Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Jótékonysági és katasztrófa-helyzeteket kihasználó csalások

A kiberbűnözők tisztában vannak vele, hogy akkor hibázunk a legkönnyebben, ha sürgetnek bennünket. Mi más adná a legjobb apropót a sürgetésre, mint valamilyen vészhelyzet? Ez az oka annak, hogy a számítógépes bűnözők kifejezetten örülnek a globális hatású tragikus eseményeknek. Amit legtöbben szerencsétlenségnek fogunk fel – mint például egy háború kitörését, egy természeti katasztrófát, és persze az olyan pandémiákat, mint a COVID-19 –, a kiberbűnözők egy jó lehetőségnek tekintenek, amit ki lehet használni. Amikor egy-egy téma kapcsán hirtelen óriási mennyiségű hír és közösségi poszt készül, a hackerek tudják, hogy eljött az ő idejük.

Ezt a kiemelt figyelmet olyan aktuális témájú csaló e-mailek készítésére használják fel, amelyeket azután akár több millió embernek is elküldhetnek. Vegyük egy természeti katasztrófát példaként. Egy ilyen esemény bekövetkezésekor a kiberbűnözők hazudhatják azt, hogy például gyermekek megsegítésére gyűjtenek pénzt. Ezek a csalások sok esetben már néhány órával azután megindulnak, hogy az adott eseményről a világ tudomást szerezett, ugyanis a támadók már jó előre felkészülnek a megfelelő háttér-technikával. És vajon mi magunk hogyan készülhetünk fel minderre?

Hogyan azonosítsuk a jótékonysági csalásokat?

A védekezés kulcsa, hogy legyünk gyanakvóak bárkivel szemben, aki üzenetet küld nekünk! Például akkor se bízzunk meg egy e-mailben, ami kétségbeesetten gyűjt adományt, ha az egy általunk jól ismert szervezettől érkezik! Ne bízzunk meg olyan telefonhívásban, ami arra próbál rávenni bennünket, hogy adományozzunk! Akkor sem, ha a hívó azt állítja, hogy egy közhasznú szervezettől, például egy élelmiszerbanktól telefonál! Minél inkább sürgetnek bennünket, annál valószínűbb, hogy egy támadásról van szó. A jótékonysági csalások leggyakoribb jellemzői az alábbiak:

- Valamilyen bankon kívüli pénzutalásra kérnek bennünket, mint például kriptovaluta, Western Union, vagy ajándékkártya.
- A telefonhívások során a kiberbűnözők megváltoztathatják a hívóazonosítót, hogy azt higgyük az egy helyi hívás, vagy, hogy egy ismert szervezettől keresnek minket. A kijelzett telefonszámban manapság nem lehet megbízni.
- Létező neveket és logókat is használhatnak, hogy valódi adománygyűjtőnek tűnjenek. Ezért jobban tesszük, ha adakozás előtt egy kis kutatást végzünk.
- A kiberbűnözők gyakran homályos és szentimentális dolgokat állítanak arról, hogy az adomány milyen célokat szolgál, ahelyett, hogy konkrétumok hangoznának el arról, hogy az adományt pontosan mire és hogyan használnák fel.

- Ne tekintsük valódinak a közösségi finanszírozású oldalakon (mint például a GofundMe), vagy a közösségi média oldalakon (mint például a TikTok) érkező segélykéréseket, különösen, ha azok egy katasztrófahelyzet idején tűnnek fel.
- A csalók esetenként azzal a trükkel is próbálkoznak, hogy először olyan adomány miatt hálálkodnak, amit állítólag a múltban küldtünk nekik, miközben valójában nem is tettünk ilyet.
- Soha ne adjunk ki személyes vagy pénzügyi adatot válaszul egy megkeresésre!

Hogyan tegyünk különbséget biztonságosan?

Ha adományozni szeretnénk, azt kizárólag jól ismert, megbízható szervezeteken keresztül tegyük! Ekkor ugyanis mi kezdeményezzük a kapcsolatot, és dönthetjük el melyik szervezethez fordulunk, valamint, hogy ezt mely telefonszámon vagy honlapon keresztül tesszük meg. Amikor azt fontolgatjuk, hogy adományozunk, keressünk rá a szervezet nevére olyan kifejezésekkel kiegészítve, mint például „panasz", „vélemény", „értékelés", „rangsor". Nem vagyunk biztosak abban, melyik adományszervezet megbízható? Kezdjük a keresést kormányzati weboldalakon, vagy induljunk ki megbízható hírportálok által közölt cikkekből és hivatkozásokból! Szükség idején az adományozás hatalmas segítség lehet, csupán arra ügyeljünk, hogy ez a megfelelő szervezethez jusson el!

A szerzőről

Dr. Jessica Barker a biztonság emberi tényezőjével foglalkozó, vezető szakember, aki már több elismerésben részesült. Többek között a Cygenta cég társ-vezérigazgatója, és bestseller könyvek szerzője is egyben. Jessica tagja a SANS Security Awareness Summit tanácsadó testületének.

Források

FTC jótékonysági csalás: https://consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams
Pszichológiai manipulációs támadások: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Top három átverés: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Üzenetküldéses/SMS csalások: https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks/
Vishing - Telefonos csaló hívások: https://www.sans.org/newsletters/ouch/vishing/
Jótékonysági Navigátor: https://www.charitynavigator.org/

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