BŰNMEGELŐZÉSI HÍRLEVÉL

2022. november

Jeles napok:

NOVEMBER 1.— MINDENSZENTEK
NOVEMBER 2.— HALOTTAK NAPPJA
NOVEMBER 3.— ISKOLÁN BELÜLI ERŐSZAK ELLNI KÜZDELEM NAPA
NOVEMBER 11.— SZENT MÁRTON ÜNNEPE
NOVEMBER 20.— GYERMEKEK JOGAINAK VILÁGNAPJA
NOVEMBER 27.– ADVENT ELSŐ NAPJA

https://www.police.hu/hu/hirek-es-informaciok/bunmegelozes/aktualis/hogy-ne-valjon-csalok-aldozatava

Közeledik a karácsony és ezzel az időszakkal a vásárlási „láz„ is megindul, a csalók is nagyobb teret kapnak „működésükhöz”.
Jelen hírlevelünkben abban próbálunk segítséget nyújtani, miként figyelhetünk arra, hogy kisebb eséllyel váljunk csalók áldozatává.
Vigyázzanak értékeikre, vigyázzanak magukra, hogy az ünnepi készülődés ne váljon rémálommá!

ELBIR
/ELEKTORNIKUS LAKOSSÁGI HÍRLEVÉL/
Komárom-Esztergom Megyei Rendőr-főkapitányság
Bűnügyi Osztály
Bűnmegelőzési Alosztály

A robbanásszerűen fejlődő digitális világ nagyon vonzóvá vált a csalók számára.

A megtévesztésen alapuló nyerészkedés, az átverések és csalások különböző formái ismertek, az elkövetők pedig egyre kifinomultabb megoldásokat alkalmaznak annak érdekében, hogy áldozataikat megkárosítva jellemzően anyagi haszonhoz jussanak.

ADATHALÁSZ BANKI E-MAILEK, SMS-ek

Az adathalászat olyan, banki ügyfeleket célzó, csaló szándékú e-mail, amely személyes, pénzügyi vagy biztonsági információi megosztására veszi rá a címzettjét. Ezek a levelek azonosnak tűnhetnek azokkal az üzenetekkel, amelyeket az igazi bankok küldenek: lemásolják a valódi e-mailek logóit, kinézetét és stílusát, esetenként korábbi (hamis vagy valós) levélváltások részleteit is tartalmazzák. Általában sürgető hangvételűek, például büntetéssel fenyegetnek arra az esetre, ha nem válaszol, de arra is kérhetik, hogy töltsön le egy mellékletet, vagy kattintson egy hivatkozásra. Az internetes bűnözők arra építenek, hogy az emberek elfoglaltak: felületes áttekintésre, futó pillantásra a hamis e-mailek igazinak tűnnek. Ennek következtében a címzett nagyobb valószínűséggel veszi komolyan őket, és cselekszik.

MEGHAMISÍTOTT BANKI OLDALAK

Az adathalász banki e-mailekben található hivatkozások gyakran egy meghamisított banki weboldalra vezetnek, ahol a célszemélyt a pénzügyi és személyes adatai megadására kérik. Ezek a webhelyek szinte teljesen ugyanolyanok, mint a mintának használt valódi oldal. Általában tartalmaznak azonban egy felugró ablakot, amelyik a banki hitelesítő adatok megadását kéri. Gyanús lehet továbbá a gyenge minőségű grafika, valamint a sürgető hangvételű üzenetek, tartalmak.
A valódi bankok nem használnak ilyen ablakokat, tartalmakat.

Mit tegyen hamis banki hívás esetén?

Kezelje óvatosan, fenntartással a kéretlen telefonhívásokat!

Minél sürgetőbb a hívás és az üzenet, annál gyanúsabb! Lassítson és gondolja át alaposan, hogy mit is kérnek valójában!

Gyanús telefonhívás esetén ne adjon meg személyes adatokat és szakítsa meg a beszélgetést!

Ha a kijelzett telefonszám valóban a bank ügyfélszolgálati telefonszáma, az sem garancia arra, hogy tényleg onnan keresik. Annak az ellenőrzésére, hogy az illető valóban az, akinek mondja magát, keresse meg a szervezet telefonszámát (a weboldalukon vagy online kereséssel), és lépjen velük kapcsolatba közvetlenül!

Ne használja az ellenőrzéshez a hívó által megadott telefonszámot! A szám hamis lehet, vagy kifejezetten a csaláshoz is létrehozhatták.

A csalók az interneten könnyen megszerezhetik az alapvető információkat Önről vagy a vállalatról, amelynek dolgozik, például a közösségimédia-profilok felhasználásával. Nem bízhat meg a hívóban csak azért, mert ő ismeri ezeket az adatokat.

Soha ne adja meg a betéti vagy hitelkártyája PIN-kódját, CVV kódját, vagy az online banki jelszavát! A bankok sosem kérik el ezeket az információkat!

Soha ne telepítsen mások kérésére olyan programot számítógépére vagy telefonjára, amit nem ismer!

Soha ne utaljon pénzt telefonon érkező kérésre! Egy bank sosem kér ilyet.

A csalási szándékú hívásokat jelentse a bankjának!

A Bankok nem alkalmaznak közös ügyfélszolgálati rendszert egymás között!

Banki hívás esetén, amikor kiderül a csaló számára, hogy hiába hívta Önt az OTP nevében, mert Ön nem ott vezeti a számláját, nem tudná a saját bankjához kapcsolni akkor sem, ha valódi ügyintéző lenne!

IT eszközök biztonsága

Ne telepítsen semilyen alkalmazást számítógépére vagy telefonjára idegen személy kérésére!

Mobilalkalmazásokat mindig a hivatalos alkalmazásáruházból töltsön le!
E-mailben, üzenetben kapott linkről ne töltsön le alkalmazásokat!

Ellenőrizze, hogy az eredeti alkalmazásról van-e szó!
A bűnözők hasonló neveket használnak, hogy megtévesszék a felhasználókat.

Letöltés előtt ellenőrizze az alkalmazás és a gyártó értékelését is!
Szánjon rá időt és olvassa el a felhasználók véleményét! Ha rossz értékelést kapott az alkalmazás, ne töltse le! Válasszon olyan alkalmazást, amit sokan töltöttek le és pozitív értékeléssel bír!

Ellenőrizze, hogy milyen engedélyeket kér az alkalmazás!
Ha nem tartja szükségesnek, akkor ne töltse le! (pl. navigációs és térkép programoknak szükségük lehet hozzáférni a telefon helyzetéhez, de a zenelejátszónak már nem).

A távoli asztal (remote desktop) szolgáltatást nyújtó programok hozzáférést biztosítanak más, távol lévő személy részére az Ön számítógépéhez. A **másik fél teljeskörűen hozzáfér** az Ön **adataihoz, fájljaihoz, böngészési előzményeihez**, a különböző oldalakon használt felhasználói neveihez és jelszavaihoz.

Távoli asztalhoz szolgáltatást nyújtó programok

- AnyDesk
- Chrome Remote Desktop
- TeamViewer
- LogMeIn
- Microsoft Remote Desktop
- VNC különböző változatai

Távoli asztal szolgáltatást nyújtó program telepítésekor és használatakor legyen fokozottan körültekintő!

Felhasználói nevét, jelszavát, bankkártyájának adatait soha **ne küldje el senkinek**! Bankkártyájának adatait csak banki fizetési oldalon vagy más megbízható pénzügyi szolgáltató oldalán adja meg!

Felhasználói fiókok (levelezési, banki, közösségi oldalak) esetében állítson be **kétfaktoros (kétlépcsős) azonosítást,** ha lehet! Több azonosítási mód közül válassza azt, amelyik SMS helyett mobilalkalmazás segítségével azonosít!

INTERNET ONLINE IS BIZTONSÁGBAN TUDATOSAN

Országos Rendőr-főkapitányság
http://www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag

Ön mit tehet?

§ Legyen éber! A bankok sosem kérnek e-mailben bizalmas információkat, például az online banki jelszavát! A bankok kizárólag biztonságos módon, az online banki felületen kommunikálnak az ügyfelekkel, sosem kérnek bizalmas adatokat ilyen formában!

§ Ne kattintson az üzenetben lévő hivatkozásokra, és ne nyissa meg a mellékleteket, a webes bejelentkezések címeit inkább manuálisan gépelje be, vagy használja a hivatalos banki oldalt!

§ Mindig legyen gyanakvó a mások által kezdeményezett olyan kapcsolatfelvételekkel szemben, amikor nem tud minden kétséget kizáróan megbizonyosodni a másik fél identitásáról! Különösen igaz ez az elektronikus kommunikációra: ne válaszoljon a gyanús e-mailekre!

§ Vizsgálja meg alaposan az e-mailt! Keressen következetlenségeket és értelmetlennek tűnő dolgokat, például furcsa nyelvezet, helyesírási hibák, sürgető hangnem, szokatlan formátumú csatolmány (.zip stb.).

§ Keressen nehezen észrevehető különbségeket a feladó címében: a nulla például „o" betűnek tűnhet! Vesse össze a küldő e-mail címét a bank korábbi üzeneteivel!

§ Legyen különösen körültekintő a mobileszközök használatakor! Telefonon vagy táblagépen nehezebb lehet észrevenni az adathalász kísérleteket. Nem lehet a gyanús hivatkozások fölé vinni az egérmutatót, és a kisebb kijelző miatt a nyilvánvaló hibákat is nehezebb észrevenni. A gyanús e-maileket jelentse bankjának: minden vállalat szívesen veszi az ilyen típusú támadásokról szóló információkat. Ha kétségei vannak, hívja fel a bankját!

§ Mindig tartsa naprakész állapotban szoftvereit, beleértve a böngészőt, a vírusirtó programokat és az operációs rendszert!

INTERNETES VÁSÁRLÁSOK

IDŐT TAKARÍTUNAK MEG
NEM KELL SORBAN ÁLLNI
ÁRAKAT HASONLÍTHATUNK ÖSSZE A KEDVEZŐBB ÁR MEGTALÁLÁSÁÉRT

-valótlan termékek megjelenítése a weboldalakon

-kicsalják a pénzt a vásárlótól /előre utalás/

-más terméket küld, nem az általunk megvásárolni kívántat

Mit tegyen, hogy elkerülje a hamis online ajánlatokat?

Ha lehet, belföldi kiskereskedelmi webhelyeken vásároljon, így nagyobb valószínűséggel kerülheti el, oldhatja meg az esetleges problémákat!

Nézzen utána a dolgoknak: vásárlás előtt olvasson értékeléseket, ismertetőket az adott termékről!

Kizárólag biztonságos fizetési szolgáltatásokkal fizessen! Gyanakodjon, ha pénzküldési szolgáltatás használatát kérik!

Csak biztonságos internetkapcsolat használatakor fizessen, ne használjon ingyenes vagy nyilvános wifihálózatokat!

Csak biztonságos készülékről fizessen! Gondoskodjon az operációs rendszer és a biztonsági szoftverek folyamatos frissítéséről!

Óvakodjon a hihetetlenül jó ajánlatokat kínáló reklámoktól vagy a csodát ígérő termékektől! Valószínűleg hamis, ha túl szépnek tűnik ahhoz, hogy igaz legyen.

Ha olyan felugró ablak jelenik meg a képernyőn, amely nem várt nyereményről tájékoztatja Önt, jusson eszébe, hogy ez nagy valószínűséggel egy rosszindulatú program!

Ha nem érkezik meg a termék, vegye fel a kapcsolatot az eladóval! Ha nem válaszol, vegye fel a kapcsolatot bankjával és az online piactér üzemeltetőjével!

MIBŐL LÁTNI, HOGY EGY WEBHELY BIZTONSÁGOS ?

Ellenőrizze, hogy a webhely címének beírására szolgáló mezőben látható-e a lakat, illetve figyeljen arra, hogy a webcím eleje https legyen, és csak biztonságos kapcsolatot használjon! Nyilvános wifi helyett saját mobilinternetre csatlakozzon!

Az interneten csak biztonságos webhelyeken fizessen!

VÉDEKEZÉS A KIBERCSALÁSOK ELLEN :

A legjobb védekezés az éberség!

Ellenőrizze rendszeresen online fiókjait, ne nyisson meg ismeretlen feladótól származó e-mailt, vagy fura, szokatlan hangvételű sms-ben érkezőt!

§ Ellenőrizze rendszeresen bankszámláját, és a gyanús tevékenységekről tegyen bejelentést bankjánál!

§ Az interneten csak biztonságos webhelyeken fizessen! Nyilvános wifi helyett saját mobilinternetre csatlakozzon! Használjon kétlépcsős azonosítási rendszert, vagy PAY-PALL-t.

§ Bankja soha nem kérdez olyan bizalmas információkat telefonon vagy e-mailben, mint az online fiókja hitelesítő adatai (felhasználónév, jelszó). Ha ilyen jellegű felszólítást kap, gyanakodjon, és mielőbb jelentse bankjánál!

§ Ne osszon meg senkivel telefonon vagy e-mailben banki vagy személyes adatot, beleértve a bankkártya-adatokat is!

§ Ne készítsen, küldjön vagy tegyen közzé közösségimédia-felületeken a bankkártyáiról készült fotót!

§ Ne telepítsen semmilyen alkalmazást a számítógépére vagy mobiltelefonjára más kérésére, még akkor sem, ha azt a bankja nevében teszik.

§ Minél sürgetőbb egy hívás vagy üzenet, annál gyanúsabb.

§ Ha egy ajánlat túl jónak tűnik ahhoz, hogy igaz legyen, szinte minden esetben csalás.

§ Nézzen utána, ellenőrizze az adott oldalt, mielőtt vásárol!

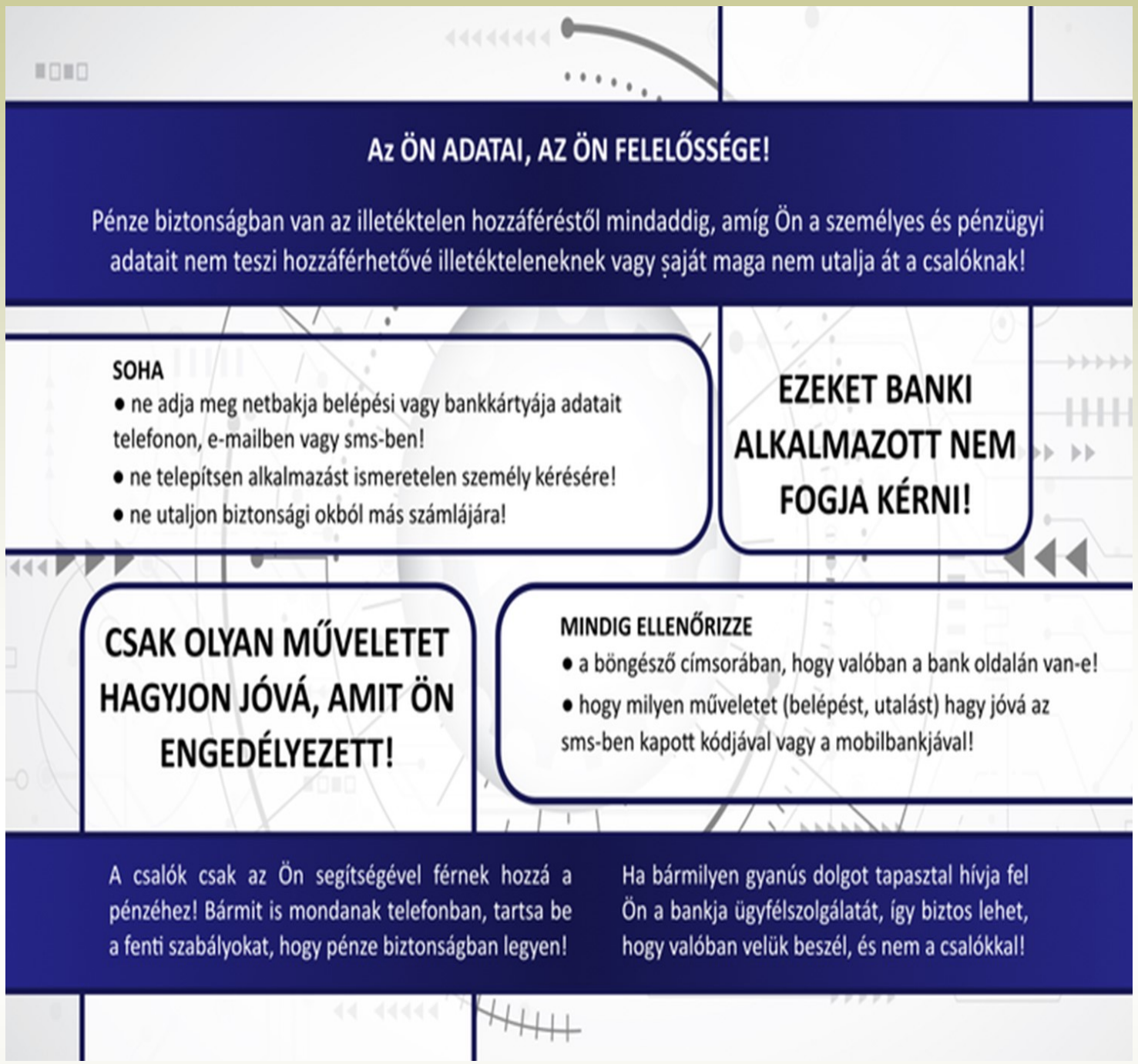
§ Mindig ügyeljen személyes adatai biztonságára, valamint azok biztonságos tárolására!

§ Szoftvereit rendszeresen frissítse, tartsa őket napra kész állapotban!

§ Gondolja át alaposan, mennyi személyes információt oszt meg a közösségimédia-oldalakon! A csalók az adatai és fényképei felhasználásával hamis személyazonosságot hozhatnak létre, vagy megpróbálhatják átverni.

§ Ha azt gyanítja, hogy megadta fiókja adatait egy csalónak, azonnal vegye fel a kapcsolatot a bankjával!

§ Ha megpróbálták megkárosítani, minden esetben tegyen bejelentést a bankjánál és a rendőrségen, még akkor is, ha a csalási kísérlet nem volt sikeres!



Segélyhívó szám: 112

Készítette: Komárom-Esztergom Megyei Rendőr-főkapitányság

Bűnügyi Osztály Bűnmegelőzési Alosztály

RENDŐRSÉG

POLICE