Házhoz megyünk!
2017. december

A Vas Megyei Rendőr-főkapitányság Gazdaságvédelmi Alosztályának felhívása a biztonságos bankkártya-használattal és az internetes vásárlásokkal kapcsolatban

Hírlevelünkkel a bankkártya és más készpénz-helyettesítő fizetési eszköz használata, valamint az internetes vásárlás során előforduló bűncselekmények megelőzéséhez kívánunk segítséget nyújtani, továbbá útmutatással szolgálunk az ilyen cselekmény észlelését követő legfontosabb teendőkről.

Bár tökéletes védelem nem létezik, az alábbi óvintézkedésekkel elejét vehetjük a legtöbb visszaélésnek. Javaslataink alkalmazása legfeljebb felhasználói szintű számítástechnikai és hétköznapi szintű pénzügyi ismereteket igényel.

A bankkártya és a kártyaadatok megóvása

Csak indokolt esetben adjuk ki kezünkből bankkártyánkat; munkahelyen, rendezvényen, ismerősi körben se hagyjuk más által hozzáférhető helyen! Sajnálatos módon a közvetlen környezetünkben is előfordulhat, hogy azt valaki jogtalanul használja. **Ha mégis át kell adnunk** másnak, folyamatosan lássunk rá, ne hagyjuk felügyeletünk nélkül! Ne adjuk meg másnak a PIN kódot, azt ne tartsuk a bankkártyával egy táskában vagy ruhadarabban!

Ne csupán magát a bankkártyát, hanem annak **adatait is óvjuk** meg! A használat során takarjuk a PIN kód bevitelére szolgáló billentyűzetet! Amennyiben szokatlan eszközt vagy változást látunk a készpénzkiadó automatán (ATM), vagy POS terminálon – különösen a billentyűzet, illetőleg a kártyaolvasó nyílás közelében –, tanúsítsunk fokozott óvatosságot! Szükség esetén érdeklődjünk az automata üzemeltetőjénél, illetve a banknál!

Pusztán a **kártyán felírt adatok** ismerete is elegendő lehet jogosulatlan vásárláshoz. Ne adjuk ki netbankos felhasználónevünket, banki azonosítónkat, jelszavunkat, a biztonsági kérdést és választ, a kártya adatait, beleértve a hátoldalán található CVC/CCV/CVV kódot (három számjegy); azokat kizárólag saját magunk használjuk és csak az általunk kezdeményezett műveletekhez!

Kerüljük az ismeretlen és nem ellenőrizhető feladótól érkező **kéretlen üzenetek** és csatolmányaik megnyitását! Ne higgyünk a PIN kód, CVC/CCV/CVV kód, jelszó, biztonsági kérdés/válasz iránt érdeklődő telefonhívásnak, SMS-nek vagy elektronikus levélnek!

Amennyiben **bankkártyával** fizetünk, azt biztonságos kapcsolatot nyújtó (https://...) oldalon, kizárólag általunk kezdeményezett tranzakció keretében tegyük meg! A kártya adatait a fizetésre szolgáló online felületen adjuk meg, ne küldjük el elektronikus levélben vagy más módon!

Ügyeljünk arra, hogy az adatokat csak az eredeti honlapon adjuk meg! Kerüljük az **adathalászok** által létrehozott, az eredeti – jellemzően banki – honlapra megjelenésében nagyon hasonló honlapokat, ennek érdekében figyeljünk a megnyitott böngészőlap címsorában lévő feliratra! A megszokott szövegtől egyetlen karakternyi eltérés is árulkodó lehet.

A kártyaadatok megadását és a netbankolást saját, **más által nem használt számítógépen**, illetőleg mobil eszközön végezzük! Ne vegyünk igénybe ilyen célra munkahelyi, valamint szálláshelyen, közösségi hozzáférési ponton kihelyezett eszközt!

Számítógépünk, telefonunk védelme

Az aktuálisan nem használt számítógépet, okostelefont vagy egyéb mobil eszközt védjük **képernyőzárral**!

A bűnelkövetők kihasználják, hogy – a levelezőrendszer beállításaitól függően – a küldő postafiókunkban látható neve nem feltétlenül azonos a tényleges **elektronikus levelezési címével**, így az ismerős személytől, illetve cégtől érkezettnek tűnhet a küldemény. A tényleges cím általában felfedhető úgy, hogy a kurzort a megjelent név fölé visszük, továbbá megtekintjük az eredeti üzenet jellemzőit.

Okostelefonon és más mobil eszközön is telepítsünk **vírusirtó alkalmazást**, amit rendszeresen frissítsünk! Javasolt egyszerű vírusirtó helyett valamennyi online és offline fenyegetés elleni komplett biztonsági szoftvercsomag használata és ütemezett teljes rendszerellenőrzés futtatása. Az úgynevezett biztonsági rések kijavítása érdekében ugyancsak frissítsük az eszköz operációs rendszerét, a böngészőt és más alkalmazásokat is!

Internetes műveletek során részesítsük előnyben a vezetékes, illetve a megbízható vezeték nélküli (wi-fi) **hálózatokat**! Kerüljük a nyilvános, különösen a jelszóval nem védett vagy könnyen hozzáférhető (például vendéglátóhelyen kiírt) jelszóval ellátott hálózatokat!

Saját vezeték nélküli hálózatunkban a megosztó eszközökön (router, switch stb.) állítsunk be **MAC cím szerinti szűrést**, így csak az általunk meghatározott számítógépek csatlakozhatnak a hálózatra. (A MAC cím a számítógépek, telefonok és más számítástechnikai eszközök egyedi azonosító száma, amit az eszköz saját menüjében és a hálózati megosztó eszközünk kezelőfelületén is megtekinthetünk. A hálózatra csatlakozáshoz engedéllyel rendelkező eszközök listáját bármikor módosíthatjuk.)

Gyakran **változtassuk meg jelszavunkat** a netbankban, a hozzá kapcsolódó e-mail fiókban és azokon a weboldalakon is, ahol bankkártyánk adatait regisztráltuk! Ne alkalmazzuk ugyanazt a jelszót más alkalmazásoknál is, illetőleg ne használjuk később újra ugyanazt! Az általunk használt alkalmazásokhoz/honlapokhoz tartozó, onnan érkezett jelszavakat módosítsuk! (Ilyen jelszavak jellemzően új szoftver telepítése, vagy weboldalon történt regisztrációt követően, továbbá elfelejtett jelszó esetén kérésre, automatikusan generált levélben érkeznek.)

A böngészők és egyéb programok felhasználónév-, jelszó- és **űrlapadat-megjegyző funkcióit** (jelszavak megjegyzése, automatikus kitöltés) kapcsoljuk ki, az esetleg már mentett adatokat töröljük. A kikapcsolást – böngészőtől függően – általában a „Beállítások >> Biztonság/adatvédelem >> Jelszavak/űrlapok automatikus kitöltése/mentése” menüpontban tehetjük meg, a mentett adatok pedig „Beállítások/előzmények >> Böngészési előzmények törlése >> Jelszavak/űrlapadatok törlése” művelettel törölhetőek.

Számítástechnikai felhő jelszavak tárolására és egyéb célokra történő igénybe vétele esetén tartsuk szem előtt, hogy adataink tárolása külföldön történhet, ahol a harmadik személy általi hozzáférés gyakorlati és jogi lehetőségei eltérhetnek a hazai adatvédelmi szabályozástól!

A számítógéphez **távoli hozzáférést**/kapcsolatot/asztalt kérő megkeresést – a kifejezetten általunk kért távsegítség esetét leszámítva – célszerű megtagadni. Ugyanakkor, kellő körültekintés mellett hasznos lehet a mobil eszközünkön a tartózkodási hely, valamint a távoli zárolás és törlés funkciók aktiválása. E funkciók segíthetnek az elveszett készülék megtalálásában, végső esetben a rossz kezekbe került eszköz zárolásában és adatainak törlésében.

A kárt megelőző/mérséklő intézkedések

Állítsunk be viszonylag alacsony, a napi szükségleteinkhez igazodó készpénzfelvételi, vásárlási és érintés nélküli (PayPass) **összeghatárt** (limitet). Szükség esetén – például nagy értékű műszaki cikk vásárlásakor – átmenetileg módosítsuk a limitet, majd állítsuk vissza.

Kérjünk SMS-ben vagy elektronikus levélben érkező **értesítést** a bankszámlához történő online hozzáférésről (netbanki belépés), a számlán végzett műveletekről (zárolás, átutalás stb.) és a bankkártya-használatról. A kis értékű műveletekről szóló, ezért feleslegesnek ítélt üzenetek értesítési összeghatár beállításával elkerülhetőek.

Legalább a nagyobb összegű műveletek engedélyezését kössük a bankunktól SMS-ben érkező, **egyszer használható biztonsági kódhoz**!

Célszerű a **műveleteket más eszközön** végezni, mint amelyikre a kódot kapjuk. Ellenkező esetben például a kémprogrammal fertőzött telefonon kezdeményezett átutalás adatai, valamint felhasználónevünk, banki (ügyfél)azonosítónk és jelszavunk mellett a tranzakció teljesítéséhez szükséges egyszeri biztonsági kódot is megszerezhetik az elkövetők.

Amennyiben lehetséges, kérjük a bankkártya használatának **földrajzi térségek szerinti korlátozását**! E módon kizárhatjuk, hogy az esetleg illetéktelenek kezébe került bankkártyánkat, illetve annak adatait olyan országokban használják készpénz-felvételre vagy vásárlásra, ahol azt magunk nem szándékoztuk.

Internetes fizetés során lehetőség szerint használjunk **webkártyá**t, amit csak a közeljövőben vagy rendszeresen így elkölteni tervezett összeggel töltsünk fel!

Csak **különösen indokolt esetben regisztráljuk** (tároljuk) bankkártyánk adatait honlapon, és kizárólag olyan honlapon, amely biztonságos kapcsolatot nyújt! Amennyiben az adott honlap és kártya lehetővé teszi, regisztrálhatjuk webkártyánkat.

Internetes megrendelés előtt **tájékozódjunk az eladóról**! Ezt megtehetjük – többek között – az adott honlapon és az ár-összehasonlító oldalakon szereplő vásárlói értékelések megtekintése, valamint a webáruház, illetőleg azt üzemeltető cég vonatkozásában hozott esetleges fogyasztóvédelmi döntések megismerése útján.

Megrendeléskor válasszuk az **utánvétes fizetési módot**!

Ha mégis bekövetkezik…

Haladéktalanul **jelentsük az problémát** a bank, a fizetési szolgáltató, illetve a webáruház felé! Egyes szolgáltatók és bankok esetében erre folyamatosan működő forródrót áll rendelkezésre. Az általuk alkalmazott eljárásrendre is figyelemmel kérjük a tranzakció felfüggesztését, illetve az összeg visszatérítését!

Szükség esetén függesszük fel, vagy **tiltsuk le** a bankkártyát!

Végezzünk **teljes keresést** az eszközeinken az esetleges kémprogramok és más, rosszindulatú szoftverek/kódok eltávolítása érdekében! Az esetleg fertőzött eszközt addig is válasszuk le a hálózatunkról és ne használjuk személyes adatainkat érintő, vagy pénzügyi műveletekre! A kitudódott jelszót – biztonságos eszközről – változtassuk meg!

Amennyiben bűncselekmény áldozatává váltunk, a Rendőrségen tett **feljelentéshez mellékeljük** az ügyhöz kapcsolódó valamennyi művelet bizonylatait, az üzeneteket és az elektronikus leveleket, a jellemzőikkel együtt!

VAS MEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNÜGYI IGAZGATÓSÁG
BŰNÜGYI OSZTÁLY
Bűnmegelőzési Alosztály
9700 Szombathely, Petőfi S. u. 1/C.
Telefon: 06/94/521-065 Fax: 06/94/521-160
E-mail: bunmeg.vasmrfk@vas.police.hu