Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Vishing – csaló telefonhívások

Áttekintés

Amikor azt halljuk, hogy kiberbűnöző, valószínűleg sokunk egy gonosz lángészt képzel el, amint egy számítógép előtt ülve sorban indítja az összetett kibertámadásokat az interneten keresztül. Habár egyes bűnözők valóban fejlett technológiát alkalmaznak, sokan csupán egy telefon segítségével szedik rá áldozataikat. A telefon használatának két nagy előnye van számukra: Más támadási módokkal ellentétben egy telefonhívás esetében kevesebb olyan biztonsági megoldás létezik, ami képes felsimerni és megállítani egy támadást. Illetve telefonon keresztül könnyebb érzelmekre alapozva bizalmat kiépíteni, ami megkönnyíti az áldozatok becsapását. Lássuk miként tudjuk felismerni és megállítani ezeket a támadásokat.

Hogyan működnek a telefonos támadások?

Először is, meg kell értenünk, hogy a bűnözők általában a pénzünket, személyes információinkat vagy a számítógépünkhöz való hozzáférést akarják megszerezni – vagy mindhármat ezek közül. Ezt a pszichológiai manipuláció eszközével próbálják meg elérni, így vesznek rá bennünket olyasmire, amit nem kellene megtennünk. A számítógépes bűnözők gyakran olyan helyzeteket teremtenek, amelyek sürgősnek és reálisnak tűnnek a hívás során. Néhány nagyon gyakori példa:

- A hívó úgy tesz, mintha valamely kormányzati szervtől telefonálna, és be nem fizetett adóra hivatkozik. Majd azt állítja, hogy amennyiben most rögtön nem rendezzük a tartozást bankkártya adatok megadásával, börtönbüntetésre számíthatunk. Ez átverés. Az adóhatóság adózással kapcsolatos értesítést kizárólag hivatalos levél útján küld. (AZ NBSZ NKI megjegyzése: a NAV ügyfélkapun, postán, illetve adószámla-kivonaton keresztül értesíti az adózókat, adóhátralék vagy túlfizetés esetén.)
- A hívó úgy tesz, mintha egy nagy cég nevében telefonálna – mint például az Amazon, az Apple vagy a Microsoft Tech Support – és arról tájékoztat bennünket, hogy a számítógépünk fertőzött. Ezt követően megpróbál rávenni minket, hogy vásároljuk meg az általa ajánlott biztonsági szoftvert, vagy biztosítsunk távoli hozzáférést az eszközünkhöz.
- Egy automatikus hangposta üzenet arról tájékoztat bennünket, hogy bankszámlánkat vagy hitelkártyánkat törölték, és az újraaktiválásához fel kell hívnunk egy telefonszámot. Ha felhívjuk ezt a számot, egy telefonos automata rendszer jelentkezik be, amely beazonosítás céljából elkéri személyes adatainkat, valamint biztonsági kérdésekre adott válaszainkat. Ez biztosan nem a bankunk. Egyszerűen csak rögzítik az összes általunk megadott adatot, hogy azokat később személyazonosság-csalások során felhasználhassák ellenünk.

Így védekezhetünk

A telefonhívásos csalások elleni legjobb védekezés mi magunk vagyunk. Az alábbiakat mindig tartsuk észben:

- Bárki is hívjon minket, ha sürgetni próbál vagy nyomást gyakorol ránk, legyünk rendkívül gyanakvóak! A támadók a sürgetéssel azt próbálják elérni, hogy hibázzunk. Még akkor is, ha a telefonhívás elsőre úgy tűnik, hogy rendben van, ha bármelyik pillanatban is furcsának tűnik, azonnal leállíthatjuk, és nemet mondhatunk.
- Legyünk különösen óvatosak azokkal a hívókkal, akik ragaszkodnak ahhoz, hogy ajándékkártyákat vagy prepaid hitelkártyákat vásároljunk!
- Ne bízzunk meg vakon a kijelzett hívószámban! A támadók gyakran meghamisítják a hívószámot, ezért úgy tűnhet, hogy a hívás során egy legitim szervezettől keresnek bennünket.
- Ne engedjük, hogy a hívó ideiglenesen irányítása alá vonja a számítógépét, vagy egy szoftver letöltésére vegyen rá minket! Ezzel ugyanis megfertőzhetik a számítógépet.
- Ne adjuk meg a másik félnek azokat az információkat magunkról, amelyeket már tudnia kellene, hacsak nem mi kezdeményeztük a hívást! Például, ha a bank hív minket, nem szabad elkérnie a számlaszámunkat.
- Ha feltételezzük, hogy a telefonhívás egy támadás, egyszerűen csak szakítsuk meg a hívást. Ha meg akarjuk erősíteni, hogy a telefonhívás jogos volt-e, keressük fel a szervezet – például bankunk – weboldalát, és hívjuk fel az ügyfélszolgálat telefonszámát. Így biztosak lehetünk abban, hogy a valódi szervezettel beszélünk.
- Ha egy olyan számról keresnek bennünket, amit nem ismerünk, hagyhatjuk, hogy a hívás átirányítódjon a hangpostára. Így az ismeretlen hívásokkal foglalkozhatunk később is, amikor jobban ráérünk. Még jobb, ha alapértelmezetten engedélyezzük a „Ne zavarjanak” funkciót, amely szolgáltatás a legtöbb telefonon elérhető.

A telefonos csalások és támadások gyakorisága növekvő tendenciát mutat. Az ilyen támadások ellen mi magunk vagyunk a legjobb védelem.

A szerzőről

Jen Fox a „DEF CON 23” rendezvényen, a pszichológiai manipuláció területén kiosztott „black badge – fekete kitűző” díj tulajdonosa, aki biztonsági tudatossági oktatással foglalkozik a Domino biztonsági program szakértőjeként. Jen a Twitteren @j_fox.

Források

Pszichológiai Manipuláció: https://www.sans.org/security-awareness-training/resources/social-engineering-attacks
Üzenetküldéses/SMS csalások: https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks
Személyre szabott csalások: https://www.sans.org/security-awareness-training/resources/personalized-scams
Telefonos csalásbejelentés (az USA-ban): https://www.reportfraud.ftc.gov

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)