

ÍGY ADJ MATTOT A KIBERBŰNÖZŐKNEK 6 LÉPÉSBEN!

 **NE ADD MEG** a személyes adataidat senkinek telefonon vagy e-mailben!

 Senki kérésére **NE TELEPÍTS FEL** semmilyen programot a telefonodra vagy a számítógépedre!

 Megfelelő jelszavakat válassz és soha **NE ADD MEG** azokat senkinek!

 **NE ADD MEG** a bankkártyád adatait, kizárólag csak banki fizetési felületeken!

 E-mail üzenetek esetén **ELLENŐRIZD** az üzenet feladóját!

 Mindig **ELLENŐRIZD** az általad meglátogatott weboldalak címét!

EGYÜTTMŰKÖDŐK:



A NEMZETI VÉDELMI SZOLGÁLAT
AZ ORSZÁGOS RENDŐR-FŐKAPITÁNYSÁG
ÉS AZ MBH BANK
BEMUTATJA



AZ INTERNET SÖTÉT OLDALA

EGY LÉPÉSEL A KIBERBŰNÖZŐK ELŐTT





MBH BANK

VEZÉR LEGYÉL ÉS NE GYALOG A KIBERTÉR SAKKTÁBLÁJÁN!

Üdvözlünk „Az internet sötét oldala – Egy lépéssel a kiberbűnözők előtt” című útmutatóban!

Hétköznapi életünk része az internet és a digitális eszközök használata, ami nagyban megkönnyíti az életünket, ugyanakkor veszélyekkel is jár. Hogy utóbbiakat jó eséllyel elkerüld, elengedhetetlen az alapvető biztonsági ismeretek elsajátítása, és az internet körültekintő, tudatos használata. Ezek birtokában a virtuális térben is biztonságban tudhatjuk magunkat és pénzügyeinket. Mint a sakban, az online térben is szükséges, hogy mindig egy lépéssel a ránk leselkedő veszélyek előtt járjunk!

Kiadványunkban ezeket a veszélyeket és a megelőzésükhöz szükséges információkat szeretnénk bemutatni, felkészítve Téged és családodat az online világ biztonságos használatára!

HAMIS WEBÁRUHÁZAK, ONLINE AJÁNLATOK

Az online ajánlatok sokszor valóban kedvezőek, de veszélyt is rejthetnek magukban!

Vevőként előfordulhat, hogy nem azt kapjuk, amit kifizettünk. Még ennél is rosszabb, ha nem a termékkel lesz gondunk, hanem a fizetés során megadott bankkártya adatainkkal élnek vissza.

A hamis áruházakat onnan lehet felismerni, hogy gyakran irreális mértékű akciókkal kívánják felhívni magukra a figyelmet.

A veszély jelentős, mivel ezek a weboldalak sokszor hónapokig működnek az interneten, mielőtt az első beérkezett panaszokat követően, elérhetetlenné teszik a szolgáltatók.

VÁSÁRLÓKÉNT

- Ellenőrizd az áruház vagy az eladó online értékeléseit, a többi felhasználó velük kapcsolatos tapasztalatait!
- Válaszd az utánvételi lehetőséget, vagy kizárólag a bankok, fizetési szolgáltatók saját felületein keresztül fizess!
- Állíts be számládhoz és kártyádhoz napi és tranzakciós limiteket, online vásárlási limitet vagy korlátozást!
- Online bankkártyás fizetéshez lehetőség szerint használj webkártyát! Ez egy olyan kártya, amelyet speciálisan online vásárlásokra használunk és csak a vásárláshoz éppen szükséges összeggel töltjük fel.
- Óvakodj a hihetetlenül jó ajánlatokat kínáló reklámoktól vagy a csodát ígérő termékektől!

A BANK NEVÉBEN ELKÖVETETT CSALÁSOK LEGGYAKORIBB FORMÁI

A színlelt banki telefonhívás során a csaló megpróbálja elhíttetni, hogy egy bank alkalmazottja, és egy, a számlánkon tapasztalt pénzügyi tranzakció, gyanús pénzmozgás miatt telefonál.

A gyanútlan áldozatot ráveszik, hogy a személyes, a bankszámla vagy a bankkártyáján lévő adatait is megadja, esetleg telepítse a csalók által kért programot. Arra is rávehetik, hogy utalja el a pénzét egy „védezt” számlára (valójában a csalóknak), vagy hagyja jóvá az általuk indított utalást.

A siker érdekében az elkövetők technikai trükkkel beállítják, hogy ne az a telefonszám jelenjen meg hívóként, amelyről a hívást valóban indították, hanem jellemzően egy olyan szám, amely a hívottnak ismerős lehet, például egy banké.

- Minél sürgetőbb a hívás, annál gyanúsabb! Lassíts és gondold át alaposan, hogy mit is kérnek valójában!
- A hívó hitelességének ellenőrzése érdekében, használd az interneten rendelkezésre álló forrásokat (tudakozó, internetes keresők, közösségi telefonszámmegosztó oldalak)!
- Gyanús telefonhívás esetén ne adj meg személyes adatokat, szakítsd meg a beszélgetést!
- Soha ne add meg a bankkártyád PIN-kódját, a hátoldalán található biztonsági kódot, online banki jelszavad vagy üzenetben kapott, egyszer használható kódodat! A bankok sosem kérik ezeket az információkat.
- Ne telepíts mások kérésére programot a számítógépedre, telefonodra!

HAMIS BEFEKTETÉSI LEHETŐSÉGEK

A befektetésekkel kapcsolatos legelterjedtebb csalások olyan területeken kínálnak vonzó lehetőségeket, mint például a részvények, a kötvények, a kriptovaluták, a tengerentúli ingatlanok vagy az alternatív energia.

Ezeket a befektetési lehetőségeket gyakran – a tudtuk és beleegyezésük nélkül – közismert emberek, sportolók, modellek képeivel és ajánlásával hirdetik.



- Ne vedd fel a telefont, ha híváskor ismeretlen külföldi hívószámot jelez ki, ne hívd vissza rögtön, először ellenőrizd azt!
- Különösen légy óvatos akkor, ha olyan külföldi számról hívnak, ahol nem él ismerősöd, vagy ha a hívás 2-es vagy 5-ös országhívóval kezdődik.
- Az ismeretlen előhívószámokról érkező külföldi hívások egyedileg letilthatók a készülék beállításáiban. Mindig gyanakodj, ha:

a kéretlen telefonhívásokat folyamatosan kapod;

gyors megtérülést ígérnek és biztosítanak arról, hogy a befektetés biztonságos;

az ajánlat csak Neked szól, korlátozott ideig él, ezért lemaradhatsz róla!



HAMIS SMS ÉS E-MAIL ÜZENETEK

A támadók SMS vagy e-mail üzenetek segítségével próbálnak megszerezni személyes, pénzügyi vagy biztonsági adatokat, információkat.

Megbízható szolgáltatónak álcázzák magukat, úgy tesznek, mintha egy bank, csomagküldő, közműszolgáltató stb. képviselőjében jelentkeznének, amelyektől egyébként is szoktunk értesítéseket, számlákat kapni.

Az üzenet általában sürgető hangvételű, és arra kéri a címzettet, hogy kattintson a kapott linkre, telepítsen egy alkalmazást, vagy hívjon fel egy telefonszámot. Ezt jellemzően fizetési késedelem miatti befizetés, csomagátvételi határidő hosszabbítása, online fiók ellenőrzése, frissítése vagy újraaktiválása érdekében kérik.

Ezek a webhelyek megtévesztésig hasonlíthatnak a mintának használt valódi oldalakhoz.

NE HAGYD HOGY SIETTESSENEK! NE CSELEKEDJ MEGGONDOLATLANUL!

- Vizsgáld meg alaposan az üzeneteket! Gyanúra ad okot, ha a megszólítás általános (nem névre szóló), ha az üzenet vagy levél szövege magyartalan, és tele van helyesírási hibákkal.
- A csalók leggyakrabban valami rendkívüli jutalommal kecsegtetnek, büntetéssel vagy a szolgáltatásból történő letiltással, kizárással fenyegetnek, illetve a kíváncsiságunkra próbálnak hatni.
- Ha fizetésre figyelmeztető üzenetet kapsz, ne kattints a linkre, hanem a szolgáltató oldalára belépve ellenőrizd, van-e tényleges tartozásod!
- Ha nem vársz csomagot, vagy nincs az adott szolgáltatónál előfizetésed, akkor biztos lehets benne: csalási kísérlettel állsz szemben!

ELADÓK ÁTVERÉSE AZ ONLINE PIACTEREKEN

Az internetes felületeken, azaz az online piactereken, egyszerűen bonyolíthatjuk egymás közötti adásvételeinket.

Az eladót a csalók üzenetben arról tájékoztatják, hogy a termékét megvették, és a kifizetett összeget már csak „fogadnia kell” az üzenetben küldött link segítségével.

Amikor az eladó gyanútlanul rákattint a linkre, akkor egy, a csalók által készített, de egy csomagküldő szolgálathoz nagyon hasonlító, hamis weboldalon találja magát. Itt elkéri a bankkártyaadatait, vagy ki kell választania a számlavezető bankját, és arra kattintva megadni a saját banki belépési adatait.

A hamis oldal a csalóknak továbbítja az adatokat, az óvatlan ügyfél (eladó) megkapja az egyszer használható bejelentkezési kódot (pl. SMS-kódot), és azt is megadja az elkövetőknek.

A csalók így bejutnak az ügyfél banki profiljába, és a számlán lévő pénzt azonnal továbbutalhatják, vagy vásárlásokat kezdeményezhetnek.

MIT TEGYÉL, HOGY NE VÁLJ ILYEN CSALÁS ÁLDOZATÁVÁ?

- Legyél tisztában azzal, hogy eladóként Te pénzt csak fogadsz, nem küldesz.
- Online piactereken vagy más, interneten keresztül értékesítésnél az a legbiztonságosabb, ha a fizetést a bankszámládra kéred, amihez nem kell más, mint a neved és bankszámlaszámod megadása!
- Gondold végig, ahhoz, hogy bankszámládra pénzt utaljanak, nincs szükség semmilyen programra, és a netbankodba sem kell bejelentkezned!
- Soha ne adj meg senkinek bankszámla- vagy kártyaadatokat, az internetbankhoz tartozó belépési adatokat és jelszavakat!

VAGYONT ÍGÉRŐ CSALÁSOK

A vagyont ígérő csalás, közismertebb néven „nigériai típusú” csalás, a megtévesztés egyik legrégebbi formája, amely kezdetben hagyományos, postai úton érkezett, majd az e-mail terjedésével az online térben szedi áldozatait.

A nigériai csalások során az elkövetők valamilyen megtévesztő kommunikációval – jellemzően e-mailben – pénz utalására veszik rá az áldozatukat.

Ezekben a levelekben az elkövetők segítséget kérnek jogtalanul elvett örökség visszaszerzéséhez, vagy valamilyen okból átmenetileg hozzá nem férhető összeg megszerzéséhez.

Közösségi- és online társskereső oldalakon terjed a nigériai csalás azon változata is, amelynél az elkövető romantikus kapcsolatot épít fel leendő áldozatával, mielőtt valamilyen érzelmekre ható történettel pénzt kérne az áldozattól.

A segítség kizárólag egy bizonyos pénzösszeg átutalását jelenti, amiért később busás jutalmat ígérnek, amelyet a károsultak végül nem kapnak meg, a befizetett összeget viszont elveszítik.

MIT TEGYÉL, HOGY NE VÁLJ ILYEN CSALÁS ÁLDOZATÁVÁ?

- Ne kezdeményezz fizetést ismeretlentől kapott levélben érkező felszólításra!
- Kéretlen levél esetén figyeld a nyelvezetet: a csaló levelekre jellemző a nyelvtani és fogalmazásbeli hiba.
- Sok esetben viszont éppen ez támasztja alá a csaló történetét: a „tört magyarság”, a megtévesztő történetben szereplő külföldi levélíró kísérlate, hogy magyarul próbáljon meg segítséget kérni. Ha ilyen levelet kapsz, legyél megfontolt és gyanakvó!
- Nem reális, hogy ismeretlenek a könnyű meggazdagodás lehetőségét ajánlják fel másoknak.
- Semmilyen körülmények között ne adj meg bizalmas információkat e-mailben vagy más úton érkező felkérésre!

GYEREKEK ÉS AZ ONLINE BIZTONSÁG

A gyerekeknek az online világgal történő megismertetése elengedhetetlen, mivel az internet rengeteg lehetőséget kínál, de sajnos kockázatokkal is járhat a fiatalabb felhasználók számára.

A kíváncsiság, a nyitottság és a feltétel nélküli bizalom különösen sebezhetővé teheti őket, a káros tartalmakon túlmenően, különféle bűncselekmények áldozatává válhatnak.

Fontos, hogy az online térben is fogjuk a kezüket!

MIT TEGYÉL, HOGY MEGVÉDD GYERMEKEDET AZ ONLINE TÉRBEN?

- Használj olyan programokat, amelyek segítenek ellenőrizni a gyermeked online tevékenységét! Ha szükséges, ehhez kérd szakemberek segítségét!
- Állíts fel szabályokat és korlátokat az online időtöltésre! Segíts nekik megérteni, miért fontos ezeket betartani!
- Tanítsd meg nekik, hogy soha ne osszanak meg személyes adatokat ismeretlenekkel, ne nyissanak meg gyanús linkeket!
- Magyarázd el nekik, hogy ne osszanak meg magukról, lakókörnyezetükről, iskolájukról, barátaikról fényképeket, mert ami felkerül az internetre, az ott is marad, mint egy digitális lábnyom!

Beszélg nyíltan gyermekeddel az online kockázatokról!

RENDŐRSÉG NEVÉBEN KÜLDÖTT HAMIS ÜZENETEK

Az adathalász csalók már a Rendőrség nevével visszaélve is megpróbálnak személyes és banki adatokhoz hozzájutni.

Az elkövetők egyik módszere, hogy rendőri vezetők nevével, a Rendőrség arculati elemeit használva, hivatalosnak látszó e-mail üzenetben, bírság megfizetésére szólítanak fel.

Áldozataikat büntetőeljárással, elfogással fenyegetik, amennyiben a fizetési felszólításnak nem tesznek eleget.

Gyakori módszer továbbá, hogy megtévesztő SMS-ben, be nem fizetett közigazgatási bírságra, tilosban parkolásra hivatkozva keresik meg az érintetteket, elküldve részükre egy adathalász linket.

A linket megnyitva egy hamis oldalra jutnak, ahol a gyanútlan sértett megadja a személyes és a bankkártyán szereplő adatait a bírság kifizetése érdekében, azonban ezzel lehetővé teszi az elkövetőknek a bankszámláján lévő pénz megszerzését.

MIT TEGYÉL, HOGY NE VÁLJ ILYEN CSALÁS ÁLDOZATÁVÁ?

- A Rendőrség kizárólag hivatalos úton (ügyfélkapun, postán keresztül) kommunikál az állampolgárokkal.
- Ne kattints a gyanús levelekben lévő linkre, azonnal töröld az üzenetet!
- Figyeld az üzenetek nyelvezetét, mivel a csaló levelekre jellemző a nyelvtani és fogalmazásbeli hiba!
- Fontos, hogy a Rendőrség e-ügyintézési portálja kizárólag a

<https://ugyintezes.police.hu>

honlapcím beírásával érhető el.

