Újabb csalás hódít - Így védekezz a bankszámlás lenyúlások ellen

Bár a bankkártya-biztonság látványos fejlődésnek indult az elmúlt években, a csalók, bűnözők is erősen próbálják tartani a lépést. Az adatlopásra sokszor ott kerül sor, ahol a leggyengébb a védelem: a felhasználók számítógépein.

A technológia fejlődését jól mutatja, hogy ma már vannak olyan vírusok, trójai kártevő, amelyek arra is képesek, hogy az SMS-üzenetekben érkező banki tranzakciós azonosítókat elfogják, és ezeket felhasználva hamis egyenleget mutassanak a bankszámla-tulajdonosok felé.

Egy friss magyar felmérés készítői arról számoltak be, hogy száz magyar bankkártya-tulajdonosból hatnál történt már visszaélés a kártyájával. Az összesített kár az óvatos becslések szerint is eléri az 1,5 milliárd forintot.

A G Data vírusirtó cég 1200 fős reprezentatív felmérésében a válaszadók 6 százaléka számolt be arról, hogy már előfordult, hogy ismeretlen személy visszaélt kártyájával. Mindez azt jelenti, hogy összességében legalább 250-300 ezer incidens történhetett eddig magyar állampolgárokkal.

A hitelkártyákkal történő visszaélések során okozott kár mértéke az esetek 26 százalékában elérte vagy meghaladta a 20 ezer forintot, 40 százalékában 20 ezer forintnál kisebb összegű volt, míg 31 százalékban sikerült megakadályozni a közvetlen károkozást. Mindez legalább 1,5 milliárd forint közvetlen veszteséget jelent, melyhez kapcsolódóan a válaszadók 62 százaléka nyilatkozta azt, hogy az okozott kárt nem térítette meg a bank. Emellett a visszaélések 55 százalékában volt szükség új bankkártya igénylésére, és ezen esetek 75 százalékában az ügyfelet terhelték az új kártya kiállításának költségei.

A számítógépeken a leggyengébb a védelem

Szakértők szerint a netbankolás és a mobilbankolás terjedésével tovább növekedhet az incidensek száma, mivel folyamatosan újabb kártevők jelennek meg, melyek a bankkártyák adatait próbálják megszerezni. Míg Magyarországon 2009-ben még csupán az internetezők 46 százaléka vett igénybe netbank szolgáltatást, ez az arány 2011-ben már 57 százalék volt.

Ahogy egyre több felhasználó használja bankkártyáját az interneten, ez a bűnözők számára egyre csábítóbb vadászterületet jelent. A Magyarországon terjedő vírusok havi 10-es toplistáján rendszeresen 4-5 trójai program szerepel. A bűnözők megszerzik a bankkártya adatokat, de a legújabb trójaiak már ennél jóval többre képesek. Utalásokat hajtanak végre a felhasználók nevében, sőt a cselekmény felderítésének megnehezítése érdekében még az egyenlegét is meghamisítják.

Már a telefonunkat támadják

A ma terjedő trójai kártevők arra is képesek, hogy az SMS-üzenetekben érkező banki tranzakciós azonosítókat elfogják, és ezeket felhasználva hamis egyenleget mutassanak a bankszámla-tulajdonosok felé - mondta el Maulis Csaba internet biztonsági szakértő. A kártevők egy alkalmazásban rejtőzve juthatnak be okos telefonunkba, annak

telepítésével kezdik meg tevékenységüket (jellemzően például ingyenes csengőhang, háttérkép letöltésével kerülhetnek készülékünkbe). Leginkább onnan vehetjük észre, hogy készülékünkben ilyen trójai garázdálkodik, ha gyakran kér valamilyen - addig nem tapasztalt - biztonsági frissítést, beállítást (ezek alapvetően mind hamis, információszerzésre irányuló jelzések). Maulis Csaba azt tanácsolja, ilyenkor azonnal ellenőrizzük le bankszámlánkat, vegyük fel a kapcsolatot bankunkkal, és jelezzük nekik a veszély gyanúját. A megelőzésben segíthet, ha készülékünkre feltelepítünk egy vírusirtó programot.

Óvatosan használjuk a netbankot

A Pénzügyi Szervezetek Állami Felügyelete (PSZÁF) ugyanakkor arra figyelmeztet, hogy az elektronikus pénzügyi szolgáltatásokkal kapcsolatos adatmásolásról, adathalászatról időnként szárnyra kapó hírek sokakat elbizonytalanítanak az elektronikus bankolás biztonságával kapcsolatban.

Azt tanácsolják, használjunk víruskereső valamint a trójai alkalmazások elleni védelmet nyújtó programot és rendszeresen frissítsük azt. A vírusirtó vagy antivírus program célja annak biztosítása, hogy a hálózatba vagy egy adott számítógépbe ne juthasson be olyan állomány, mely károkozást, illetéktelen adatgyűjtést vagy bármely, a felhasználó által nem engedélyezett műveletet hajt végre. Ma már számtalan ingyenesen letölthető vírusirtó program létezik, melyek használata és frissítése egyszerű. A vírusirtókkal rendszeres vírusirtás is végezhető, de e programok folyamatosan is tudják figyelni a számítógép kommunikációját és kiszűrik a káros állományokat.

A PSZÁF azt ajánlja, telepítsünk tűzfal-szoftvert is, amit szintén rendszeresen frissítsünk. A tűzfal az illetéktelen hálózati hozzáféréseket megakadályozó szoftveres vagy hardveres eszköz, amely a kommunikáció folyamatába beépülve figyeli és szabályozza az átáramló forgalmat. A tűzfalakat általában az internetre kapcsolt számítógépek és helyi hálózatok védelmére alkalmazzák, hogy illetéktelenek ne férhessenek hozzá a hálózathoz és a számítógépeken tárolt adatokhoz. Fontos megjegyezni, hogy az ingyenesen letölthető vírusvédő programok nem rendelkeznek beépített tűzfal-funkcióval, ezért azt külön kell telepíteni az antivírus program mellé.

Fontos, hogy interneten keresztül csak biztonságos helyről intézzük pénzügyeinket. Ne adjunk lehetőséget arra, hogy elektronikus kódunkat más is láthassa. Csak végső megoldásként használjunk nyilvános internetet (például internet kávézóban), vagy jelszóval nem védett Wi-Fi hálózatot bankügyeink intézésére. Ha mégis ezt tesszük, saját érdekünkben tartsunk be néhány fontos biztonsági szabályt:

- Ne válasszuk azt a lehetőséget, hogy a számítógép megjegyezze a belépéshez szükséges jelszót!

- Tanácsos törölni a böngésző tárolóját is az internetes bankolás után, hogy illetéktelen személy ne tudjon adatainkkal visszaélni.

- Ha nyilvános helyen intézzük pénzügyeinket, célszerű ezt követően megváltoztatni a belépési jelszót.

- Az internetes rendszerből ne a böngésző bezárásával, hanem a kilépés gombbal jelentkezzünk ki.

- Az internetbank használata közben a böngésző címsorában szereplő linket adatainak biztonsága érdekében ne küldjük tovább.

Forrás: RPozitív Híreső