



Rendőrségi felhívás!

Kiberbűnözők telefonálnak a Microsoft nevében

Legyen óvatos a kéréstlen telefonhívások esetén! Nem mindig igaz, amit a kijelzőn látunk!

Több bejelentés is érkezett a KiberPajzs alapító partneréhez, az NBSZ NKI-hoz, a Microsoft nevével visszaélő angol nyelvű telefonhívásokkal kapcsolatosan.

A csalók azt állítják, hogy a Microsoft technikai támogató részlegéről telefonálnak, és arról szeretnék meggyőzni az áldozatot, hogy számítógépét valamilyen veszély fenyegeti (például, hogy az vírusos lett), amit segítenek elhárítani. A hívások során a csalók angolul beszélnek, azonban a hívószámot meghamisítják (ezt a csalási technikát [hívószám-spoofing](#)-nak is nevezik), ami magyar telefonszámként jelenik meg a hívott félnél.

Az NBSZ NKI-hoz jelentett esetekben a csalóknak jellemzően nem sikerült rászedniük a hívott feleket, akik többnyire egyszerűen csak bontották a vonalat, azonban így is volt olyan, aki csak akkor kapcsolt, amikor a csalók már a bankkártya adatait kérték tőle. Érdemes tehát felhívni a figyelmet arra, hogy a kiberbűnözők nemcsak bankok dolgozóinak, hanem call centerek (ügyfélszolgálat) munkatársainak is kiadják magukat.

Mire megy ki a játék?

Hasonlóan az **AnyDeskes** csalásokhoz a csalók megpróbálják rávenni az áldozatot arra, hogy telepítsen egy programot az eszközére. A mostani esetek során ez nem az AnyDesk, hanem a **RemoteApp** volt, egy azon szoftverek közül, amivel egy csaló átveheti az irányítást az áldozat számítógépe felett.

Ezzel a hozzáféréssel telepíthet akár káros programokat is (éppen ezzel fertőzve meg a számítógépünket), így még könnyebben győzi meg az áldozatot arról, hogy a számítógépen kritikus problémák vannak, amelyeket sürgősen javítani kell. Ezután előbb-utóbb arra terelik az áldozatot, hogy adja meg bankkártya adatait vagy lépjen be a netbankjába, amihez így a csaló is hozzáférhet.

Mire figyeljünk?

- A Microsoft soha nem kezdeményez kéréstlen telefonhívásokat, hogy személyes vagy pénzügyi adatokat kérjen, illetve, hogy technikai segítséget adjon a számítógép javításához, és soha nem fogja kérni, hogy kriptovaluták (például Bitcoin) vagy ajándékkártyák formájában fizessünk a támogatásért.
- Amennyiben kicsit is gyanús egy bejövő hívás, a legegyszerűbb védekezési mód, ha azonnal bontjuk a vonalat, és ha mégis kétség merült fel bennünk, hívjuk fel a szolgáltató hivatalos ügyfélszolgálatát!
- Fontos, hogy a szolgáltatót ne azon a számon hívjuk vissza, amiről az imént kerestek bennünket, hanem például keressünk rá a szolgáltató weboldalára, ahol a kapcsolat/kontakt menüpont alatt vagy az oldal impresszumában szereplő elérhetőséget keressük!
- Azt se fogadjuk el, ha az ügyintéző felajánlja, hogy „átkapcsol” minket egy másik kollégához, ez csupán egy trükk, és a maguk is „call centerként” működő kiberbűnözők egy másik tagjával fogjuk folytatni a beszélgetést!
- Végezetül: ne telepítsünk mások kérésére programot se a számítógépünkre, se a telefonunkra!

A csalásokfajtákról tudjon meg többet a <https://kiberpajzs.hu/csalastipusok> oldalon.

Védje, őrizze értékeit, szeretteit biztonsági kamerával!



Otthonunkat, távolabb lévő ingatlanjainkat, ott található értékeinket, de akár magunkat és hozzátartozóinkat is, akkor érezhetjük biztonságban, ha minden tőlünk telhetőt megtettünk a védelmünk, védelmük érdekében.

A behatolás ellen védő mechanikus eszközök, riasztók mellett kiemelkedő jelentőségűek e-tekintetben a biztonsági kamerák.

A kamera számos hasznos tulajdonsággal rendelkezhet. Önmagában azon túl, hogy megelőző jelleggel biztosíthatja illetéktelen személyek távoltartását, alkalmas lehet távoli eléréssel állapot ellenőrzésére, illetve esetleges rendőrségi eljárásban elkövető felkutatására, jogsértő cselekmények bizonyítására, de akár eltűnt személyek felkutatásának támogatására is.

Napjainkban - a technika fejlődésével - jó minőségű felvételt biztosító, sokoldalúan használható, egyszerűen szerelhető kamerákat lehet beszerezni, elérhető áron.

Kamerák beszerzésénél érdemes az alábbiakat figyelembe venni:

- A védendő terület elhelyezkedését, méreteit a kamerák számának meghatározásához.
- A kamera felbontását, mely lehetőség szerint minimum 2 megapixel legyen.
- Jó minőségű éjszakai felvételt készítésen, mely érdekében beépített lámpával is rendelkezzen.
- Távoli elérést tudjon biztosítani.
- Felvétel rögzítésére elegendő tárolókapacitása legyen.
- Forgatható kameránál áramszünet esetén a kamera ne álljon vissza alaphelyzetbe.
- A telepített programja magyar nyelvű legyen és képes legyen a felvételek visszánézésakor a lejátszás gyorsítására.



Amennyiben nincs lehetőség az adott területen villamos hálózatra történő csatlakozásra, beszerezhetőek akkumulátorral üzemelő, napelemmel töltődő kamerák is, melyek alkalmasak lehetnek például közmű nélküli ingatlanok, tanyák, legelőterületek, gépparkok megfigyelésére.

A kamerák beállításával, elhelyezésével kapcsolatban fontos kritérium, hogy nem szolgálhat mások jogosulatlan megfigyelésére, illetve jogszabály alapján a kamerával megfigyelt területen jól látható helyen figyelem felhívó táblát kell elhelyezni.



Tegyen Ön is lépéseket biztonsága érdekében, szerezzen be biztonsági kamerát!

Balmazújvárosi Rendőrkapitányság

RENDŐRSÉGI FELHÍVÁS

ONLINE CSALÁSOK MEGELŐZÉSÉRE



FELHASZNÁLÓI FIÓKOK VÉDELME



Felhasználói fiókjai

(levelezés, közösségi oldalak, online tárhelyek és egyéb szolgáltatások) védelme érdekében:

- Használjon minden oldalon eltérő, **ERŐS JELSZAVAKAT!**
- Jelszavai biztonságos tárolásához használjon **JELSZÓKEZELŐ ALKALMAZÁST!**
- Ahol lehet, állítson be **KÉTFAKTOROS HITELESÍTÉST!**

Az ajánlott jelszó:

- hosszú, min. 12 karakter
- összetett: kisbetűk, nagybetűk, számok, speciális karakterek
- nem kötődik semmilyen formában a felhasználóhoz
- Például: \$#Q!4o2Tv6x\$

ADATHALÁSZAT MEGELŐZÉSE



- Mindig ellenőrizze az e-mail feladóját!
- Alaposan olvassa el az e-mailt. Figyeljen a helyesírási hibákra, ékezetek hiányaira!
- Üzenetben kapott linkre kattintás előtt ellenőrizze, hogy a link valóban arra az oldalra mutat, ahogy látszik!
- Megnyitást követően ellenőrizze a böngésző címsorában, hogy valóban a megfelelő oldalra jutott-e!



BANKI TELEFONOS CSALÁSOK MEGELŐZÉSE

Bankok nevében, látszólag a bank telefonszámáról telefonáló csalók próbálják megszerezni az ügyfelek személyes és pénzügyi adatait. A csaló jogosulatlan bankkártya-használatra vagy átutalásra hivatkozik.

- A beszélgetés elején kérdezze meg, hogy kit keres, ha a telefonáló nem tudja az Ön pontos nevét, akkor szakítsa meg a hívást!
- Semmilyen programot ne telepítsen és ne utaljon pénzt biztonságosnak mondott bankszámlára még a bank nevében telefonáló személy kérésére sem!
- Személyes vagy banki adatot, ideértve a bankkártya-adatokat is, ne osszon meg senkivel telefonon! Ha valóban a bank ügyintézője telefonál, ő ismeri a szükséges adatokat.



AZ ÖN PÉNZE BIZTONSÁGBAN VAN, AMÍG MÁSNAK NEM BIZTOSÍT HOZZÁFÉRÉST A BANKSZÁMLÁJÁHOZ. HA KÉTSÉGEI TÁMADNAK A HÍVÁSSAL KAPCSOLATBAN, SZAKÍTSA MEG AZT ÉS HÍVJA FEL ÖN A BANK ÜGYFÉLSZOLGÁLATÁT!



DIGITÁLIS KÁRTEVŐK ÉS BIZTONSÁGI MENTÉS

A számítógépek és mobileszközök internetre történő csatlakozása jelentősen megkönnyíti a számítógépes vírusok és más rosszindulatú szoftverek elterjedését. Éves szinten több mint 10 milliárd USD kárt okoznak a rosszindulatú programok.

ROSSZINDULATÚ SZOFTVEREK

A rosszindulatú szoftverek (angolul malware: malicious software összevonás) a vírusok, férgek, kémprogramok, agresszív reklámprogramok és a rendszerben láthatatlanul megbúvó, a támadónak emelt jogokat biztosító eszközök összefoglaló neve.

A rosszindulatú programok célja lehet:

- a számítógép vagy eszköz tönkretétele,
- fájlok, adatok módosítása vagy törlése,
- a megfertőzött számítógép internetkapcsolatának használata illegális célokra (pl. spam küldésre),
- zsarolás a fájlok titkosításával,
- a felhasználó jelszavainak, bankkártya adatainak megszerzése.



A vírusok manapság jellemzően pendrive vagy e-mail segítségével terjednek az internetes böngészés (a megbízhatatlan oldalakról történő letöltések) mellett. Számítógépes értelemben a trójai faló (röviden trójai) egy olyan rosszindulatú program, ami mást tesz a háttérben, mint amit a felhasználónak mutat. A trójaiak esetében leggyakoribb fertőzési módszert az ingyenes vagy nem jogtisztá programok letöltése és a veszélyes honlapok jelentik.

A VÉDEKEZÉS LEHETŐSÉGEI

A rosszindulatú szoftverek a számítógépen futó szoftverek (operációs rendszerének és egyéb programok) biztonsági hibáit használják ki. A szoftverek gyártói az ismertté vált hibákat rendszeresen javítják, és frissítések kiadásával juttatják el a felhasználókhoz. A frissítések kiadásával az addig esetleg nem nyilvános hibákról is tudomást szerezhetnek a rosszindulatú szoftvereket készítő, így azok a rendszerek, amelyeken a hibákat javító frissítés nem történt meg fokozottan veszélyeztetettek.

A vírusok (és egyéb kártékony programok) elleni védekezés céljából feltétlenül javasolt vírusirtó program telepítése, amelyek elérhetőek ingyenes és fizetős változatban is.

A tűzfal (angolul firewall) célja a privát (otthoni/vállalati) és nyilvános (internet) hálózat elkülönítése, továbbá annak biztosítása, hogy a hálózaton keresztül egy adott számítógépbe ne történhessen illetéktelen behatolás. Amennyiben a számítógép közvetlenül kapcsolódik az internethez szoftveres tűzfal használata javasolt. Ha az internetelérés routeren keresztül történik, akkor az általában tartalmaz tűzfalat. Ebben az esetben győződjünk meg róla, hogy az be van kapcsolva!

BIZTONSÁGI MENTÉS

Rendszeresen készítsünk biztonsági másolatot fontos adatainkról.

Erre alkalmas lehet egy külső merevlemez, amit csak a biztonsági mentés idejére csatlakoztatunk a számítógéphez vagy olyan online tárhely, amely tárolja a fájlok korábbi verzióját.

Online tárhely esetében azért fontos a fájl verziók korábbi eltárolása, mert, ha zsarolóvírus támadás éri a gépet, akkor az automatikus szinkronizációnak köszönhetően a titkosított fájlok kerülnek az online tárhelyre is, de a vírus eltávolítását követően a legutolsó ép verziók visszaállíthatók.

- Frissítések telepítése érdekében javasolt az automatikus frissítés bekapcsolása.
- Felhasználói fiókok felügyeletén állítsuk be, hogy a kritikus műveletekhez (pl. program telepítése) felhasználó engedélyére legyen szükség.
- Böngészők biztonsági beállításai: a magasabb védelmi szint a külső támadások ellen nyújt védelmet.
- Ismeretlen eredetű szoftvereket ne telepítsünk!
- Telepítsünk vírusirtó programot a gépre, és ne kapcsoljuk ki!
- Rendszeresen készítsünk biztonsági másolatot a fontos adatainkról!