OUCH! 2026. január

Az Ön Havi Biztonsági Tudatosságról Szóló hírlevele

Ál-technikai ügyfélszolgálat: Az egyetlen dolog, amit megjavítanak, az a bankszámlád.

Hogyan vált költségessé egy "segítő szándékú" hívás

Aisha otthonról dolgozott, amikor böngészőjében hirtelen megjelent egy felugró ablak a laptopján: ***„Az ön Windows operációs rendszere többé nem támogatott, és úgy tűnik, fertőzött! A személyes, banki és egyéb érzékeny adatai nagy valószínűséggel veszélybe kerültek. Biztonsága érdekében azonnal keresse fel a Windows Technikai Ügyfélszolgálatát! Hívja most: 1-8XX-XXX-XXXX"***

Mivel Aisha aggódott, hogy elveszíti a pénzét és az adatait, felhívta a telefonszámot. Rövid várakozás után egy szakértőnek hangzó „technikus” vette fel a telefont, és biztosította róla, hogy a problémát meg tudják oldani távolról is. Azt tanácsolta, töltsön le egy „biztonsági szoftvert”, amely lehetővé teszi számukra a rendszerének átvizsgálását. Látta, hogy tömérdek "vírus" jelent meg a képernyőjén. A technikus elmagyarázta, hogy a számítógépe „súlyosan fertőzött”, de egy egyszeri 375 dolláros díjért megtisztítják és biztonságossá teszik számára. Aisha megkönnyebbülve fizetett bankkártyájával.
Később a héten kártyatársasága több jogosulatlan terhelésről figyelmeztette. Aisha ekkor jött rá, hogy a barátságosnak tűnő „technikai támogatás” valójában csalók csapata volt, és nemcsak a hitelkártyájához, de a számítógépéhez is hozzáfértek! Sajnos Aisha története nagyon gyakori eset — és számtalan **technikai ügyfélszolgálatos csalás** pontosan így működik.

Mik azok a technikai ügyfélszolgálatos csalások?

A technikai támogatással kapcsolatos átverések úgy működnek, hogy a bűnözők elhitetik az emberekkel, hogy valami nincs rendben a számítógépükkel, telefonjukkal vagy online fiókjukkal, és azonnali segítségre van szükségük a probléma megoldása érdekében. A csalók olyan legitim vállalatok dolgozóinak adják ki magukat, mint a Microsoft, az Apple vagy a bankunk. A céljuk? **Becsapni minket, hogy átadjuk a pénzüket, érzékeny adatainkat vagy hogy hozzáférést szerezzenek eszközeinkhez, fiókjainkhoz.**

Az ilyen típusú csalások gyakran hamis böngésző- vagy operációs rendszer-frissítési felugró ablakokkal, telefonhívásokkal vagy szöveges üzenetekkel kezdődnek, amelyek azt állítják, hogy a számítógépünk megfertőződött, vagy a fiókunk veszélybe került. Nem számít ezek közül pontosan melyikkel kezdődik a csalás, a cél mindig ugyan az: pánikot kelteni és elhitetni velünk, hogy **azonnal** cselekednünk kell.

Mit keresnek?

A technikai ügyfélszolgálatos csalók általában három dolog reményében keresnek fel:

1. **A pénzünk:** Pénzt kérhetnek nem létező problémák „megoldásáért”, gyakran ajándékkártyás vagy kriptovalutás fizetést követelve — olyan módszerekkel, amelyeket nehéz visszakövetni.
2. **Az információink:** Nevünket, címünket, jelszavainkat vagy banki adatainkat kérik azzal az ürüggyel, hogy személyazonosságunkat igazolják, vagy visszatérítést dolgozzanak fel.

3. **Hozzáférés eszközeinkhez vagy fiókjainkhoz:** Rávesznek, hogy távoli hozzáférést biztosító szoftvert telepítsünk, így kémkedhetnek utánunk, fájlokat lophatnak vagy valódi kártevőt telepíthetnek későbbi támadásokhoz.

Hogyan működnek ezek a csalások

A technikai ügyfélszolgálatos átverések erősen **social engineering** alapokra támaszkodnak —az érzelmeinket manipulálják, hogy félelmet és a sürgősség érzetét keltsék bennünk. Itt egy tipikus minta:

1. **Félelemkeltéssel rántanak bennünket csapdába:** felugró ablakot látunk, vagy üzenetet avagy telefonhívást kapunk, amely azt állítja, hogy rendszerünk vagy fiókunk veszélybe került. Az üzenet riasztó szóhasználattal él, mint például: „Az adatai el fognak veszni!” vagy „Fiókja felfüggesztésre kerül!"
2. **A bizalom:** A csaló egy jól ismert vállalat szakemberének adja ki magát, sőt hivatalos logókat vagy hamisított telefonszámokat is használ.
3. **Kontroll és fizetés:**Arra kérnek minket, hogy egy szoftvert telepítsünk vagy kattintsunk egy hivatkozásra, amivel hozzáférést adunk készülékünkhöz. Ezt követően díjat számítanak fel a „javításokért” vagy a „védelmi szolgáltatásokért”. Még ha rá is jövünk, hogy csalásról van szó, és bontjuk a kapcsolatot, előfordulhat, hogy az eszközünkhöz való hozzáférésük megmarad.

Hogyan védjük meg magunkat

1. **Maradjunk higgadtak és gondolkodjunk:** A valódi cégek **nem** jelenítenek meg telefonszámot tartalmazó felugró figyelmeztetéseket, és nem hívnak bennünket váratlanul. Ha valami sürgősnek vagy ijesztőnek hat, azonnal álljunk meg, és bizonyosodjunk meg róla független forrásokból is!
2. **Ne adjunk távoli hozzáférést:** Soha ne engedjük egy számunkra ismeretlen embernek, hogy távoli hozzáférése legyen az eszközünkhöz vagy fiókjainkhoz! Ne hívjuk fel a megjelenített telefonszámot, és ne kattintsunk a megjelenített linkre!
3. **Ne adjunk távoli hozzáférést:** Sohase engedjük egy számunkra ismeretlen embernek, hogy távoli hozzáférése legyen az eszközünkhöz vagy fiókjainkhoz! Ha ők léptek kapcsolatba velünk, és erőltetik hogy adjunk nekik hozzáférést, akkor csalásról van szó.
4. **Figyeljük és biztosítsuk fiókjainkat:** Ha azt sejtjük, kapcsolatba léptünk egy csalóval, azonnal változtassuk meg jelszavainkat és figyeljük a bankfiókunkat szokatlan aktivitást keresve!

Záró gondolatok

A technikai ügyfélszolgálatoknak álcázott csalások a félelmünkre, a sürgetésre és a bizalmunkra építenek — és bárkivel megtörténhetnek, függetlenül attól, mennyi szakmai tapasztalattal rendelkezik. Jusson eszünkbe: **A megbízható vállalatok soha nem fognak bennünket felhívni, e-mailt küldeni, vagy felugró ablakban megjelenni azért, hogy távoli hozzáférést vagy fizetést kérjenek egy probléma megoldásáért.</1>** A legjobb védelem, ha higgadtak és szkeptikusak maradunk.

Vendégszerkesztő

Jennifer Cox a Tines nevű intelligens automatizációs vállalat megoldás-konzultációs igazgatója, amely a kiberbiztonsági műveletek átalakításán dolgozik. Többszörösen díjnyertes kiberbiztonsági vezető, aki szenvedélyesen mentorálja a jövő iparági szakembereit, és előmozdítja az innovációt, a kiválóságot és a befogadást a globális kiberbiztonsági és automatizációs ökoszisztéma műszaki csapatain belül. https://www.linkedin.com/in/jennifermcox/

Források

A frissítés ereje: https://www.sans.org/newsletters/ouch/power-updating/
Hogyan használják ki a kiberbűnözők érzelmeinket: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
A Jelmondatok Ereje: https://www.sans.org/newsletters/ouch/power-passphrase/

A Közösség számára fordította: Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI)

Többet találhat az Ouch!-ból A következő linken: https://www.sans.org/newsletters/ouch