Kíberbűnözők a Microsoft nevében

Legyen óvatos a kéretlen 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 kértek 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 – amire a legjobb példa a KiberPajzs együttműködés keretében készített korábbi tippünk – 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 kéretlen 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!