudiciu.

"BNR, în exercitarea atributiilor legale ce îi revin, monitorizeaza în mod permanent evolutiile din domeniul platilor, urmarind respectarea de catre prestatorii de servicii de plata a cerintelor operationale si de securitate aferente serviciilor de plata. În acest sens, banca centrala a emis în decembrie 2021 un comunicat prin care a avertizat utilizatorii serviciilor de plata cu privire la fraudele ce se bazeaza pe inginerii sociale (phishing) si la necesitatea pastrarii în conditii de siguranta a elementelor de securitate aferente instrumentelor de plata", se spune în comunicat.

Institutia mentioneaza ca în ultima perioada au fost observate noi tipologii/scenarii de fraude prin manipularea platitorului, care vizeaza instrumentele de plata de tip card, internet banking sau mobile banking. În cele mai multe cazuri, utilizatorii serviciilor de plata sunt indusi în eroare de catre atacatori si, sub diverse pretexte înșelatoare - de exemplu necesitatea de actualizare a datelor personale, notificarea privind blocarea conturilor sau a instrumentelor de plata, obtinerea de informatii legate de carduri de catre falsi cumparatori de bunuri sau servicii postate pe platformele de anunturi online - sunt convinsi sa divulge elemente de securitate personalizate ale instrumentelor de plata pe care le detin, informatii ce sunt folosite ulterior pentru accesarea conturilor victimelor si sustragerea fondurilor acestora.

În acest context, BNR atrage din nou atentia utilizatorilor de servicii de plata asupra faptului ca elementele de securitate personalizate aferente instrumentelor de plata (datele cardului, codul PIN, codul CVV/CVC, codurile de activare ale aplicatiilor de internet/mobile banking, parolele statice sau dinamice, codurile de înrolare ale cardurilor în aplicatii de tip portofel electronic) reprezinta informatii care, potrivit legii, trebuie pastrate în conditii de siguranta. Aceste informatii au caracter confidential si nu sunt niciodata solicitate de catre emitentul instrumentului de plata sau de catre o alta autoritate.

Conform BNR, divulgarea acestor informatii catre terte persoane, inclusiv prin accesarea unor site-uri de internet false, care imita din punct de vedere vizual pagina oficiala a bancilor emitente a instrumentelor de plata sau a unor institutii si autoritati, reprezinta cel mai important factor de risc care permite atacatorilor sa acceseze conturile victimelor, iar ulterior sa initieze operatiuni de plata frauduloase.

De asemenea, banca centrala precizeaza ca, potrivit prevederilor legale în vigoare, în cazul în care titularul instrumentului de plata a transmis elementele de securitate personalizate unor terte persoane si, ca atare, nu si-a îndeplinit obligatia de a pastra în siguranta a informatiilor respective, acesta este în culpa în situatia producerii unei fraude, iar prestatorul serviciilor de plata nu poate fi obligat sa suporte eventualul prejudiciu.