



Százmilliók nyomában: akcióban a hamiskártyások



540 millió forint. Ennyi kárt okoztak a bankkártya-hamisítók, hackerek és más, bankkártyákkal visszaélő bűnözők az elmúlt évben az ártatlan áldozatoknak és ezáltal a bankoknak hazánkban a Magyar Nemzeti Bank adatai szerint. Az összeg nem csekély, és ráadásul egyre többet hallani ezekről a visszaélésekről - a hamisítók, csalók nem riadnak vissza a legvetemültebb módszerektől sem.

Ki ne hallott volna már ismerősétől, rokonától olyan esetet, amikor a kártyán lévő mágnes csíkot lemásolják és aztán az érintett egyszer csak arról kap értesítést, hogy külföldön vásárolt vagy pénzt vett ki. Ebben az esetben még az a szerencsésebb, aki erről a - fizetős - sms-szolgáltatás révén szerez tudomást, mivel így azonnal intézkedhet.

Az adatok megszerzését követően ráadásul általában azonnal lecsapnak a bűnözők, de előfordul, hogy a nyomozás megnehezítése miatt akár hónapokat is kivárnak.

Hatalmas összegeket kasszíroznak csalással

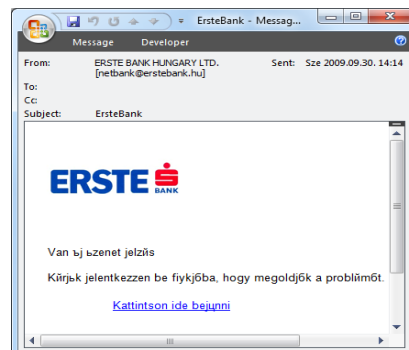
A legnagyobb értékben (263,33 millió) hamisított kártyákkal szereztek pénzt a csalók, ezt követi (136,76 millió) a levél, telefon, vagy internet útján ellopott (136,76 millió), majd az elvesztett, ellopott kártyákkal okozott kár összege (124,433 millió forint). Ezekhez képest elenyészően kevés problémát okoztak egyéb technikákkal - mindössze 15 millió forintot loptak el más módszerekkel.



Érdemes tehát megvédeni magunkat, illetve a bankszámlánkon lévő pénzt, amelyhez elengedhetetlen ismerni a leggyakoribb technikákat.

Sokszor előforduló csalásfajta, amikor telefon vagy email útján - általában egy pénzintézet nevében - a kártyánk adatait vagy PIN kódunkat, esetleg a számlánkhöz köthető más hozzáférési adatunkat kérik tőlünk. Fontos tudni, hogy a PIN kódot a bankok valójában nem kérik, kérhetik tőlünk (kivéve ATM-nél vagy POS terminálnál), így óvakodjunk ennek megadásától. A többi adat esetében is feltétlenül győződjünk meg arról, hogy valóban a bankunkkal kerülünk-e kapcsolatba, például visszahívás vagy a szám tudakozónál történő leellenőrzése által.

Legyünk rendkívül elővigyázatosak akkor is, ha olyan e-mailt kapunk, amelynél a levélben lévő linkre kell kattintani ahhoz, hogy elérjük internetbankunkat. Ebben az esetben egy eredetinek tűnő banki oldalra navigálnak bennünket, ahol adataink megadása után az oldal kijelzi, hogy az internetbank éppen nem működik. Ekkorra azonban a csalók már megszerezték a számukra fontos információkat.



Mágnescsík - a sebezhető pont

ATM termináloknál is legyünk résen, hiszen a bejutáskor az ajtó kinyitásához sokszor szükségünk van kártyánk használatára. Ide azonban egyre többször helyeznek fel a tolvajok egy olyan másolóeszközt, amellyel megszerzik a kártyaklónozáshoz szükséges mágnescsík-adatokat. Hordjunk tehát magunknál régi, lejárt kártyánkat, vagy egy bármilyen, jelentéktelen - mágnes csíkkal rendelkező - plasztik lapot, és csakis azzal nyissuk ki az ajtót!



Ezzel szorosan összefügg az, amikor egy kis kamerát szerelnek fel az ATM-re, amelyet a billentyűzetre irányítva ismerik meg PIN kódunkat. Bármikor, amikor ezt a kódot megadjuk (akár a boltban is vásárláskor), mindig takarjuk el másik kezünkkel a billentyűzetet. Érdemes tudni azt is, hogy az automatánál lévő kamera csak az arcunkat rögzítheti, nem pásztázhatja a billentyűzetet.

Ugyancsak bank automatáknál fordulhat elő az is, amikor az ATM pénzkidó nyílását leraasztják, amely így megakadályozza, hogy kijöjjön a bankjegy, sőt azt is, hogy az automata visszahúzza azt. Ilyenkor semmiképpen se hagyjuk el a helyszínt, még akkor sem, ha látszólag segítőkész emberek jelennek meg hirtelen. Hasonló helyzetbe kerülhetünk, ha a bűnözők egy nagyon apró leolvasót helyeznek el a kártyabeolvasó nyílásánál, amely a mágnescsík adatait rögzíti. Ezek kivédéséhez mindig nézzük meg az ATM-et, és ha a nyílások körül szokatlan dolgot tapasztalunk, inkább válasszunk másik automatát.



Legyünk gyanakvóak!



A klónozás többféle formáját alkalmazhatják a csalók bankkártyás fizetéskor. Ilyenkor előfordul, hogy többször húzzák le a kártyát vagy egy kis szerkezettel tárolják a mágnescsík adatait, esetleg a POS-t alakítják át úgy, hogy az megjegyyezze kártyánk számát és a PIN kódot. Bár ez utóbbi kettőt igencsak nehéz kiszűrni, alapszabály a védekezésben, hogy kártyánkat sose veszítsük szem

BÁCS-KISKUN MEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNMEGELŐZÉSI OSZTÁLY
KECSKEMÉT



elől, és ha bármi gyanúsítást észlelünk, azonnal válasszunk más megoldást!

A kártyacsалók mindig újabb és újabb trükköket eszelnek ki, azonban kellő körültekintéssel, gyanakvással, a számlánkon lévő összeg napra pontos nyilvántartásával, az sms-szolgáltatással, valamint a legújabb dombornyomott kártyák használatával csökkenthető az esélye, hogy áldozattá váljunk.

Ha viszont mégis jogtalanul vesznek le pénzt csalók a kártyánkról, akkor a bank - beépítve a banki költségekbe - megtéríti kárunkat, majd kivizsgálja az ügyet, ellenőrizve, hogy nem mi fizettünk-e mégis az említett tranzakciónál. Sőt, olyan is előfordul, hogy maga a pénzügyintézet jelzi az ügyfélnek, hogy letiltotta kártyáját, mivel ahol korábban használta, ott több gyanús esetet is vizsgálnak. Az ilyenkor felmerülő átmeneti kellemetlenségeknél gondoljunk arra, hogy rosszabbul is járhattunk volna, ha a bűnözők megszabadítanak bennünket számlánk tartalmától.

A bankok mindent megtesznek azért, hogy kivédjék a csalásokat, de fontos, hogy mi is minden kártyahasználatnál óvatosak, körültekintőek legyünk.

Bács-Kiskun Megyei Rendőr-főkapitányság
Bűnmegelőzési Osztály

BÁCS-KISKUN MEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNMEGELŐZÉSI OSZTÁLY
K E C S K E M É T

6000 Kecskemét, Batthyány u. 14., Postacím: 6001 Kecskemét, Pf.:302 Tel:76/513-300/30-27, BM: 33/30-27, Fax: 76/513-300/30-98 BM 33/30-98, e-mail: elbir@bacs.police.hu