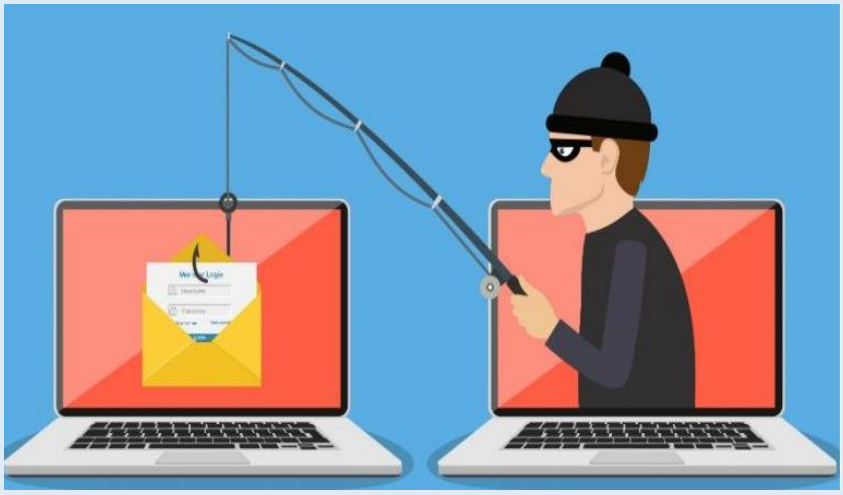
Hírlevél

A Veszprémi Rendőrkapitányság Bűnmegelőzési Melléklete – 2023. 4. szám

TARTALOM

Idei első hírlevelünkben utaltunk rá, hogy ebben az évben elsősorban az online csalások különféle módszereit és módszercsoportjait járjuk körül. Ebben a számban a nyereményjátékokhoz köthető és a nigériai csalások egyes módszereit ismertetjük. Ezek a csalási módszerek több mint száz éve velünk vannak. A 19. század végén még levélben érték el áldozataikat a csalók, majd az internet térhódításával újra reneszánszát éli a módszer. Napjainkban az online térben nagy számban kiküldött e-mailek, üzenetek jelentik a csalit, amelyre válaszolva a sértett „horogra akad”.



Harmadik cikkünkben a külföldi biztonságos internetezéshez adunk tanácsot. A nyilvános, ingyen WiFi használata vonzó lehet, mert ilyenkor nem a telefonelőfizetés adatforgalmi kerete fogy. De előfordulhat, hogy a bűnözők a helyszínre jellemző névvel látnak el és osztanak meg internetelérési pontokat. Amennyiben felcsatlakozunk egy nem megbízható hálózatra, minden internetes forgalmunk a támadó eszközén megy keresztül, így illetéktelenek érzékeny adatokhoz, banki információkhoz is hozzáférhetnek.

Online csalás: a nyereményjáték módszer

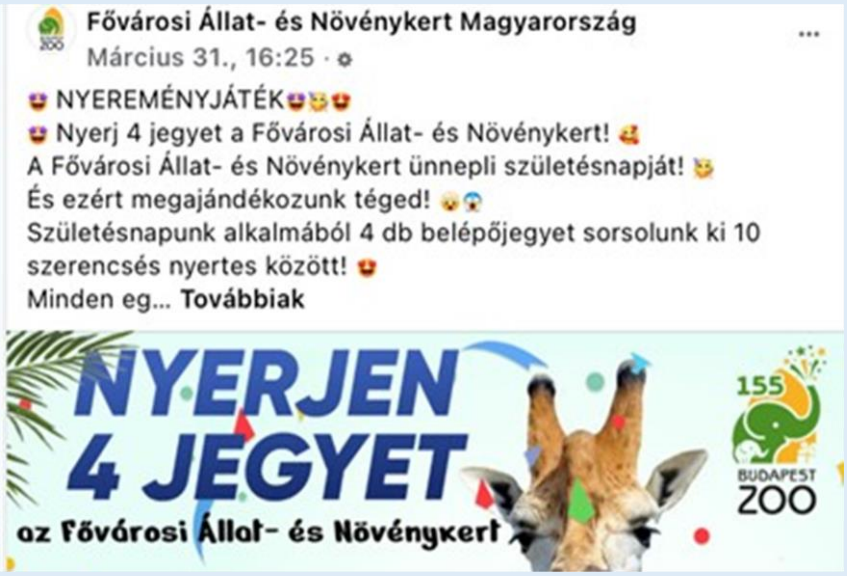
Leggyakrabban a közösségi oldalakon keresztül küldött üzenetekben vagy e-mailekben, esetleg felugró ablakokon keresztül találkozhat a felhasználó online nyereményjáték csalásokkal. A bűnözők nagy számban küldenek ki üzeneteket abban a reményben, hogy valamelyik címzett végül válaszol nekik. Céljuk, hogy a felhasználótól pénzt csaljanak ki, vagy megszerezzék a bankkártyájának, a netbankjának belépési adatait.

A módszer az utóbbi évtizedben folyamatosan tovább fejlődött. Néhány éve még az elkövetők jellemzően azzal keresték meg a kiszemelt áldozatot, hogy valamilyen nyereményjátékon nyert, de a nyeremény véglegesítéshez szükség van arra, hogy feltöltse egy telefonkártya egyenlegét, vagy egy meghatározott kódot SMS-ben küldjön el egy telefonszámra (ez szintén egyenleget tölt fel a küldő számlájának terhére).

Napjainkban már gyakoribb, hogy egy nyeremény (például mobiltelefon, játékkonzol) átvételéhez kérik egy kisebb összeg átutalását szállítási, vagy kezelési díj címén. Máskor nem a díj átutalását kérik, hanem a bankkártya adatokat, azzal, hogy arról vonják le a költségeket. Ez utóbbi esetben nem csak a jelzett összeget, hanem akár a teljes egyenleget is elkölthetik. A felkínált nyeremény lehet utazás, autó, belépőjegy, de olykor még kriptovalutával is kecsegtetik a kiszemelt áldozatot, akitől mindenféle költségek megfizetését kérik, mindaddig, amíg a megtévesztett hajlandó utalni. Amikor végül rájön, hogy hiába fizetett, csalókkal van dolga, a bűnözők elérhetetlenné válnak.

A másik módszer, amikor a bűnözők egy nagy presztizsű cég, vagy szolgáltató oldalát lemásolva hirdetnek nyereményjátékot, amelyre akár több százan is bejelentkeznek, kifizetve a „regisztrációs díjat”. Idén tavasszal a Fővárosi Állat- és Növénykert hivatalos Facebook-oldalával elkövetett visszaélés kavart fel nagy port. A csalók a fővárosi állatkert oldalához hasonló álprofilt hoztak létre a legnépszerűbb közösségi portálon, szándékosan igyekezve azt a benyomást kelteni, mintha az intézmény hivatalos Facebook-oldala lenne. A megtévesztés érdekében az eredeti oldalról átmásolt posztok jelentek meg a kamuoldalon.
Az álprofil URL címe csaknem azonos volt, azonban az „állatkert” szó második „l” betűje helyett nagy „i” betű szerepelt. Az oldal létrehozása után nyereményjátékot hirdettek, amelynek valódi célja az adathalászat és az „ügyintézési díjak” bezsebelése volt.

Fővárosi Állat- és Növénykert a hivatalos Facebook-oldalán és a honlapján is közzétett erre vonatkozó figyelmeztetést, de a médián keresztül szintén felhívták az emberek figyelmét arra, hogy ne dőljenek be a szándékos megtévesztésnek.
A csaló poszt többszáz embert megtévesztett, akik megadták személyes adataikat, majd kifizették a nyeremény postaköltségét és várták a jegyeket…



A nyereményjáték csalás módszerről összefoglalva elmondható, hogy a gyanútlan játékossal a bűnözők kapcsolatot keresnek, majd közlik vele a nyeremény hírét. Gyakran a közösségi oldalakon keresztül, chat alkalmazásban szólítják meg, ezért mindig kezeljük kellő gyanakvással az ismeretlenektől így érkező üzeneteket. Különösen azokat, amelyekben csak egy rövid, figyelemfelhívó vagy sürgető üzenet szerepel! A nyeremény eljuttatásához valamilyen okra hivatkozva postázási címet, telefonszámot kérnek, s így folytatják az adathalászatot, profilozást. Ezután a bűnözők költségekre hivatkoznak, például problémaként jelzik, hogy a postaköltséget kell kifizetni, amelyhez bankkártyás fizetést kérnek, akár szintén hamis oldal közbeiktatásával.

Amennyiben egy ismert cég, vagy szolgáltató által meghirdetett nyereményjátékra szeretne jelentkezni, győződjön meg az oldal valódiságáról. Ellenőrizze, hogy hány ember követi az adott közösségi média profilt, ki hozta létre és ezen időpont óta folyamatosak-e a posztok, vagy csak néhány jelenik meg az utóbbi időszakból.

Ha pedig valaki nem regisztrált be egy nyereményjátékba, akkor nincs is rá esély, hogy nyerjen. Legyen gyanakvó, ha olyan üzenetet kap, amely váratlan nyereményről szól és törölje az üzenetet!

A klasszikus „nigériai” csalás új köntösben

A „nigériai” típusú csalás a megtévesztés egyik legrégebbi, 19. század végén már elterjedt formája. Kezdetben hagyományos, postai úton, majd faxon terjedt, de a telekommunikációs eszközök fejlődésével, valamint az internet és az e-mail terjedésével ennek a csalástípusnak is az online tér vált a fő platformjává.

A hamis levelekben, megkeresésekben jellemzően segítséget kérnek az elkövetők: menekültek vagyonának visszaszerzéséhez, jogtalanul elvett örökség, valamilyen okból átmenetileg hozzá nem férhető összeg megszerzéséhez stb. Közösségimédia-oldalakon, online társkereső portálokon terjed a nigériai csalás azon változata, melynél az elkövető romantikus kapcsolatot épít fel leendő áldozatával, mielőtt valamilyen megható történettel pénzt kér tőle.

A megtévesztő történetet valódinak látszó, de hamis közösségimédia-profillal és eredetinek tűnő, de szintén fiktív iratokkal igyekeznek alátámasztani. Annak érdekében, hogy a történet hihetőbb legyen, előfordulhat, hogy a csalók nemzetközi átutalást kezdeményeznek, amit aztán visszavonnak, így mutatva, hogy az összeg valójában rendelkezésre áll, csak a levélben jelzett adminisztratív nehézség áll a kifizetés útjában. A levélben kért segítség kizárólag egy bizonyos pénzösszeg átutalását jelenti. Mindezért későbbi busás jutalmat ígérnek, amit azonban a károsultak végül nem kapnak meg, de a befizetett összeget is elveszítik. Szintén bevett forma, hogy a vagyon kimenekítéséhez a címzettnek meg kell adnia a bankszámlaadatait, aminek az eredménye természetesen nem az, hogy pénzösszeg érkezik rá, ellenkezőleg: az elkövetők immár hozzáférnek a bankszámlához, így akár le is nullázhatják azt.

Kéretlen levél esetén figyelje a nyelvezetet: a nigériai levelekre jellemző a pongyola megfogalmazás, a számtalan nyelvtani és stilisztikai hiba. Ám sok esetben épp ez támasztja alá a történetet: a „tört magyarság”, a megtévesztő történetben szereplő külföldi levélíró kísérlete, hogy magyarul próbáljon meg segítséget kérni. Ha ilyen levelet kap, legyen megfontolt és gyanakvó!

Ne higgyen e-mailben érkező, már-már romantikus történeteknek! Nem reális, hogy ismeretlenek a könnyű meggazdagodás lehetőségét ajánlják fel másoknak. Ha ilyen tartalmú levelet kap, gyanakodjon!

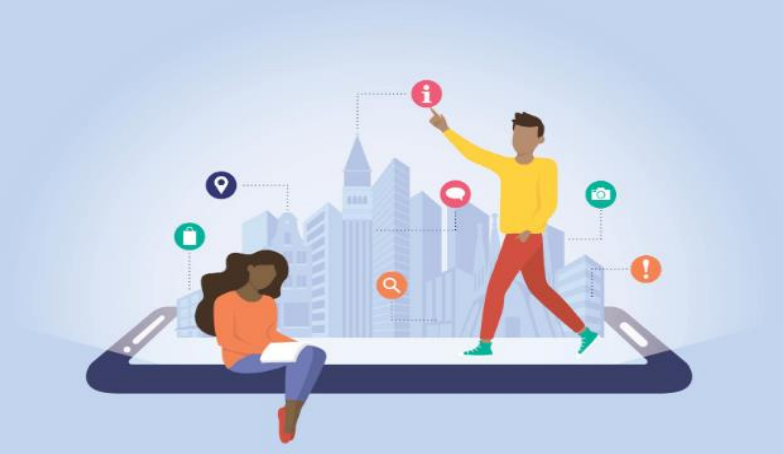
A Kiberpajzs tanácsai külföldi nyaraláshoz

A Nemzeti Kibervédelmi Intézet nyaralási tanácsai segítségével megismerhetjük, hogy mire figyeljünk utazás és nyaralás során, amikor kifejezetten hasznosnak bizonyul, ha hozzáférünk az internethez, legyen szó akár útvonaltervezésről, böngészésről vagy szeretteink eléréséről. Legyünk bármennyire is kitettek az utazás feltételeinek, mindig érdemes a biztonságos internethasználatra törekedni.

Nyilvános Wi-Fi

Manapság már bárhová megyünk nagyon gyorsan találhatunk publikus internetet elérést. Nagyon csábító lehet, hogy ingyen és bérmentve tudjuk az internetet böngészni kávénk szürcsölése mellett, de kétszer is gondoljuk meg, hogy rácsatlakozzunk-e az első szabad elérésű Wi-Fi-re, ugyanis nem minden az, aminek látszik! Gyakori, hogy a kiberbűnözők a helyszínre jellemző névvel látnak el és osztanak meg internet elérési pontokat. Amennyiben felcsatlakozunk egy nem megbízható hálózatra, minden internetes forgalmunk a támadó eszközén megy keresztül. Ha az üzenetek nincsenek levédve titkosító protokollokkal (mint például HTTPS), úgy olyan szenzitív információk is lehallgathatóvá válnak, mint a jelszavak, a felhasználónevek, vagy a banki azonosítók.

A nyilvános hálózatok esetében az is problémás lehet, hogy a bűnözők számára könnyű elérést biztosíthatunk az eszközeink kompromittálásához. Ilyenkor hálózati fájlmegosztás által sokkal kitettebbek lehetünk káros kódoknak vagy bármilyen rendszerünk sérülékenységeit kihasználó tevékenységeknek. Mindezekből adódóan javasoljuk a nyílt internet használat mellőzését.



Mobilinternet és VPN

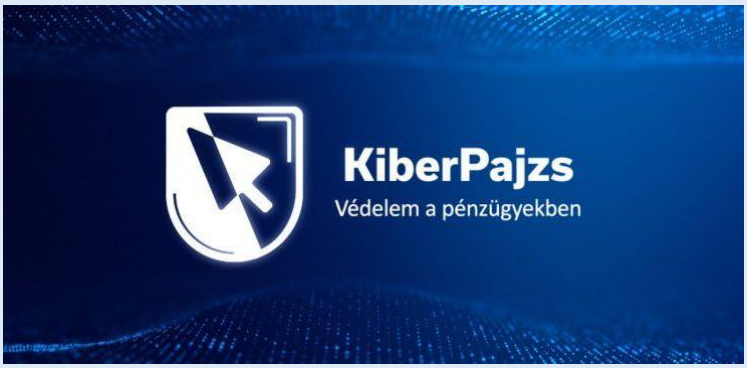
A nyílt hálózatok veszélyeinek talán legegyszerűbb és leghatásosabb módja a mobilinternet használata. Ilyenkor ugyanis a szolgáltatónk egy teljesen privát és megbízható hálózati kapcsolatot biztosít a mobil eszközünk és a torony között. Külföldi utazás esetén is érdemes lehet mobilszolgáltatónknál megismerni a roaming szolgáltatások lehetőségeit. A mobilinternet a biztonság mellett egyfajta rugalmasságot és kényelmet is biztosít, amellyel a mai eszközök többségével meg tudjuk osztani az internetet más eszközeinkkel is. Így szükség esetén tudunk saját vezeték nélküli hálózatot biztosítani bárki számára.

Érdemes ilyen esetben VPN alkalmazást is használni. A virtuális privát hálózat vagyis a VPN képes egy teljesen titkosított csatornát kiépíteni, amelyet a végpontokon kívül senki más nem tudja feloldani – beleértve a beékelődött támadót se. Így biztonságba tudhatjuk az elküldött üzeneteink és személyes adataink bizalmasságát. Természetesen előfordulhat az az eset is, hogy mobil adatforgalom hiányában rászorulunk az ingyenes nyílt hálózatokra, ám ebben az esetben csak böngészésre használjuk a net-hozzáférést, internetes fiókokba sose jelentkezzünk be!

(Forrás: Kiberpajzs.hu)

Kiberpajzs

KiberPajzs néven közös oktatási és kommunikációs együttműködésről döntött a **Magyar Nemzeti Bank, a Magyar Bankszövetség, a Nemzeti Média- és Hírközlési Hatóság, az Nemzetbiztonsági Szakszolgálat-Nemzeti Kibervédelmi Intézet, illetve az ORFK**. A digitális pénzügyi bűnözők ma elsősorban a fogyasztók érzelmi manipulálásával, illetve megtévesztésével támadnak. Így a KiberPajzs szervezői a lakossági ügyfelek pénzügyi tudatosságának erősítése, a kiberkockázatok minél hatékonyabb kezelése érdekében fognak össze.



Az együttműködés honlapja a **kiberpajzs.hu**, melyen már jelenleg is számos csalás módszerének leírása megtalálható, melyek segítik a weblap látogatóját abban, hogy idejekorán felismerje, ha sérelmére bűncselekményt kísérelnek meg elkövetni. Ezen bűncselekmények felderítése, sértettjeik kártalanítása még bizonytalan, az egyedül hatékony megoldásnak a megelőzés tűnik. A támadások elhárítására pedig csak azok képesek, akik kellőképpen felkészültek a témában.

A Veszprém vármegyei rendőrség elnevezésű Facebook oldalon a Veszprém Vármegyei Rendőr-főkapitányság Sajtószolgálata rendszeresen megosztja az aktuális híreket, közleményeket. Ezek között az online csalások is szerepelnek, továbbá az azok megelőzését segítő információk.

Információkéréssel forduljon hozzánk bizalommal!

Veszprémi Rendőrkapitányság
8200 Veszprém, Bajcsy-Zsilinszky utca 2.
Tel: 06-88/428-022
E-mail: **rauszi@veszprem.police.hu**

A kiadásért felel: Rausz István r. ezredes rendőrkapitány

Tájékoztatjuk, hogy a Rendőrségi Adatvédelmi Nyilvántartás szerinti adatvédelmi tájékoztató a következő linkről letölthető:
http://www.police.hu/hu/a-rendorsegrol/adatvedelem/altalanos-informaciok
Tájékoztatjuk továbbá, hogy amennyiben a jövőben nem kívánja hírlevelünket megkapni, a Veszprémi Rendőrkapitányság rauszi@veszprem.police.hu e-mail címre küldött üzenetével kérheti e-mail címe törlését.