# Egyre több a visszaélés - Így használja biztonságosan a bankkártyáját

**Az elmúlt hónapokban nagy nyilvánosságot kaptak azok a bűncselekmények, melyek során bankkártya-adatokkal éltek vissza, esetenként több százezer forintos kárt okozva a vétlen ügyfeleknek. A legtöbb visszaélés kis odafigyeléssel megelőzhető, legalábbis vannak olyan praktikák, amelyekkel jelentősen növelhetjük kártyánk védelmét.**

Elmondjuk, hogy milyen módszerekkel élnek a bűnözők, mit érdemes tudni a kártyabiztonságról, a tudatos felhasználói magatartásról.

A Magyar Nemzeti bank (MNB) statisztikái szerint három területen a leggyakoribbak a visszaélések: a készpénzfelvétel, a bankkártyás fizetés, a harmadik pedig az "egyéb típusú terminálon elkövetett visszaélés", ami gyakorlatilag az online vásárlást jelenti. Fejes Kálmán a MasterCard Europe kártyabiztonsági szakértője szerint hazánk meglepően jól áll a bankkártyák biztonságának szempontjából. Az MNB adataiból azt lehet kiolvasni, hogy az elmúlt néhány évben abszolút értékben, kis mértékben ugyan növekedtek a visszaélésszámok, viszont arányaiban ezek nem mutatnak különösebb változást - véli a MasterCard szakértője.

A magyar statisztikák Európához és a világhoz viszonyítva sokkal kedvezőbbek, arányaiban ötöde, hatoda annak a visszaélés-mennyiségnek, mint amit globálisan, illetve az EU-ban regisztrálunk. A szakértő szerint a magyar bankok komoly lépéseket tettek a kártyabiztonság fejlesztése érdekében. Az egyik fontos eszköz az SMS értesítő a kártyás tranzakciók után, a másik az a kifinomult kártyás műveleteket ellenőrző monitoring-rendszer, mely segítségével a bankok nagy pontossággal szűrik ki a gyanús tranzakciókat.

"Az 1990-es évek elején, amikor még nem volt mindenkinek mobiltelefonja, az SMS értesítő egy elég érdekes, unikális megoldás volt - mondta el a MasterCard szakértője, - ma már viszont több mobil van a piacon, mint bankkártya, és ez minden ügyfél számára elérhető."

A magyar kártyabiztonság javulása ezzel a szolgáltatással kezdődött, az újítás minden banknál elterjedt, és az ügyfelek nagy része él is ezzel a lehetőséggel. Az SMS-es tranzakció-értesítő azért jó biztonsági megoldás, mert az ügyfél az, aki a leghamarabb tudja érzékelni az esetleges visszaélést. Természetesen ezzel együttműködve dolgozik a banki monitoring rendszer, amely küld különböző felszólításokat arról, hogy valamely tranzakció gyanús, le kell ellenőrizni. Ha az ügyfél meg tudja

mondani, hogy ez a tranzakció nem tőle származik a kártyát a lehető leghamarabb letiltják, a tranzakciót kivizsgálják, és megkezdődik az ügyfél kártalanítása.

**A chipesítés sokat segített**

A magyar helyzet látványos javulásán nagyon sokat segített az a nemzetközi, a chip bevezetését előíró szabály, amit a nemzetközi kártyatársaságok a kétezres évek közepén írtak elő a bankok számára. 2011-től már nem lehet olyan kártyát kibocsátani, amelyiken nincs chip, a forgalomban lévő kártyákat pedig záros határidőn belül le kell cserélni.

"Nem mondom, hogy a chip mindenre megoldást adna, de a chipes kártyák másolása gyakorlatilag nem lehetséges, a chipadatok még egyszer nem használhatók fel egy újabb tranzakcióra. A chipen történt műveletek jóval magasabb biztonságot képviselnek, mint a korábbi technológia, a mágnes csík" - mondta el Fejes Kálmán.

A chip mellett ugyanakkor még mindig, az új kártyákon is helyet kap a mágnes csík. Ennek az az oka, hogy a chipesítés Európában indult el, és itt meg is történt, mind az eszközök, mind a kártyák migrációja a chipre. A kártyatársaságoknak viszont az a célja, hogy globális felhasználási lehetőséget biztosítsanak az ügyfelek számára. Ha valaki más régióból Európába jön, és itt akarja használni a kártyáját, akkor tudja a mágnes csíkos technológiát továbbra is használni, illetve ha az európai ügyfelek szeretnének más régióban fizetni, pénzt felvenni, azt másképp egyelőre nem tudják megtenni, mint mágnescsík-alapon. "Természetesen a többi régió is próbál felzárkózni, a világ nagy részében elfogadták a chipesítést, látják ennek az előnyeit. Kanada, Dél-Amerika, Afrika, a Távol-Kelet számos országa komoly lépéseket tett már a chipesítés irányába, de globálisan még nem tartunk azon a szinten, hogy megoldható lenne, hogy a mágnes csíkot ne szerepeltessük a kártyán."

**Az ügyfelek nagyon sokat tehetnek a tranzakció biztonsága érdekében**

A kártyabiztonsági szakértő nagyon fontosnak tartja, hogy az ügyfelek megfelelő tájékozottsággal rendelkezzenek a biztonságos bankkártya-használatról, és ami rajtuk múlik, azt tegyék meg.

"Kezdjük az ATM-es készpénzfelvétellel, mert ez az egyik legrégebbi tranzakciótípus, és az egyik leggyakoribb. Ha egy ügyfél ATM-et használ, mindenképpen érdemes odafigyelnie arra, hogy lehetőség szerint olyan automatánál vegyen fel készpénzt, amit rendszeresen szokott használni. Ha lehetőségünk van rá, használjuk azt, amiről tudjuk, hogyan néz ki, észre tudjuk venni az esetleges változtatásokat, módosításokat. Nagyon fontos, hogy ismerjük az ATM fizikai megjelenését, olyan ATM-et használjunk, amely valamilyen biztonsági környezetben van. Óriási a különbség biztonság szempontjából egy elhagyatott, sötét külvárosi, és egy plázában lévő ATM között - én szakemberként természetesen az utóbbit preferálom. A készpénzfelvételnél vannak olyan alapvető szabályok, amelyeket érdemes betartani: fontos, hogy a PIN kód megadásakor takarjuk el a kezünkkel a klaviatúrát. Ha bármilyen eszköz fel van szerelve az automatára, ami a kártyaadatok megszerzésére irányul, akkor az egyik fontos mozzanat az, hogy megszerezzék a PIN kódot is - ezt általában valamilyen kamerával kísérlik meg elérni. Ezt nagyon jól ki tudjuk védeni, ha a kód megadásakor eltakarjuk egyik kezünkkel a másikat. Ha ezt a minimumot betartják az ügyfelek, már nagyon sokat tettek annak érdekében, hogy a kártyájuk biztonságban maradjon.

Nagyon fontos, hogy figyeljünk oda, ne együnk hamburgert, ne telefonáljuk miközben készpénz veszünk föl az automatából. Előfordul, hogy a bűnözők megfigyelik azt az embert, aki szétszórt a tranzakció lebonyolítása közben: egyik kezében egy táska, a másikkal telefonál, közben beüti a PIN kódot - ez szinte a legjobb terep ahhoz, hogy egy kártyabirtokost megtévesszünk. Létező módszer az is, hogy az ügyfélnek szólnak, hogy leejtett valamit, miközben az ATM éppen adja vissza a kártyáját

vagy adja ki a pénzt. Elég egy pillantást vetni a földre, hogy tényleg van-e ott valami, esetleg fel is venni azt a bankjegyet, amit ők tettek oda, és közben egy harmadik ember elszalad a kártyával vagy a pénzzel. Ugyanakkor abban a pillanatban, amikor az ügyfél már készpénzzel rendelkezik, egy újabb támadási felületet nyit - kifigyelhetik, kirabolhatják. Többek között ezért a legjobb a kártyát inkább vásárlásra használni, mint készpénz felvételre."

A megkérdezett szakértők szerint az egyik fontos eszköz, amit az ATM használónak keresni érdemes az egy, a mágnes csík adatainak megszerzésére irányuló szerkezet. Ezeket az adatokat annál a pontnál kell megszereznie a bűnözőknek, amelyen keresztül a kártya bejut az ATM-be, tehát az ilyen jellegű eszközök a kártyanyílás közelében fordulhatnak elő. A mai kor technológiája már lehetővé teszi, hogy ezek az eszközök nagyon aprók szinte észrevehetetlenek legyenek. A bankok azonban mindent megtesznek annak érdekében, hogy olyan ellenlépéseket alakítsanak ki az ATM-eken, hogy ilyen eszközök felszerelését nagyban megnehezítsék, illetve ellehetetlenítsék. Hasonló eszközökkel találkoztunk a közelmúltban, amikor magyar bankkártyák adataival Chicagóban, majd Chilében vásároltak, vettek fel készpénzt. A bűnelkövetés módja abból fakad, hogy a mágnes csík, amelyről megszerezték az adatokat, olyan, mint egy magnószalag: leolvasni róla az adatot és ráírni egy másik kártyára nem jelent különösebb problémát.

Fejes Kálmán szerint ezekben az ügyekben nem volt különösebb újdonság, csak most jobban ismertté vált a média és az ügyfelek számára ez az esemény, ilyen jellegű bűncselekmény korábban is előfordult. Fontos kiemelni, hogy a banki monitor rendszer és az ügyfeleknek küldött SMS nagyon rövid idő alatt kiszűri ezeket a tranzakciókat, az ügyfelet pedig rövid vizsgálat után teljes mértékben kártalanítja a bank.

A chipes kártyával viszont nem lehet véghez vinni hasonló típusú visszaélést - mondja a MasterCard szakértője, - ilyen kísérlettel még egyáltalán nem találkoztunk. Ez teljesen más technológia, teljesen más biztonsági szintet képvisel. Úgy tűnik az Achilles-sarka a dolognak pillanatnyilag a mágnescsík, és ameddig ennek helyet kell kapnia a kártyán, addig a bankok és a kártyatársaságok kénytelenek speciális védelmi rendszereket bevezetni az ATM-eken, hogy az esetleges másolásokat, ha lehet, megelőzzük mindig egy lépéssel előrébb járva a bűnelkövetőknél.

A bolti vásárlás során ugyanakkor még ennél is ritkábban kerülnek illetéktelen kézbe bankkártya-adatok, de - figyelmeztet Fejes Kálmán - a vásárlásnál is nagyon fontos, hogy védjük PIN kódunkat. Ezért fontos hangsúlyozni, hogy lehetőleg takarjuk el a PIN padet, azaz a numerikus billentyűzetet, amikor az üzletben megadjuk a kódot. A szakértő szerint ugyanakkor nem lehet eléggé kiemelni, hogy a kártyás vásárlás sokkal biztonságosabb, mint a készpénzfelvétel, tehát mindenkit arra bátorít, hogy elsősorban vásárlásra használja a kártyáját, már csak azért is, mert ez költségmentes.

Forrás: Pozitív Híradó