

OUCH!

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Hogyan védjük meg az időseket a csalásoktól?

Egy telefonhívás lesújtó következményekkel

Robert, a 73 éves nyugdíjas férfi, 35 évig dolgozott egy helyi termelőüzemben, hogy pénzt tehessen félre nyugdíjas éveire és családja számára. A sok év kemény munkája kifizetődött. Robertnek sikerült elég pénzt összegyűjtenie bank-, megtakarítási-, és nyugdíjfolyósító számláján ahhoz, hogy ő és felesége életük végéig kényelmesen tölthessék nyugdíjas éveiket.

Egy hétfő reggel Robert egy riasztó hívást kapott valakitől, aki azt állította, hogy bankja csalás elleni részlegéről keresi. A hívó arról tájékoztatta az idős férfit, hogy bankszámláját kiberbűnözők törték fel, így komoly veszélybe kerültek megtakarítási- és nyugdíjfolyósítói számlái. A telefonáló siettetve utasította Robertet, hogy számlái védelme érdekében azonnal utalja át pénzét a bank által vezetett „biztonságos” számlákra. A csaló megadta az új banki adatokat, biztosítva a férfit arról, hogy ez az egyetlen mód pénzének megóvására. Megbízva a hívásban, az ijedt Robert beleegyezett, és minden megtakarítását átküldte a csaló által megadott számlára.

Az idős férfi csak néhány nappal később vette észre, hogy átverték, és az összes nyugdíjas éveire spórolt pénz eltűnt. Ez az eset Robertet teljesen összetörte, zavarba hozta, a jövőjét pedig bizonytalanná tette.

Miért az időseket célozzák meg a csalók?

Sajnos a csalók gyakran az idősebb felnőtteket veszik célba, mert azt hiszik, hogy ők könnyebben megbíznak az idegenekben, vagy kevésbé jártasak a technológia világában. Ezen túlmenően az idősek gyakran tehetős célpontok, mivel bőséges nyugdíj- és befektetési számlákat, kiváló hiteleket vagy más értékes vagyontárgyakat halmoztak fel, amelyeket a csalók szívesen kihasználnak. Végül, az idősebbek talán kevésbé jelentik be, hogy átverték őket, mert szégyenlik, félnek a függetlenségük elvesztésétől, vagy egyszerűen nem tudják, kihez forduljanak. A csalók számára a tény, hogy teljesen tönkreteszik mások életét, nem sokat jelent.

Megérteni a csalók stratégiáit kulcsfontosságú, hogy megvédhessük idős társainkat. A legelterjedtebbek közé tartoznak a telefonos csalások. Ezek során a hívók gyakran úgy tesznek, mintha kormányzati szerveket, pénzintézeteket, közműszolgáltatókat képviselnének, vagy akár bajba jutott családtagoknak adják ki magukat. A csalók sürgősség érzetét vagy félelmet keltenek, és nyomást gyakorolnak az idősekre, hogy azonnal cselekedjenek, anélkül, hogy meggyőződnének az információk hitelességéről. Például azt állítják, hogy egy közüzemi számla nem került befizetésre, és amennyiben nem fizetik ki azonnal, az adott közüzemi szolgáltatást kikapcsolják. Egy másik gyakori taktika az „unokázós” csalás, ahol a csalók az idősek unokáinak adják ki magukat, akiknek sürgősen pénzre van szüksége óvadék kifizetésére, egészségügyi ellátás finanszírozására, vagy hazajutáshoz.

Ezek a hívások még hatékonyabbak lehetnek, ha a csalók mesterséges intelligenciát használnak hangklónozásos támadásokhoz.

Az e-mail- és az SMS-alapú phishing is egy széles körben elterjedt módszer az idős emberek célba vételére. Ezek a megtévesztő üzenetek úgy tűnhetnek, mintha törvényes forrásból, például bankoktól, hitelkártyatársaságoktól, családtagoktól vagy ismerős vállalkozásoktól érkeznének. Ezek gyakran tartalmaznak félelemkeltő üzeneteket, amelyek arra ösztönzik a címzetteket, hogy kattintsanak linkekre, töltsenek le mellékleteket vagy személyes adatokat adjanak meg.

Mit tehetünk?

Annak ellenére, hogy a bűnözők gyakori célpontjai, az idős emberek ugyanolyan típusú kiberfenyegetéseknek vannak kitéve, mint bárki más. A biztonságos online jelenléttel kapcsolatos oktatás – például csalások felismerése, jelszavaink biztonságos kezelése és kizárólag megbízható weboldalak használata – drámaian csökkentheti sebezhetőségüket. A kockázatokról szóló nyílt és rendszeres beszélgetések ösztönzése hatékony megelőző intézkedés lehet. A családoknak emlékeztetniük kell az időseket, hogy a legitim szervezetek soha nem fognak azonnali fizetést kérni ajándékkártyákon, átutalásokon vagy készpénzátvételen keresztül. Tanácsolniuk kell továbbá az időseket, hogy soha ne osszanak meg olyan személyes adatot magukról mint például adóazonosító jel, bankszámla- vagy hitelkártya adatok, kizárólag akkor, ha ők kezdeményezték a kapcsolatfelvételt, és teljes mértékben megbíznak a forrásban. Soha ne adjunk távoli hozzáférést vagy irányítást PC- és mobil eszközeink felett.

A célunk az, hogy a biztonságot a lehető legegyszerűbbé tegyük számukra. A hívásblokkolók használata segíthet az időseknek elkerülni a nem kívánt vagy gyanús hívásokat. Segítsünk nekik beállítani, hogy a családtól érkező telefonhíváson kívül minden hívás egyenesen a hangpostafiókba menjen. Egy másik ötlet az, hogy a leggyakrabban használt webhelyeket lássuk el könyvjelzővel a böngészőjükben, így tudják, hogy a megfelelő oldalakat keresik fel. Ha a jelszókezelők összezavarják őket, javasoljuk nekik a jelszófüzeteket használatát, ahova lejegyezhetik belépési adataikat, majd egy biztonságos helyen tárolhatják. A családok továbbá rendszeresen ellenőrizhetik idős rokonaik pénzügyi kimutatásait és számláit, hogy gyorsan felismerjék és kezeljék a gyanús tevékenységeket. A legfontosabb, hogy megerősítsük az időseket abban, hogy a csalók célpontjává válni nem az ő hibájuk, és nem is kell emiatt szégyenkezniük.

Vendégszerkesztő

Dean Parsons az ICS Defense Force vezérigazgatója, a SANS egyik vezető oktatója, és a kritikus infrastruktúrák elhivatott védelmezője. Több mint 20 éve dolgozik a kiberbiztonság területén, ipari incidensek elhárításával foglalkozik, és a 80-as évek ihlette zenét ír Arcade Knights nevű zenekarával.



Források

Hízélgés és üres pénztárca: romantikával átitatott befektetési csalások: <https://www.sans.org/newsletters/ouch/sweet-talk-empty-wallet-romance-fueled-investment-scams/>

Ne hagyjuk, hogy a kiberbűnözők lenyúlják a megtakarításainkat: <https://www.sans.org/newsletters/ouch/dont-let-cybercriminals-swipe-your-savings-lock-down-your-financial-accounts/>

Fantomhangok: Védekezés a hangklónozásos támadások ellen: <https://www.sans.org/newsletters/ouch/phantom-voices-defend-against-voice-cloning-attacks/>

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

OUCH! A SANS Security Awareness által közzétett és a [Creative Commons BY-NC-ND 4.0 licence](https://creativecommons.org/licenses/by-nc-nd/4.0/) alatt terjesztett kiadvány. Ezt a hírlevelet szabadon megoszthatja vagy terjesztheti egészen addig, amíg nem adja el vagy nem módosítja. Szerkesztőbizottság: Phil Hoffman, Leslie Ridout, Princess Young.