E L B Í R

Elektronikus Lakossági Bűnmegelőzési Információs Rendszer
Lakossági hírlevél

2013. január

14000-570-1/2013. ált.

Adatvédelem, bankkártya- és Internet-használat, okos telefonok, táblagépek védelme

Az ún. okos telefonok és táblagépek használatának elterjedésével újabb eszközök váltak a bűnözők célpontjaivá. Egyes elkövetők a készülékeket értéke, eladhatósága miatt akarják megszerezni, másokat inkább a rajta tárolt jóval nagyobb értéket képviselő személyes, esetleg céges adatok érdekelnek.

Legtöbbször gépkocsi-feltörések, alkalmi lopások, a zseblopások, strandlopások, betörések, utcai rablás, kifosztás útján jutnak a bűnözők a személyes adatokat tartalmazó iratokhoz, bankkártyákhoz és telekommunikációs készülékekhez. Az így megszerzett adatokkal, okmányokkal pl. visszaéléseket, csalásokat követhetnek el.

A személyes adatok, bankkártyák és mobileszközök védelmének kétirányúnak kell lennie. Egyrészt biztosítani kell ezek fizikai megszerezhetetlenségét, másrészt a virtuális térben „utazó” adatok biztonságáról is gondoskodni kell.

Az alábbi tanácsok betartásával nagy lépést tehetnek saját biztonságuk érdekében, kérjük, fogadják meg azokat!

Gépkocsi feltörés és megelőzésének lehetőségei:

Rendőrség tanácsai:

- Okmányokat tartalmazó táskát soha ne hagyjon a gépkocsiban!
- Látható helyen ne hagyjon értéktárgyat, táskát, műszaki cikkeket az utastérben! Az üléseken hátrahagyott tárgy – akár ruhanemű, vagy üres táska - felkeltheti a tolvaj érdeklődését. A megvásárolt értékeket a csomagtartóban célszerű elhelyezni.
- Ha csak „egy pillanatra” hagyja őrizetlenül autóját, akkor is zárja be!
- Szereltessen járművébe riasztót! A mechanikai és elektronikus védelemi rendszer együttese a leghatékonyabb.
- Sötétedés után parkoljon megvilágított, vagy lehetőleg forgalmas helyen.
- Ha megtörtént a baj és feltörték járművét, semmihez nem nyúljon, őrizze meg azt eredeti állapotában, majd értesítse a rendőrséget.

Zseblopás és alkalmi lopás:

Hogyan védje meg magát a zsebtolvajoktól?

- Fokozottabban figyeljen értékeire, ha forgalmas helyen tömegben tartózkodik, utazik!(válltáskáját maga előtt fogva közlekedjen).
- Ne tartson okmányokat, értékeket hátizsák, hátitáska külső zsebeiben!
- Ne tegyen egy helyre pénztárcát, csekket, hitelkártyát, iratokat, mobiltelefont! (Viszonylag biztonságos tárolási helyek a belső zsebek, vagy a kézre, lábra erősíthető, övön hordható, illetve a ruházat alatt nyakba akasztva viselhető táskák.)
- Bankkártyája mellett soha ne legyen ott a PIN kód!
- Vásárláskor, az áru válogatásakor soha ne tegye le táskáját, pénztárcáját bevásárlókocsira, pultra!

Besurranásos lopások:

- Ha otthon tartózkodik, zárja lakásának bejárati ajtaját, alacsonyan levő ablakait, kert-, vagy garázskapuját!
- Iratokat, táskákat, mobiltelefonokat lehetőleg ne az előszobában, vagy a bejárati ajtó közvetlen közelében tároljon!
- Vásárlások, szórakozóhelyek, vendéglátóhelyek látogatása során iratait, táskáját mindig tartsa felügyelet alatt, kabátjában ne tartson pénzt, ill. értékeket!
- Munkahelyén is – főleg ahol ügyfelek fordulnak meg - tartsa biztonságos helyen személyes értékeit, iratait, telefonját!

Bakkártyahasználat:

Az ATM használat veszélyei, biztonságos használata

Az ATM-knél az elkövetők célja a pénz és/vagy bankkártya adatok és PIN kód megszerzése.
Nem egyszerű felismerni az elkövetők által az automatákra felszerelt eszközöket, berendezéseket, minden pénzkivétel előtt ellenőrizze a kártyafogadó nyílást, a pénzkiadó nyílást, esetleges billentyűzetre irányuló kamera elhelyezését. Amennyiben úgy ítéli meg, hogy nem biztonságos, válasszon egy másik ATM-t.
Beltéri automata használata esetén próbálja elkerülni, hogy mások is a helyiségben tartózkodjanak. Ne hagyja, hogy készpénzfelvétel végrehajtása közben idegenek megzavarják, vagy elterelj̈ék figyelmét, a „segítséget” felajánlóktól pedig óvakodjon.

A PIN kód beütésekor el kell takarni a billentyűzetet, meg kell bizonyosodni róla, hogy a következő sorban álló ne láthassa azt, illetve a felvenni kívánt összeget. Amennyiben a tranzakció közben bármi gyanúsat észlel, inkább törölje a tranzakciót és hagyja el a helyszínt. A készpénzfelvétel befejezését követően ne kezdje el az ATM előtt állva számolni pénzt, inkább mielőbb tegye el a kártyát és a készpénzt. Lehetőleg ne kérjen bizonylatot a tranzakcióról. Ha mégis, akkor ne hagyja az automatánál, ne dobja el, mert ez lehetőséget ad az esetleg figyelő tolvajoknak arra, hogy számlaegyenlegét megtudják, vagy adatait megszerezzék.
Fontos, hogy kártyáját sose hagyja az ATM-ben!

Bankkártyával történő vásárlás
A bankkártyák kereskedelmi használatára bevezetett POS terminálokon 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 figyeljen, hogy a kártyája kezelését sose tévessze szem elől! Távollétében ugyanis több tranzakciót is végezhetnek a számlájáról, melyek bizonyítása utólag nehézkes lehet. Külföldön esetleg más pénznemben terhelik be számláját.
A PIN-kódot mindig úgy üsse be, hogy azt mások ne láthassák meg! A bizonylat aláírása előtt minden esetben ellenőrizze a azon szereplő adatokat (pl. kártyaszám, összeg). Ellenőrizze, hogy vásárlás után visszakapta-e a kártyáját.
Többszörös kártyalehúzás is előfordulhat bizonyos esetekben. Ilyenkor arra figyeljen, hogy olyan bizonylatot csak egyszer írjon alá, amely tartalmazza a terhelés összegét, a bankkártyja számát, a dátumot és az engedélyszámot.

Az Internethasználat veszélyei, megtévesztő honlapok, e-mail-ek, adathalászat

Az Internet elterjedésének köszönhetően napjainkban megszokottá vált a „webes" vásárlás és az „online bankolás" és már a „mobil bankolás" is. 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 kérik a címzettet, hogy látogasson el egy hamis weboldalra és adjanak meg, aktualizáljanak vagy erősítsenek meg érzékeny személyes adatokat.
- Hogy minél biztosabban rábírják 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

Nagyon fontos! A bankok soha nem küldenek sürgős intézkedést igénylő vagy időhöz kötött e-maileket, sem pedig olyanokat, amelyben arra kérik 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 kérik az ügyfeleket, hogy a saját biztonsága érdekében adjon meg személyes, ill. folyószámlájára, bankkártyájára vonatkozó azonosító adatokat. Amennyiben az internetes banki felület használata során helyesírási hibákat

tartalmazó, magyartalan megfogalmazású üzenetet kap, a megszokottól eltérő a képernyő, esetleg új adatbeviteli mező jelenik meg, azonnal szakítsa meg a kapcsolatot az adott weboldallal, és értesítse számlakezelő bankját.

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 kérik. 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 töltse le a vírusfelismerők frissítéseit, amint értesítést kapott elérhetőségükről!
- Otthoni számítógépébe való illetéktelen behatolások megakadályozására telepítsen személyes tűzfalat.
- Itt hívjuk fel a figyelmet az okostelefonok és táblagépek kiemelkedően fontos védelmére, hiszen gyakorlatilag azokkal a funkciókkal rendelkeznek, mint a számítógépek, laptopok. A mobileszközökre is kifejlesztettek már a vírusvédelmi programokat, tűzfalakat. Sok ingyenesen elérhető, használja ezeket.

- 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 olyan feltörő-program, amely által az Ön személyes, banki információit megszerezhetik.

Biztonságos-e az Interneten történő vásárlás?
Az Interneten, telefonon, postai úton történő fizetések közös jellemzője, hogy a kártya fizikailag nincs jelen a tranzakció során. Ez sok szempontból nagyobb körültekintést igényel az Ön részéről.

Bankkártyája adatait mindig kezelje bizalmasan!
Ügyeljen rá, hogy a kártyaszámot és a kártya lejárati 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 pénzét,
- figyeljen a megfogalmazásra, helyesírási hibákat talál-e, legyen gyanús, ha összecsapottnak 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 címben 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 kávézókban 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 engedélykérések 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. Dombornyomású 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.

Vigyázzanak értékeikre és adataikra!!

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. Pf.:121
TEL:82/502-700-2732, FAX:82/502-700-2772
E-mail:bunmeg@somogy.police.hu