BŰNMEGELŐZÉSI HÍRLEVÉL

2023. január

BOLDOG ÚJ ÉVET KÍVÁN
a
Komárom-Esztergom Vármegyei Rendőr-főkapitányság Bűnügyi Osztály Bűnmegelőzési Alosztálya

Új év, régi és új problémák, új és régi trükkök.
A csalóknak mindig sikerül újabb és újabb ötletekkel előállni amikor az emberek átveréséről van szó. 2023. első hírlevelében ismételten az internetes és telefonos csalásokról, azok megelőzésének, valamint a vagyon elleni erőszakos bűncselekmények elkerülésének lehetőségeiről szeretnénk tájékoztatást adni. Beszéljenek Önök is róla, hogy elkerülhető legyen az áldozattá válás.
Továbbra is legyenek óvatosak és körültekintőek!

Ne adjunk esélyt a bűnözőknek!

RENDŐRSÉG
POLICE

VIGYÁZAT, CSALÓK!

Telefonon SOHA ne adja meg:
- bankkártyája vagy
- netbankja belépési adatait!

Ne telepítsen ismeretlen programot számítógépére, telefonjára!

Akkor sem, ha a bankja nevében, a bankja telefonszámáról telefonáló személy kéri!

Ha a hívó valamilyen bankkártyával vagy bankszámlával kapcsolatos problémára hivatkozik, szakítsa meg a hívást, és hívja fel Ön a bank ügyfélszolgálatát!

KIBERBŰNÖZÉS

A robbanásszerűen fejlődő digitális világ nagyon vonzóvá vált a kiberbűnözők 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.

Mint mindenki elött ismert, hogy az országban és megyénkben is szinte napi szinten indulnak bűntetőeljárások a kibertérben elkövetett csalások miatt. Az adathalász csalásoknak rendkívül sok formája ismert, az elkövetések módja, eszköze és célja alapján megfigyelhetők bizonyos általános jellemzők, amelyek alapján meg lehet határozni a leggyakoribb típusokat.

Annak érdekében, hogy ne legyünk a kiberbűnözés áldozatai ezért szeretnék pár hasznos tanácsot megosztani, melyet több szakmai internetes portálról gyűjtöttem össze. Kérlek figyeljetek oda a lent leírt ajánlásokra, lehetőség szerint szüleitek szeretteitek között is mondjátok el ezeket az ajánlásokat.

AZ ADATHALÁSZ CSALÁSOK LEGJELLEMZŐBB TÍPUSAI

PHISHING: ADATHALÁSZ BANKI E-MAILEK

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. A kiberbűnözők 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 a leírtak szerint.

Mit tehet?
Legyen különösen éber, ha egy „banki” e-mail bizalmas információkat kér, 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!

MEGHAMISÍTOTT BANKI OLDALAK
Az adathalász banki e-mailekben (phishing) 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, ha adathalász banki e-mailt kapott?
Soha ne nyissa meg a bank webhelyét e-mailben található hivatkozásra kattintva! Mindig gépelje be a hivatkozást, vagy használja a „Kedvencek” közé elmentett linket!
Használjon olyan böngészőt, amely lehetővé teszi a felugró ablakok blokkolását! Előugró ablakok általában bizalmas adatokat kérnek Önről. Ne kattintson rájuk és ne adjon meg személyes adatot az ilyen oldalakon!

HAMIS TRANZAKCIÓK JÓVÁHAGYÁSA

A bankok az online belépéshez és a tranzakciók jóváhagyásához kétlépcsős hitelesítést követelnek meg, az ügyfélnek a jelszón kívül egy másik módon is azonosítani kell magát. Ez az azonosítás történhet az ügyfél birtokában lévő kódgenerátorral, az ún. tokennel, amely a sorozatszámától és a használat időpontjától függően egy egyszer felhasználható, rövid ideig (1-2 perc) érvényes kódot szolgáltat, vagy az ügyfél által megadott telefonszámra érkező SMS-ben szereplő szám megadásával. Előfordulhat azonban olyan eset is, amikor a másodlagos hitelesítéshez elégséges csak a telefonon megjelenő felugró gombot megnyomni, vagy az ujjlenyomat-olvasóhoz hozzáilleszteni az ujjat. Ezek a jóváhagyási kérelmek megjelenhetnek az ügyfél telefonján akkor is, ha nem személyesen maga az ügyfél, hanem a bankszámlája felett rendelkező más személy kezdeményezte a belépést vagy a tranzakciót. Ha egy csaló próbál belépni vagy hamis tranzakciót indítani, az ügyfélnek ugyanúgy meg kell adnia a másodlagos hitelesítési adatokat ahhoz, hogy a belépés vagy a tranzakció sikeres legyen.

Mit tegyen, ha hamis azonosítási folyamatot észlel?

Mindig ellenőrizze, hogy a belépési kísérletet vagy a tranzakciót, melyet jóvá akar hagyni, valóban Ön, vagy az Ön által megbízott személy kezdeményezte! Sose hagyjon jóvá ismertlen kérést!

A kapott jóváhagyó SMS-ben ellenőrizze a jóváhagyásra váró műveletet, az összeget és a címzettet, ha szerepel benne!

A banki műveletek jóváhagyásához használt tokent sose hagyja felügyelet nélkül!

Használjon a mobiltelefonján képernyő-zárat!

Csak saját ujjlenyomatait regisztrálja a telefonjába!

Állítsa be úgy a mobiltelefonját, hogy az SMS-ben kapott üzenetek tartalma csak a képernyőzár feloldása után legyen látható!

VISHING: HAMIS BANKI HÍVÁSOK

A vishing (az angol „voice” és „phishing”, vagyis hang és adathalászat szavak kombinációja) olyan telefonos csalás, amelynél a támadó megpróbálja személyes, pénzügyi vagy biztonsági információi megosztására, vagy pénz átutalására rávenni az áldozatokat, akik általában banki ügyfelek. Tipikus formája a vishingnek, amikor a csaló az adathalász hívás során megpróbálja elhitetni a felhasználóval, hogy ténylegesen egy banki alkalmazottal beszél, és egy pénzügyi tranzakció során fellépett hiba vagy csalásgyanú miatt telefonál.

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!

SMISHING: HAMIS BANKI SMS-EK

A smishing (az angol „SMS” és „phishing”, vagyis SMS és adathalászat szavak kombinációja) olyan csalás, amelynél a támadó SMS segítségével próbál megszerezni személyes, pénzügyi vagy biztonsági információkat. Megbízható forrásnak álcázzák magukat, úgy tesznek, mintha egy bank, kártyakibocsátó, futárszolgálat, közműszolgáltató vagy valamilyen egyéb szolgáltató képviseletében jelentkeznének. Az üzenet arra kéri a címzettet – általában sürgető módon –, hogy nyisson meg egy weboldalra vezető hivatkozást, telepítsen egy alkalmazást, vagy hívjon fel egy telefonszámot a fiókja ellenőrzése, frissítése vagy újraaktiválása érdekében. A hivatkozás hamis weboldalra mutat, a telefonszámon pedig egy csaló jelentkezik, aki az adott cég munkatársának adja ki magát. Célja olyan információk megszerzése, amelyek segítségével aztán ellophatják a pénzét.

Mit tegyen, ha hamis banki SMS-t kapott?

Ne kattintson kéretlen szöveges üzenetekben érkezett hivatkozásokra, mellékletekre vagy képekre a küldő személyazonosságának ellenőrzése nélkül! Az ellenőrzéshez keressen rá a számra az interneten (ha csalásról van szó, valószínűleg nem Ön lesz az első), vagy hasonlítsa össze a számot az érintett szervezet hivatalos telefonszámával!

Ne hagyja, hogy siettessék! Végezze el a megfelelő ellenőrzést, bármennyi időbe is kerüljön!

Ha ismerős számról érkezik az SMS, az sem garancia arra, hogy megbízható. Lehetséges, hogy egy ismerőse már áldozatul esett a csalóknak, így fel tudják használni az ő telefonszámát és adatait.

Soha ne válaszoljon olyan SMS-re, amely a PIN-kódját, az online banki jelszavát vagy bármilyen más biztonsági azonosító adatát kéri!

Azonnal vegye fel a kapcsolatot a bankjával, ha azt gyanítja, hogy válaszolt egy smishing üzenetre és megadta banki adatait!

VÉDEKEZÉS A KIBERCSALÁSOK ELLEN

Felkészültséggel, odafigyeléssel és előrelátással csökkenthető annak az esélye, hogy ilyen típusú bűncselekmény áldozatává váljon: **legjobb védekezés az éberség!** A következő tippek a kibertámadások elleni védekezéshez, azok elkerüléséhez nyújtanak segítséget.

Ellenőrizze rendszeresen online fiókjait!

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

Az interneten **csak biztonságos webhelyeken fizessen**! 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!

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!

Csak akkor fizessen, ha biztonságos az internetkapcsolat! Kerülje az ingyenes vagy nyilvános wifit!

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.

Használjon biztonságos hitelesítést!

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!


A CSALÓK GYAKRAN
PRÓBÁLNAK MEG ÁTVERNI
BANKI DOLGOZÓNAK KIADVA
MAGUKAT SÜRGETŐ ÜGYEKBEN.
LAJOS
* AZ EGÉSZ UTCA TŐLE KÉR KÖLCSÖN SZERSZÁMOKAT
* SZÓVICCEKBŐL SOSEM ŰZ TRÉFÁT
* NEM DŐL BE A HAMIS BANKI HÍVÁSOKNAK

Tanácsaink a biztonságos mindennapokért

Sajnos az év eleje is tartogathat nem várt „vendégeket”, „meglepetéseket”. Könnyen válhatunk bűncselekmény, többek között akár rablás áldozatává, amely során az értékeket úgy veszik el az áldozatoktól, hogy fenyegetik vagy bántalmazzák őket. Nincs olyan módszer amellyel biztosan meg lehet akadályozni, de az alábbi ajánlások és tanácsok segíthetnek abban, hogy megnehezítsék az ingatlanokba bejutni kívánó rablók dolgát.

-A bűnelkövetők a könnyebb célpontokat részesítik előnyben.
-Szereljen fel riasztót, mozgásérzékelő rendszert.
-Használjanak komoly, több ponton záródó, modern bejárati ajtót. Visszatartó hatása lehet a kamerának és a mozgásérzékelő lámpáknak, csakúgy, mint bármilyen feliratnak, ami a ház folyamatos megfigyelésére és biztonsági rendszerére utal.
-Egy jó házőrző elrettentő hatású lehet.
-Családi ház esetén az ingatlant érdemes átlátható kerítéssel teljesen körbe keríteni.
-Az udvaron lévő növényzet legyen átlátható és alacsony. A bejárati ajtókat, ablakokat ne takarják!
-Távfelügyeleti rendszer használata jó lehetőség az idősebb korosztály számára.
-Ha rablás áldozatává válik, ne kíséreljen meg ellenállni! A testi épség a legfontosabb, az értékek pótolhatók.
-Jól figyelje meg az elkövetőt –pl.: magasság, hajszín, szemszín, egyedi azonosítók, ruházat, sérülések, stb.- amellyel a hatósági eljárásban segíteni tud az elkövető elfogásában.

Ha rablás, vagy egyéb bűncselekmény áldozatává vált, akkor a 112-es segélyhívó számon a lehető legrövidebb időn belül értesítsék a rendőrséget! Amennyiben lehetséges a helyszínen semmit ne változtassanak meg!

Készítette: Komárom-Esztergom Vármegyei Rendőr-főkapitányság

Bűnügyi Osztály Bűnmegelőzési Alosztály

bunmeg@komarom.police.hu