

Poliția Atenționează! A fost depistat un nou tip de fraudă telefonică ce vizează aplicațiile bancare.



Centrul pentru combaterea crimelor cibernetice al INI, #avertizează populația despre apariția unei noi metode de înșelăciune, prin care infractorii obțin acces de la distanță la telefoanele mobile și la aplicațiile bancare instalate pe acestea.

Cum acționează infractorii?

Victimele sunt contactate telefonic de persoane necunoscute care se prezintă drept „angajați ai companiilor de telecomunicații” și, sub pretextul acordării de asistență tehnică, le cer să instaleze o versiune „actualizată” a aplicației operatorului, primită prin link transmis prin SMS, e-mail sau aplicații de mesagerie (WhatsApp, Viber, Telegram etc.).

Odată accesat linkul, pe dispozitivul mobil se instalează o aplicație suplimentară, aparent legitimă, dar care conține funcții ascunse de control la distanță.

Menținem că infractorii folosesc un ton profesionist și invocă motive tehnice credibile cum ar fi „necesitatea actualizării urgente a aplicației operatorului în vederea evitării întreruperii serviciului”.

Ce se întâmplă după instalare?

Pe ecran apare mesajul „**Actualizare în curs**” sau dispozitivul se blochează complet. Infractorii obțin acces la aplicația de mobile banking a victimei, dezactivează notificările privind tranzacțiile și efectuează transferuri repetate de bani către mai multe conturi și carduri bancare, pentru a ascunde traseul sumelor și a îngreuna recuperarea acestora. Operațiunile se fac rapid, de obicei în afara orelor de lucru ale băncilor, pentru a întârzia reacția instituțiilor.

În cele mai multe cazuri, victimele pierd sume considerabile în doar câteva minute, fără a observa tranzacțiile în timp real, din cauza blocării notificărilor.

Reamintim: Niciun operator de telefonie mobilă, bancă sau instituție oficială a statului, nu solicită reinstalarea aplicațiilor prin apel telefonic și nu transmite linkuri neautentificate pentru actualizări. Orice solicitare de acest tip trebuie tratată cu suspiciune și verificată prin canalele oficiale ale instituțiilor.

Recomandările poliției:

Verificați identitatea apelantului, contactând direct compania de telecomunicații prin numerele afișate pe site-ul oficial.

Nu instalați aplicații la cererea unor persoane necunoscute, indiferent de calitatea invocată.

Nu accesați linkuri primite prin canale nesigure sau neverificate.

Activați autentificarea în doi pași pentru aplicațiile bancare.

Monitorizați constant conturile și setați alerte pentru tranzacții (e-mail, notificări push).

IMPORTANT:

Dacă ați instalat o astfel de aplicație sau ați furnizat date, contactați imediat Poliția, operatorul de telefonie mobilă și banca la care aveți conturi.

14 august 2025