



**ELEKTRONIKUS LAKOSSÁGI BŰNMEGELŐZÉSI
INFORMÁCIÓS RENDSZER**
Polgármesteri Hírlevél
2010. május

**Bankkártyával kapcsolatos bűncselekmények
és azok megelőzése**

A technika fejlődésével széles körben elterjedtek a készpénz-helyettesítő eszközök, vagyis a bankkártyák. Ebben közrejátszott az, hogy használatuk kényelmes, nem szükséges nagyobb mennyiségű készpénzt magunkkal hordani, viszont amikor szükségünk van rá, el tudjuk érni a bankszámlánkon lévő összeget. Alapvetően tehát a bankkártyák jelentősen megkönnyítik az életünket. A bűnözők azonban felismerték a lehetőséget, és ezért a kártyabirtokosoknak is meg kell tenniük bizonyos óvintézkedéseket.

A bankkártya használat során, a bankkártyán digitálisan tárolt adatokkal azonosítják a kapcsolódó számlát, majd a központ a tranzakcióval együtt ellenőrzi a megadott PIN-kódot is. A rendszer csak akkor hagyja jóvá a tranzakciót, ha a PIN-kód helyes. Nem minden bank dombornyomott kártyájának használatához szükséges PIN kód; ilyenkor a tulajdonos aláírásával igazolja jogosultságát.

Hogyan juthat bankkártyánk illetéktelen személyhez, ill. milyen módszerekkel szerezhetik meg a bankkártyánkat és a hozzá kapcsolódó azonosító adatokat? Ez megtörténhet úgy, hogy elveszítjük vagy ellopják tőlünk. Ezért az egyik legfontosabb dolog, hogy a PIN kód soha ne legyen a bankkártya mellett, és soha ne legyen arra ráírva. A másik fontos és általános tanács, hogy a bankkal állítsunk be egy napi limitet a számlán történő pénzmozgást illetően, így elkerülhetjük, hogy a tolvajok és csalók nagyobb összeget emeljenek le számlánkról.

A kártya adatainak és a PIN kód megszerzésének további módszerei, amikor az elkövetők bankjegykiadó automatáknál (ATM), vásárlások során kártyaelfogadó helyeken, internetes vásárlás, adathalászat során kísérleteznek.

Az ATM használat veszélyei, biztonságos használata

Az ATM-knél is többféle módszert alkalmaznak az elkövetők a kártyaadatok megszerzésére. Az egyik, amikor a kártyabefogadó nyílás elé felszerelnek egy leolvasó berendezést, mely a kártya behelyezése során rögzíti annak adatait. A tranzakcióhoz szükséges PIN kódot egy alkalmas helyre felszerelt és álcázott kamerával, vagy a billentyűzetre tett vékony, átlátszó fólia segítségével szerzik meg. Ehhez hasonló a zárt térben levő ATM-hez való bejutást engedélyező, ajtóra szerelt kártyaolvasó berendezés manipulálása is.

Másik módszer az ún. „Libanoni hurok” alkalmazása. Ennek során a kártyafogadó nyílásba helyezett egyszerű szerkezet segítségével megakadályozzák, hogy az ATM a sikertelen pénzkivétel után visszaadja a kártyát. A közelben várakozó elkövető ekkor felajánlja „segítségét” és a PIN kód újbóli beütésére ad tanácsot, miközben leolvassa azt. Természetesen így sem tudunk készpénzt kivenni, az elkövető viszont hozzájutott bankkártyánkhoz, a PIN-kódunkhoz és a számlán levő pénzünkhöz is.

Bár nem egyszerű felismerni az elkövetők által az automatákra felszerelt eszközöket, berendezéseket, minden pénzkivétel előtt ellenőrizzük a kártyafogadó nyílást, a pénzkivétel nyílást, esetleges billentyűzetre irányuló kamera elhelyezését. Amennyiben nem ítéljük biztonságosnak, válasszunk egy másik ATM-t.

Beltéri automata használata esetén próbáljuk elkerülni, hogy velünk együtt mások is a helyiségben tartózkodjanak. Ne hagyjuk, hogy készpénzfelvétel végrehajtása közben idegenek megzavarjanak minket, vagy eltereljék a figyelmünket, a „segítség” felajánlótól pedig óvakodjunk.

A PIN kód beütésekor el kell takarni a billentyűzetet, meg kell bizonyosodnunk róla, hogy az utánunk sorban állók ne láthassák azt, illetve az általunk felvenni kívánt összeget. Amennyiben a tranzakció közben bármi gyanúsat észlelünk, inkább töröljük a tranzakciót és hagyjuk el a helyszínt. A készpénzfelvétel befejezését követően ne kezdjük el az ATM előtt állva számolni pénzt, inkább mielőbb tegyük el a kártyát és a készpénzt. Lehetőleg ne kérjünk bizonylatot a tranzakcióról. Ha mégis, akkor ne hagyjuk az automatánál, ne dobjuk el, mert ez lehetőséget ad az esetleg figyelő tolvajoknak arra, hogy számlaegyenlegünket megtudják, vagy adatainkat megszerezzék.

Fontos, hogy kártyánkat sose hagyjuk az ATM-ben.

Bankkártyával történő vásárlás

A bankkártyák kereskedelmi használatára bevezetett POS terminálokra a kereskedő vagy a pénztáros feladata a kártya kezelése (áthúzása a terminálon leolvasás céljából). Ez a terminál lehet hordozható, illetve mobilhálózaton keresztüli összeköttetésű is. Arra viszont minden esetben figyeljünk, hogy a kártyánk kezelését sose tévesszük szem elől! Távollétünkben ugyanis több tranzakciót is végezhetnek a számlánkról, melyek bizonyítása utólag nehézkes lehet. Külföldön esetleg más pénznemben terhelik be számlánkat.

A PIN-kódot mindig úgy üssük be, hogy azt mások ne láthassák meg! Minden esetben ellenőrizzük a bizonylaton szereplő adatokat (pl. kártyaszám, összeg), mielőtt a bizonylatot aláírnánk. Ellenőrizzük, hogy vásárlás után visszakaptuk-e a kártyánkat. Könnyen előfordulhat, hogy a nagy sietségben a bolt, étterem alkalmazottja elfelejti visszaadni a kártyát, netán más kártyáját adja vissza.

Többszörös kártyalehúzás is előfordulhat bizonyos esetekben. Egy tranzakció során többször áthúzzák bankkártyánkat a POS terminálon, az nem jelent többszörös terhelést. Az összeköttetések ugyanis nem minden esetben épülnek fel sikeresen, ezért a terminál kijelzőjéről vagy a kinyomtatott bizonylatról leolvasható a sikertelenség. Amennyiben ez összeköttetési problémából adódik, a POS terminál kinyomtat egy bizonylatot, de azon nem szerepel az engedélyszám és egyéb adat sem. Ezek a bizonylatok nem adnak lehetőséget visszaélésre, de eltehetjük ezeket is, hátha hasznát vehetjük az esetleges későbbi félreértés tisztázásánál. A tranzakcióról mindig bizonylat (nyomat) készül, amelyből akkor lesz terhelés, ha azt alá is írjuk. Arra figyeljünk, hogy olyan bizonylatot csak egyszer írjuk alá, amely tartalmazza a terhelés összegét, a bankkártyánk számát, a dátumot és az engedélyszámot.

Internethasználat veszélyei, megtévesztő honlapok, e-mail-ek

Az Internet elterjedésének köszönhetően napjainkban megszokottá vált a „webes” vásárlás és az „online bankolás”. Sajnos a bűnözők is lesben állnak, és a zavarosban halásznak.

Elektronikus leveleket küldenek, melynek feladója látszólag egy megbízható vállalat vagy egy barát, de céljuk igazából az, hogy Önt rávegyék egy vírus letöltésére vagy egy olyan, csalás céljából készített webhelyre való belépésre, ahol személyes információkat – folyószámlaszámot, PIN-kódot - akarnak megszerezni. Minden Internet-felhasználónak fel kell ismernie a csaló szándékkal küldött e-maileket. (más néven "halászás" (phishing), megtévesztés, félrevezetés)

A csalók által küldött levelek ismertetőjelei:

- Nehéz az ilyen leveleket azonosítani, de általában arra kéri a címzettet, hogy látogasson el egy hamis weboldalra és adjanak meg, aktualizáljanak vagy erősítsenek meg érzékeny személyes adatokat.
- Hogy minél biztosabban rábírák a címzettet adatainak megadására, a címzett számláit fenyegető, sürgős intézkedést igénylő körülményre hivatkoznak.
- Észrevehető helyesírási hibákat tartalmazhatnak. A helyesírási hibák lehetővé teszik, hogy a csalási céllal küldött e-mailek az Internet-szolgáltatók által használt spam-szűrőkön átjussanak

A bankok nem küldenek sürgős intézkedést igénylő vagy időhöz kötött e-maileket, sem pedig olyanokat, amelyben arra kéri ügyfeleiket, hogy adják meg, aktualizáljanak vagy erősítsenek meg érzékeny adatokat. (mint pl. a bankkártya száma, az ATM PIN, a Felhasználói Név, a Jelszó, a T-PIN, a számlaszám, a hitelkártya száma vagy lejáratának dátuma, anyja leánykori neve stb.) Az Online szolgáltatásba történő regisztráció után csak Felhasználói Nevét és Jelszavát kell megadnia bejelentkezéskor.

Nem küldenek olyan e-mailt, amelyben arra kéri az ügyfelet, hogy a saját biztonsága érdekében adjon meg személyes, ill. folyószámlájára, bankkártyájára vonatkozó azonosító adatokat.

Saját védelme érdekében teendő biztonsági szabályok, módszerek:

- Minden esetben azonosítsa be az internetes oldal címét, szánjon rá néhány másodpercet és minden esetben gépelje be maga a www oldal címét!
- Személyes információk bevitele ELŐTT keresse meg a lakat jelet a webhely jobb alsó sarkában (Internet Explorer esetén jobb alsó sarok), hogy meggyőződhessen róla, a webhely biztonságos üzemmódban fut! A lakat szimbólumra (🔒) való dupla kattintás eredményeképp megnyíló ablak jelzi a weblap tulajdonosát.
- Ne kattintson a hivatkozásokra olyan kéretlen e-mailekben, amelyek személyes adatok megadására kéri. Ha nem adja meg a kért adatokat, a hivatkozásra való kattintással lehetővé teszi a tolvaj számára, hogy hozzáférjen az Ön számítógépéhez, és figyelje az Ön által leütött billentyűket és jelszavakat, amikor a különböző weboldalakra bejelentkezik.
- Legyen rendkívül óvatos az olyan cégekkel vagy személyekkel szemben, akik jelszavát, társadalombiztosítási számát vagy egyéb, személyes információt kérnek Öntől!
- Legyen különösen óvatos az olyan e-mailek megnyitásánál, amelyekhez csatolt fájl is tartozik! Még barátai között is lehet olyan, aki akaratlanul vírust küld Önnek e-mailben.
- Járjon el körültekintően, mielőtt rákattint egy e-mailben vagy egyéb üzenetben található linkre! Előfordulhat, hogy a link nem megbízható.
- Kizárólag biztonságos webhelyről, titkosított módon küldjön személyes vagy pénzügyi adatokat!
A közönséges e-mailek nem titkosítottak.
- Csak olyan cégekkel végezzen üzleti, pénzügyi tranzakciókat, amelyeket ismer, és amelyekben megbízik!

- Legyen óvatos! A nem valódi, "szélhámos" webhelyeket azért hozták létre, hogy megtévesszék az ügyfeleket és személyes információkat szerezzenek tőlük. Győződjön meg arról, hogy azok a webhelyek, amelyeken üzleti tranzakciókat végez, tartalmaznak adatvédelmi és biztonsági nyilatkozatokat, és ezeket tekintse át alaposan!
- Internetes felhasználói azonosítójaként mindig bonyolult jelszavakat és PIN-kódokat válasszon! Olyan jelszavakat használjon, amelyeket mások nehezen találnának ki! Személyes adatokat ne használjon!
- Operációs rendszerét és böngészőjét frissítse rendszeresen. A szoftverfrissítések gyakran biztonsági bővítéseket tartalmaznak, amelyeket ingyenesen tölthet le.
- Gondoskodjon arról, hogy otthoni számítógépére mindig a legfrissebb vírusfelismerő program legyen telepítve. A vírusfelismerő programokat gyakran kell frissíteni, hogy az új vírusok ellen is védjenek. Mindig azonnal töltsse le a vírusfelismerők frissítéseit, amint értesítést kapott elérhetőségükről!
- Otthoni számítógépébe való illetéktelen behatolások megakadályozására telepítsen személyes tűzfalat.
- Tartózkodjon bármilyen pénzügyi, banki tranzakció elvégzésétől olyan nyilvános helyen, ahol az Internet hozzáférés bárki számára biztosított (pl: internet kávézók). Rendkívül nehéz meggyőződni arról, hogy az ott használt számítógépeken nincs elhelyezve bármilyen olyan feltörő-program, amely által az Ön személyes, banki információit megszerezhetik.

Felvetődik egy másik kérdés is. Biztonságos az interneten vásárolni?

Az interneten, telefonon, postai úton történő fizetések közös jellemzője, hogy a kártya fizikailag nincs jelen a tranzakció során. Ez sok szempontból nagyobb körülményt igényel az Ön részéről.

Bankkártyája adatait mindig kezelje bizalmasan!

Ügyeljen rá, hogy a kártyaszámot és a kártya lejárat dátumát ne adja ki illetékteleneknek! A kártyabirtokos azonosítását szolgálja a kártya aláírási paneljében található 3 jegyű ellenőrző kód - amit CVC2-nek vagy CVV2-nek is szoktak nevezni - (a kártyaszám utolsó négy számjegye után), melynek megadását egyre több kereskedő kéri az egyéb adatok között. Ezt a kódot ugyanolyan gondossággal kezelje, mint a PIN-kódot!

Csak ismert, megbízható helyen kezdeményezzen bankkártyás fizetést!

Csak olyan internetes elfogadóhelyen vásároljon kártyájával, ahol ezt korábban már probléma nélkül megtette. Amennyiben új helyen fizetne, alaposan vizsgálja meg a weboldalt a következő szempontok alapján:

- mit árul, milyen szolgáltatást nyújt,
- talál-e részletes termékismertetőt,
- a cég telephelye, vonalas telefonszáma és e-mail címe megtalálható-e,
- szerződési, fizetési és szállítási feltételeket feltüntették-e.
- nézze meg, minőségi kifogás esetén hova és mennyi időn belül fordulhat reklamációval, milyen feltételek mellett vonhatja vissza megrendelését, mikor és milyen formában kapja vissza a pénzt,
- figyeljen a megfogalmazásra, helyesírási hibákat talál-e, legyen gyanús, ha összezapottnak tűnik a weboldal szerkesztése. Ilyen esetekben ne vásároljon az adott kereskedőnél!

Amint a kártyás fizetésre kerül a sor, mindig ellenőrizze, hogy a kereskedő által elfogadott kártyák logója (MasterCard és/vagy VISA) fel van-e tüntetve (ugyanúgy, mint a

"hagyományos" üzletekben)! Ezt hasonlítsa össze a kártyáján lévővel! Tényleg ugyanolyan vagy csak nagyon hasonló?

Nézze meg, hogy a kommunikáció titkosítva van-e! Erre utal az URL címében a "https" és az oldal jobb alsó sarkában szereplő lakat vagy a bal alsó sarkában szereplő kulcs, melyre rákattintva meg kell jelennie a tanúsítványnak.

Minden vásárlás alkalmával nyomtassa ki a megrendelését, annak visszaigazolását, a fizetéskor megadott adatokat, a megrendelt áru termékismertetőjét, stb!

Internetes azonosítóit kezelje bizalmasan! Mindig jelentkezzen ki a weboldalról, ha befejezte a vásárlást, nézelődést! Különösen fontos ez az internet kávézóknál és minden olyan számítógép esetén, amit más is használ!

Ha mégis megtörtént a baj

Javasolt, hogy amennyiben bankkártyánkat elveszítettük, lehetőség szerint azonnal próbáljuk meg az egyenlegünket (ha van, hitelkerettel együtt) kivenni egy másik kártyánkkal ATM-ben, postán, bankfiókban (számláról történő készpénzfelvétel esetén másik kártya sem szükséges), vagy lekötni, átutaltatni. Ezáltal a kártyával elérhető számlán nem marad pénz, az engedélykéresek visszautasításra kerülnek. Ha van rá lehetőség, az is megoldás lehet, ha lenullázzuk kártyánk napi/heti limitjét telefonon vagy az Internet bankon át.

Másik megoldás az azonnali letiltás. Legcélszerűbb telefonon megtenni ezt, ahhoz azonban szükség van a kártyánk számára és titkos kódunkra. A letiltás azonnali, és elektronikus tranzakciók esetében a bank engedélyező központja semmiféle további tranzakciót nem enged. Dombor nyomású bankkártyák esetében ATM és elektronikus vásárlás során a letiltás azonnal életbe lép, a fennmaradó elfogadóhelyeken csak mintegy 2-3 nap múlva.

A letiltott kártyákat az ATM azonnal bevonja. Ebben az esetben egyetlen próbálkozás sem lehetséges. POS (vásárlási) terminálok esetében a terminált kezelő kereskedő vagy postai alkalmazott kötelessége bevonni a letiltott bankkártyát.

Amennyiben a témával kapcsolatban kérdése merül fel, keresse osztályunkat az alábbi elérhetőségeken.



Somogy Megyei Rendőr-főkapitányság Bűnügyi Igazgatóság Bűnmegelőzési és Áldozatvédelmi Osztály

7400 Kaposvár, Szent Imre u. 14/c.
Tel.: 82/502-771; BM: 03/23/27-71; Fax:27-72
