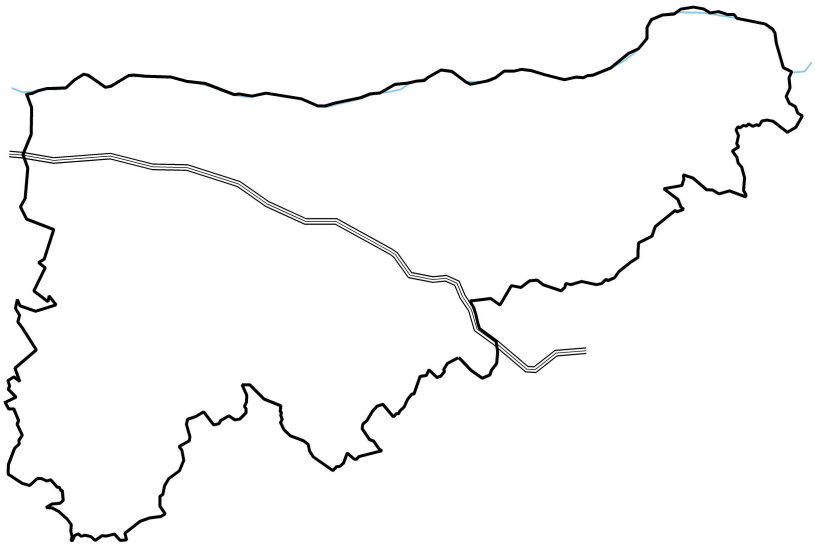
KOMÁROM-ESZTERGOM VÁRMEGYEI
RENDŐR-FŐKAPITÁNYSÁG



ELBIR - elektronikus lakossági bűnmegelőzési hírlevél

Komárom-Esztergom Vármegyei Rendőr-főkapitányság

Bűnügyi Osztály Bűnmegelőzési Alosztály

2024. január

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

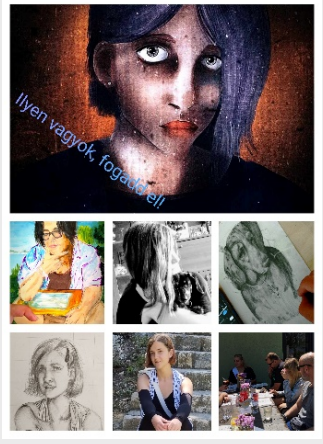
Új év, régi és új problémák, új és régi trükkök…
A csalóknak mindig sikerül újabb és újabb ötletekkel előállni, amikor az emberek átveréséről van szó. 2024. első hírlevelében az internetes és telefonos csalásokról, azok megelőzésének, valamint a vagyon elleni erőszakos bűncselekmények elkerülésének lehetőségeiről adunk tájékoztatás. Beszéljenek Önök is róla, hogy elkerülhető legyen az áldozattá válás!

Továbbra is legyenek óvatosak és körültekintők!

Ne adjunk esélyt a bűnözőknek!

Generációk találkozása

A szépkorúak kedves tanácsokkal látták el a fiatalokat, a gyermekek pedig rajzokkal, digitális alkotásokkal készültek arra a pályázatra, melyet a Komárom-Esztergom Vármegyei Rendőr-főkapitányság Bűnmegelőzési Alosztálya hirdetett meg. A beérkezett írásokban az idősek az egymás iránti figyelem, türelem fontosságára hívták fel az ifjabb korosztály figyelmét. A gyermekek alkotásaiból pedig jól látszik, hogy aktívan, tartalmasan töltik a szabad idejüket családi, baráti körben. Vágynak az elfogadásra, a közösségi életre, szívesen foglalkoznak képzőművészettel - legyen szó a hagyományos kézzel készült vagy a modern, informatikai eszközökkel létrehozott képekről.
A pályázat eredményhirdetésén dr. Vaczula József rendőr ezredes, bűnügyi rendőrfőkapitány-helyettes adta át a díjakat.
A legaktívabbak a Füzes Utcai Általános Iskola tanulói voltak, így közülük került ki a legtöbb díjazott: Varga Rajmund, Bús Rikárdó, Lévai Zsüliett, Horváth János, Krizsán Rebeka, Bús Jázmin, Balogh Zsüliett, Gyöngyösi Leila Zsuzsanna, Kis Brendon és Kiss László Gábor.
Díjat vehetett át a TSZC Bláthy Ottó Szakképző Iskola és Kollégium három tanulója: Tóth Ármin, Verbánszky Fanni és Juhász Mercédesz. A TSZC Mikes Kelemen Technikum és Szakgimnázium tanulója Götz Nikolett, valamint a Launai Miklós Református Iskola diákja Vojcsek Kata szintén elismerésben részesült.
A szépkorúak pályázatán Cserna Andrásné, Babolcsai Sándorné Teca, Linn Márton, Hegyi Jánosné és Belkovics Mária vehetett át egy-egy ajándékcsomagot.



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.

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?

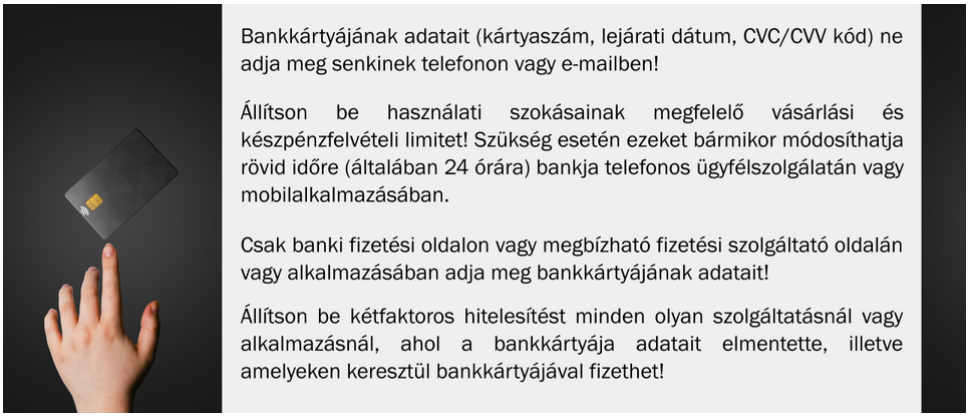
- Legyen különösen éber, ha egy „banki” e-mail bizalmas információkat kér, például az online banki jelszavát! A bankok kizárólag biztonságos módon, az online banki felületen kommunikálnak az ügyfelekkel, sosem kérnek bizalmas adatokat ilyen formában!
- Ne kattintson az üzenetben lévő hivatkozásokra, 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!
- Amennyiben a bank szeretné felhívni a figyelmet valamilyen fontos dologra, a figyelmeztetést az online banki felületen jeleníti meg.



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!

HAMIS ONLINE AJÁNLATOK, VÁSÁRLÁSOK

A fogyasztók és a vállalkozások egyre többet vásárolnak és adnak el az interneten. Az online ajánlatok sokszor valóban kedvezők, de óvakodjon a csalóktól!
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!

forrás: https://www.mnb.hu/fogyasztovedelem/digitalis-biztonsag/?gclid=Cj0KCQjwnbmaBhD-ARIsAGTPcfXCZfTq4eGMrP5wAKw0Pi0B-1fLljJvVLhSzI7KpFwKqUOR4tpWUiMaAgF_EALw_wcB

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!

Tisztelt Intézményvezetők, kedves Pedagógusok!

Az előző évekhez hasonlóan a Komárom-Esztergom Vármegyei Rendőr-főkapitányság Bűnügyi Osztály Bűnmegelőzési Alosztálya továbbra is vállalja, hogy térítésmenetesen tart eseti, bűnmegelőzési tájékoztató órákat diákoknak, valamint igény esetén tantestületeknek, szülőknek a következő témákban:

1./ A gyermek-és fiatalkorú jogsértések jellemzői, az elkövetővé és sértetté válás megelőzése /bűncselekmények és szabálysértések, a legjellemzőbb gyermekeket és fiatalokat érintő jogsértések beazonosítása, elkövetési formák az iskolákban, következmények/
A téma feldolgozásához ajánlott idő: 45 perc
Ajánlott célcsoport: általános iskolák 5-8., valamint középiskolák 1-2. évfolyamai
2./ Drogprevenciós tájékoztató óra /legális és illegális drogok veszélyei, kábítószerek és designerek jogi vonatkozásai, diszkóbalesetekkel való összefüggések/
A téma feldolgozásához ajánlott idő: 45 perc
Ajánlott korcsoport: általános iskolák 7-8., valamint a középiskolák 1-2-3. évfolyamai
3./ Az internet veszélyei, a biztonságos internet használat néhány alapvető szabálya.
A téma feldolgozásához ajánlott idő: 45 perc
A megcélozni kívánt korcsoport: általános iskolák 5-8., valamint középiskolák 1-2. évfolyamai
4./ Az iskolai erőszak /alapvető információk az iskolai erőszak formáiról, a jelenség veszélyei, lehetséges következmények, a probléma kezelésének lehetőségei/
A téma alapszintű feldolgozásához ajánlott idő: 45 perc
Ajánlott korosztály: általános iskolák 5--8. évfolyamai
5. / Személyes biztonság kisiskolásoknak /alapvető biztonsági szabályok kicsiknek; egyedül otthon, az utcán, mit tehet, ha elkeveredik valahol stb./
A téma alapszintű feldolgozásához ajánlott idő: 45 perc
Ajánlott korosztály: általános iskolák 1-2-3. évfolyamai
6./ A környezet-és állatvédelem alapjai rendőri szemmel
A téma feldolgozásához ajánlott idő: 45 perc
A megcélozni kívánt korcsoport: általános iskolák
Minden tájékoztatóhoz használunk kisfilmet, valamint Power Point prezentációt. A foglalkozások megtartásához minden esetben szükségünk van technikára: laptop, projektor, hangfal
7./ Kerékpárok ingyenes regisztrációja/Bikesafe program
Lehetőséget nyújtunk az iskolába kerékpárral járó gyermekek és dolgozók biciklijének ingyenes rendőrségi regisztrációjára. A BIKESAFE program országos nyilvántartásába a vármegyei rendőr-főkapitányságok ingyenesen beregisztrálják a kerékpárokat azok legfontosabb paramétereivel, fénykép-melléklettel. Amennyiben a kerékpárt eltulajdonítják, a hatóság rendelkezik a jármű körözésének kiadásához szükséges adatokkal.A kerékpáros regisztrációt igénylő iskolákkal a részleteket a jelentkezésük után telefonon egyeztetjük.
Mind a diákok, mind pedig a pedagógusok, szülők részére felajánlott tájékoztatókkal kapcsolatban fontos tudnivaló, hogy az írásban /lenti e-mail címre /megérkezett felkéréseket lehetőségeinkhez mérten, sorrendben próbáljuk kielégíteni, azonban előfordulhat, hogy csak hetek múlva jelentkezünk konkrét időpontot egyeztetni az iskolánál, lakóotthonnál, ezért türelmüket kérjük.
Kérjük, hogy az egyes témákhoz ajánlott korosztályokat legyenek szívesek figyelembe venni, hiszen a tanulók életkori sajátosságai szerint próbáltuk kiajánlani az egyes témaköröket.
A konkrét órák megtartására való megkereséseiket az alábbi e-mail címre várjuk:
bunmeg@komarom.police.hu

A csalók csomagküldő szolgáltatók nevében küldenek üzeneteket

A karantén-szabályok életbe lépése óta jelentősen megemelkedett az internetes vásárlások, valamint a csomagküldő szolgáltatók általi kézbesítések száma. A helyzet új lehetőséget teremtett a kiberbűnözőknek arra, hogy személyes adatokat szerezzenek meg, kompromittálják az elektronikus kommunikációt, és ezek felhasználásával további bűncselekményeket kövessenek el.

Az elmúlt napokban több lakossági bejelentést is érkezett a rendőrségre olyan SMS-üzenetekre hivatkozva, melyben a címzettet egy csomagküldemény rövid időn belüli érkezésére emlékeztetik. Az üzenet egy linket tartalmaz, amelyet megnyitva valamely csomagküldő szolgálat arculati elemeivel ellátott weboldal jelenik meg, azonban ott semmilyen funkció nem érhető el. Az oldal egyetlen célja, hogy az óvatlan látogató telefonjára vagy más okoseszközére egy kártékony kódot tartalmazó alkalmazást telepítsen, melynek segítségével az elkövetők hozzáférhetnek az eszközön tárolt adatokhoz. A támadás elsősorban Android-rendszert futtató eszközöket érint, melyeken települést követően az alkalmazás akár a netbank-applikációban tárolt adatokhoz is hozzáférhet.

Az áldozattá válás elkerülése érdekében fogadják meg az alábbi tanácsokat!

A támadás megelőzése céljából minden esetben ellenőrizze, hogy valóban attól a csomagküldő-szolgáltatótól kapja-e az értesítést, amelytől a csomagot várja!

Vegye figyelembe azt is, hogy a csomagküldő szolgáltatók saját, hivatalos weblapjukra irányítják át a felhasználókat a csomagkövetési rendszer eléréséhez! A legtöbb esetben a szolgáltatók közvetlenül az üzenetben is tájékoztatják a csomagkézbesítés várható időpontjáról, azt nem szükséges külön felületen ellenőrizni.

Az üzenetben érkezett hivatkozásra kattintás előtt minden esetben érdemes megtekinteni, hogy milyen címen nyílik meg az adott tartalom, és amennyiben ez már látszólag is eltér a szolgáltató valós oldalától, azt mielőbb zárják be!

Az androidos eszközökön nem javasolt az ismeretlen forrásból származó alkalmazások telepítésének engedélyezése.Ezen kívül célszerű lehet valamilyen biztonsági szoftver használata is, amely automatikusan blokkolja a kártékony tartalmak elérését.

Kisállattartók figyelmébe! Ha sürgős segítség kell

BŰNCSELEKMÉNY VAGY TULAJDON ELLENI SZABÁLYSÉRTÉS ÁLDOZATÁVÁ VÁLT? SEGÍTSÉGRE VAN SZÜKSÉGE? NINCS EGYEDÜL!

VAN SEGÍTSÉG!

Hívja a hét minden napján éjjel-nappal INGYENESEN elérhető **ÁLDOZATSEGÍTŐ VONALAT:**

06 80 225 225

Milyen segítséget kaphat?*

- Tájékoztatás
- Érzelmi támogatás, pszichológusi segítségnyújtás
- Jogi tanácsadás az elszenvedett sérelmekkel összefüggésben
- Gyakorlati és egyéb ügyviteli segítség
- Áldozati státusz igazolása más szerv által nyújtott ellátás, szolgáltatás vagy támogatás igénybevételéhez
- Azonnali pénzügyi segély a lakhatással, ruházkodással, élelmezéssel és utazással kapcsolatos, valamint a gyógyászati és kegyeleti jellegű rendkívüli kiadások fedezésére
- Állami kárenyhítés a szándékos személy elleni erőszakos bűncselekmények esetén

*A SEGÍTSÉGNYÚJTÁSI FORMÁK MIND INGYENESEN, SZOCIÁLIS RÁSZORULTSÁG VIZSGÁLATA NÉLKÜL VEHETŐK IGÉNYBE, UGYANAKKOR EGYES TÁMOGATÁSOK IGÉNYBEVÉTELE JOGSZABÁLYBAN MEGHATÁROZOTT FELTÉTELHEZ KÖTÖTT.

FŐVÁROSI ÉS MEGYEI KORMÁNYHIVATALOKBAN MŰKÖDŐ TERÜLETI ÁLDOZATSEGÍTŐ SZOLGÁLATOK:

ÁLDOZATSEGÍTŐ KÖZPONTOK:

WWW.VANSEGITSEG.HU

IGAZSÁGÜGYI MINISZTÉRIUM

ÁSK
ÁLDOZATSEGÍTŐ KÖZPONT

KORMÁNYHIVATALOK