OUCH! 2024. szeptember

Fantomhangok: Védekezés a hangklónozásos támadások ellen

A váratlan hívás: Egy megtévesztés története

Margaret, egy nyugdíjas tanárnő, élvezte a békés reggeleket kicsi külvárosi otthonában. Egy nap, miközben a reggeli kávéját kortyolgatta, felhívta őt Jacob, az unokája, aki már egyetemre járt. Jacob hangja pániktól remegett miközben elmesélte, hogy autóbalesetet szenvedett, és sürgősen pénzre van szüksége a károk rendezéséhez és a jogi következmények elkerüléséhez. Ha nem kapja meg azonnal a pénzt, akár börtönbe is kerülhet. A vonal másik végéről érkező hang összetéveszthetetlenül Jacobé volt – Margaret szíve hevesen vert az aggodalomtól. Kérdés nélkül rohant a bankjához, és pénzt utalt arra a számlára, amit Jacob megadott. Margaret csak akkor jött rá, hogy átverték, amikor aznap később felhívta Jacob édesanyját érdeklődni, hogy hogy van a fia. A hívás csak egy kegyetlen csel volt: egy kiberbűnöző mesterséges intelligencia (MI) technológia alapú hangklónozást használt Jacob hangjának lemásolására, így kihasználva Margaret unokája iránt érzett szeretetét és aggodalmát.

Mi az a hangklónozás?

A hangklónozás az, amikor valaki mesterséges intelligenciát használ egy személy hangjának újraalkotására, beleértve az intonációikat és beszédritmusukat, így létrehozva egy majdnem tökéletes másolatot.

A hangklónozásos támadás első lépéseként a kiberbűnöző hangmintákat gyűjt a célponttól. A mintákat különböző forrásokból, például YouTube-videókból vagy személyes TikTok posztokból szerzik be. Az összegyűjtött hanganyagot a mesterséges intelligencia betanítására használják, amely ennek eredményeképp egy olyan új hangot hoz létre, amely hasonlít az áldozatéhoz. Az így létrehozott hang különböző módokon használható, például telefonhívásokhoz vagy hangüzenetekhez, így hatékony eszközzé válik a megtévesztésre.

A hangklónozásos támadások előtt a kiberbűnözők gyakran alapos kutatást végeznek. A szükséges információk nagy része nyilvánosan elérhető a közösségi média oldalakon. Tanulmányozzák a kiszemelt áldozatokat, beleértve azt a személyt, akinek a hangját másolni fogják, valamint azét is, akit fel fognak hívni. A csalók nemcsak azt tanulják meg, hogy kiket ismernek és kikben bíznak meg az áldozataik, hanem azt is, hogy mely érzelmi triggerek a leghatékonyabbak. Amikor ezeket a telefonhívásokat intézik, a kiberbűnözők gyakran módosítják a hívóazonosítót, így amikor a célpontok megnézik telefonjukat, a hívás egy olyan számról érkezik, amelyben megbíznak. A hívóazonosító könnyen hamisítható, így nem megbízható módszer a telefonáló személyek hitelesítésére vagy azonosítására.

Így védekezzünk

Ahhoz, hogy meg tudjuk védeni magunkat az ilyen jellegű támadásoktól, fontos tudatában lennünk annak, hogy a hangklónozás már lehetséges, és a kiberbűnözők számára napról-napra egyre egyszerűbben véghezvihető. Néhány kulcsfontosságú lépés ezügyben:

- **Adatvédelem**: Figyeljünk arra, hogy milyen információkat osztunk meg másokkal, és korlátozzuk, hogy kik férhetnek hozzá a rólunk készült felvételekhez a közösségi médiában!

- **Jelek**: Figyeljünk azokra a gyakori jelekre, amelyek arra utalnak, hogy valami nincs rendben! Ha valaki sürgető hangnemben beszél, vagy azonnali cselekvésre próbál késztetni, akkor az nagy valószínűséggel csalás. Minél inkább sürgetnek bennünket (például valakinek most azonnal pénzre van szüksége) annál nagyobb a valószínűsége annak, hogy ez a valaki arra pályázik, hogy a nagy sietségben átgondolatlanok legyünk, hibát kövessünk el. Más gyakori jelek közé tartozik az, ha valami túl szép ahhoz, hogy igaz legyen (nem, nem nyertünk a lottón), vagy olyan váratlan hívást kapunk, ami bizarrnak tűnik.

- **Ellenőrzés**: Ha nem vagyunk biztosak abban, hogy egy telefonhívás valódi-e, tegyük le, és hívjuk vissza az illetőt egy megbízható telefonszámon! Például, ha egy felsővezetőtől vagy kollégától kapunk hívást a munkahelyünkön, hívjuk vissza őket egy olyan megbízható telefonszámon, amelyről biztosan tudjuk, hogy azt ők használják. Ha furcsa telefonhívást kapunk egy családtagtól, próbáljuk meg visszahívni (esetleg videohívással), vagy hívjunk fel egy másik családtagot, aki jól ismeri őt.

- **Jelszó**: Hozzunk létre egy titkos jelszót, amit csak mi és a családunk ismer! Így, ha furcsa telefonhívást kapunk, ami látszólag családtagtól származik, megbizonyosodhatunk róla, hogy valóban vele beszélünk-e. Csak kérdezzük meg, mi a jelszó!

A szerzőről

Maria Singh az EnterpriseKC cyber tartalom menedzsere és lelkes WiCyS tag, több mint 14 év technológiai és kiberbiztonsági tapasztalattal. SANS GIAC GSEC minősítéssel rendelkezik és a Purdue Egyetem Kiberbiztonság mesterszakának hallgatója. Mint a Kansas városi Women in Security korábbi elnöke és az OCA Corporate Achievement díj kitüntetettje, Maria inspirálja a nőket a STEM és kiberbiztonság területén. Előadásai és vezetési gyakorlata egyengetik az utat a jövő generációi számára, hogy sikeresen boldoguljanak ezeken a területeken.

Források

Top három módszer, ahogy a (Kiber)támadók célpontjává válunk: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
Állítsuk meg a telefonos csaló hívásokat: https://www.sans.org/newsletters/ouch/stop-phone-call-scams
Érzelmi triggerek – Így csapnak be minket a kibertámadók: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

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