

Itt a banki csalások toplistája, új módszerrel verik át az ügyfeleket

Milliárdokat buktak a magyar ügyfelek a bankkártyákkal vagy átutalásokkal megvalósított csalásokon, amelyeknek a száma még nőtt is. A lakossági ügyfelek kára ugyan nem nagyobb, mint korábban, de a céges számlák megcsapolásával okozott veszteség meredeken növekedett. A BiztosDöntés.hu kibervédelmi szakemberekkel összeállította a csalások toplistáját, amelyek között egy új módszer is megjelent, az NFC-s visszaélés.

A Magyar Nemzeti Bank adatai szerint 2026 második negyedévében hozzávetőleg 52 ezer sikeres visszaélés történt a bankkártyás fizetési forgalomban, ami 8 százalékkal több az előző negyedévinél. Az okozott kár értéke viszont gyakorlatilag megegyező volt azzal, 1,74 milliárd forintot tett ki. A végül leírt, 1,38 milliárd forintnyi veszteség 66 százalékát a kártyabirtokosok viselték.

Az átutalási forgalomban 3839 sikeres visszaélést regisztráltak a pénzügyi szolgáltatók, ami 8,4 százalékos növekedést jelent. Az okozott kár értéke viszont már 28 százalékkal 5,37 milliárd forintra emelkedett. Új jelenség, hogy a növekedés ezúttal teljes egészében a vállalati számlás visszaélésekből jött. Itt a csalások száma és összértéke is több mint duplájára ugrott egyetlen negyedév alatt, utóbbi így megközelítette a 2,9 milliárd forintot. Ezzel szemben a lakossági ügyfeleknél a [bankszámlás](#) átutalásokat érintő visszaélések összértéke több mint 400 millió forinttal csökkent, 2,4 milliárd forintot tett ki. Az átutalási forgalomban történt csalások esetében leírt kárt szinte teljes egészében az ügyfelek viselték.

Ez a pénzügyi átverések slágerlistája

A BiztosDöntés.hu az Erste kibervédelmi szakembereivel összesítette, milyen módszerek a legelterjedtebbek jelenleg, mire kell különösen figyelni az ügyfeleknek, ha nem akarnak áldozattá válni.

1. Hivatalos személyek nevében elkövetett csalások
2. Befektetési csalások
3. Online piactér
4. SMS adathalászat
5. Túl szép, hogy igaz legyen
6. Örökléses, romantikus csalások
7. NFC-s csalások

Az egyik leggyakoribb forgatókönyv, amikor a csaló **hivatalos személynek** adja ki magát. Banki ügyintézőként, rendőrként vagy a Magyar Nemzeti Bank (MNB) munkatársaként telefonál, és arra hivatkozva, hogy a számlát támadás érte, gyors cselekvésre sűrgeti a számla tulajdonosát. A cél ilyenkor az, hogy a megijedt ügyfél maga utalja át a pénzét egy „biztonsági számlára”. Vagy az, hogy egy letöltött alkalmazással hozzáférést szerezve az online banki felületre, a csaló maga hajtson végre átutalásokat, amelyekhez a kódokat „törlés” címszó alatt elkérve hitelesítse is azokat. Fontos tudni, hogy sem a bank, sem a rendőrség, sem a jegybank nem kér telefonon jelszót vagy kódot, nem kéri alkalmazás telepítését, és senkit nem utasít arra, hogy máshová mentse a megtakarításait.

Szintén sokakat károsítanak meg **befektetési csalásokkal**, amelyek jellemzően Facebook-hirdetésekből indulnak. Ismert közszereplők arcával, hamis cikkekkel és garantált, irreálisan magas hozammal csalogatnak. Aki pedig megadja az elérhetőségét, azt egy „befektetési tanácsadó” hívja vissza, és először kisebb, majd egyre nagyobb összegek befizetésére veszi rá. Illetve ebben az esetben is fontos szerepe lehet egy távoli elérést biztosító alkalmazásnak.

Az **online piactereken** már nem csak a vevőket, hanem egyre inkább az eladókat is célba veszik, és az Erste tapasztalatai szerint ezek az esetek jóval súlyosabb károkkal járnak. A csaló vevőnek adja ki magát, és jellemzően futárszolgálatra hivatkozva küld egy linket, ahol a vételár fogadásához kellene belépni online banki felületére, de a linken kapott bankválasztós oldalról. A cél természetesen a felületre történő belépés elérése, hiszen a pénz fogadásához elegendő lenne a bankszámlaszám és kedvezményezett nevének közlése. A szakemberek szerint ráadásul most kezdődik a piacteres csalások szezonja, hiszen közeleg a Black Friday és az ünnepi vásárlások ideje.

Továbbra is elterjedt az **SMS-es adathalászat**: a csalók közüzemi szolgáltatók vagy streaming platformok nevében küldenek üzenetet elmaradt számláról, lejárt előfizetésről, majd egy hamis oldalra terelve szerzik meg a kártyaadatokat.

Egy újabb nagy csoportot a „túl szép, hogy igaz legyen” ajánlatok adják. Ide tartoznak a népszerű márkák oldalait megszólalásig utánzó, feltűnően olcsó termékeket kínáló hamis webáruházak. A **nem létező szálláshelyek**, amelyekre előleget kérnek.

Meglepően gyakoriak a **romantikus csalások** is, amelyekben a csaló hetekig, hónapokig építi a kapcsolatot csodás közös jövő ígéretével kecsegtetve, hogy aztán „áldozata” egy váratlan élethelyzetre, vagy a közös fészek megteremtésére hivatkozva szinte minden vagyonát képes elutalni.

Az Erste szakemberei szerint egyre gyakrabban bukkan fel az **örökléses csalás** is. Ilyenkor egy magát ügyvédnek, közjegyzőnek vagy banki ügyintézőnek kiadó csaló (e-mailben, de akár Messengeren vagy Viberen) arról értesíti a kiszemelt áldozatot, hogy egy távoli, gyakran külföldi rokona után jelentős vagyont örökölt. Ahhoz, hogy hozzájusson a busás örökséghez, előbb illetéket, közjegyzői vagy ügyvédi díjat kell fizetnie. Sokszor nem is csak a pénz a cél, hanem a személyes és banki adatok megszerzése, a módszer legcinikusabb változatában pedig valódi haláleset után a gyászoló hozzátartozókat keresik meg.

Kifinomult új módszer terjedésére figyelmeztetnek a szakértők

A legújabb, gyorsan terjedő módszerben a csalók a **telefon érintéses (NFC) funkcióját** használják ki. Önmagában az, hogy a bankkártyát a mobilhoz érintjük, nem veszélyes, ahogy az érintéses fizetés sem az. A gond akkor van, ha a telefonon már fut egy csaló alkalmazás, amely az érintéssel beolvasott kártyaadatokat azonnal továbbítja a bűnözőknek – figyelmeztet Kósa Anna, az Erste Compliance vezetője.

A forgatókönyv jellemzően egy telefonhívással indul, amelyben nyeremény, jóváírás vagy egy befektetés hozamának kifizetését ígérik. Ehhez le kell tölteni egy alkalmazást, amellyel a csalók hozzáférést szereznek a telefonhoz, a beszélgetés alatt pedig a háttérben, az áldozat tudta nélkül egy újabb appot telepítenek. Az app és a kártya érintése együttesen lehetővé teszi a kártya adatainak továbbítását. Egy átadott PIN-kóddal és a kártya limitjének megemelésével pedig készpénz-felvételt, illetve magas összegű vásárlást is „megengednek” a csalóknak. A módszer különösen alattomos, mert a bankkártya végig az ügyfélnél van, és sokáig semmi nem utal arra, hogy illetéktelenek használják.

Kósa Anna szerint a legfontosabb szabály, hogy ismeretlen kérésére soha nem szabad alkalmazást letölteni, akkor sem, ha nyereményt vagy bármilyen kifizetést ígér. A bankkártyát sem érdemes más utasítására a telefonhoz érinteni, a PIN-kódot senkinek nem szabad megadni, és a kártyalimitet sem szabad idegen kérésére megemelni. Legyünk tisztában azzal, hogy a PIN kód és a limit a kimenő összeget korlátozzák. Ha egy hívásban szóba kerül valamilyen alkalmazás letöltése, a legjobb azonnal bontani a vonalat, és felhívni a bankot a kártya hátoldalán vagy a hivatalos honlapon található számon. Ha pedig már megtörtént a baj, minden perc számít. Érdemes rendőrségi feljelentést is tenni, és azt a bankhoz is eljuttatni, mert segíti a vizsgálatot.