Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

A három leggyakoribb közösségi média csalás

Áttekintés

Miközben a közösségi média kíváló lehetőséget nyújt a kapcsolattartásra, a tartalmak megosztására és a szórakozásra, sajnos a kiberbűnözők számára viszont arra ad lehetőséget, hogy költséghatékony módon emberek millióit kihasználhassák. Ez a három leggyakoribb csalás a közösségi média oldalakon, amire érdemes odafigyelnünk.

Befektetési csalások

Találkozott már olyan befektetési lehetőségről szóló poszttal, ami rendkívüli hozamot ígért extrém rövid idő alatt, kicsi vagy nulla kockázat mellett? A valóság az, hogy ezek befektetési csalások. A csalók pedig egyszerűen ellopják a befektetés céljából átutalt pénzt. Ezek az átverések gyakran reklámokat tartalmaznak, például korábbi vásárlók "sikertörténeteit", azért hogy meghozzák a kedvet a befektetéshez, azonban ezek hamisak, és csupán a bizalom megszerzésére szolgálnak. Az ilyen csalások sok esetben valamilyen kriptovaluta vagy ingatlan vásárlására buzdítanak, és a kifizetést is kriptovalutában vagy más, nem hagyományos fizetési formában kérik. Ha egy befektetési hirdetés túl jónak tűnik ahhoz, hogy igaz legyen, valószínűleg nem is az. Ne feledjük, nem létezik garantáltan magas hozamú befektetés! Kizárólag megbízható, jól ismert befektetési formákba invesztáljunk, és ne bízzunk meg idegenekben, akik „gazdagodjon meg gyorsan”-típusú lehetőségekkel bombáznak minket az online térben!

Romantikus csalások

Romantikus csalásnak nevezzük, amikor a kiberbűnözők online kapcsolatot alakítanak ki a magányosnak vagy sebezhetőnek tűnő áldozatokkal, hogy pénzt csaljanak ki tőlük. A bűnözők mindent megtesznek azért, hogy bizalmat építsenek ki az áldozattal, például hamis fényképekel, ajándékokkal, majd előbb-utóbb egy tragikus történetet adnak elő, amellyel megpróbálják alátámasztani, hogy miért van szükségük pénzre. Jellemző történet a költséges kórházi kezelés, illetve, hogy az áldozattal való találkozás csak akkor valósulhat meg, ha az áldozat állja az utazási költségeiket. Azért hogy elkerüljék az áldozattal való tényleges találkozást, sokszor azt hazudják, hogy munkájuk miatt nem lehetséges a személyes találkozás, mert például az építőiparban, nemzetközi gyógyszerkereskedelemben vagy épp a hadseregben dolgoznak. A pénzt gyakran banki átutaláson keresztül vagy ajándékkártya formájában kérik, azért, hogy minél előbb hozzáférhessenek az összeghez, de közben megőrizhessék a névtelenségüket. Ez a fajta csalás nem csak a közösségi média oldalakon gyakori, hanem a rendialkalmazásokon is.

Legyünk óvatosak az online kapcsolatainkkal! Igyekezzünk lassítani, és soha se küldünk pénzt valakinek, akivel addig csak online kommunikáltunk!

Sőt, ha tudomásunk van arról, hogy egy ismerősünk hasonló helyzetben van, vagy feltételezzük, hogy kiszolgáltatott lehet egy ilyen átveréseknek, ajánljuk fel a segítségünket! Aki érzelmileg érintett egy ilyen helyzetben, annak gyakran nagyon nehéz felismernie, hogy ez mennyire veszélyes lehet.

Online vásárlási csalások

Online vásárlási csalás az, amikor extrém alacsony áron vásárolunk valamit egy online shopban, azonban sosem kapjuk meg magát a terméket. A közösségi média oldalakon feltűnő hirdetések esetenként hihetetlenül alacsony árakat mutatnak, és olyan weboldalakra vezetnek, amelyek első ránézésre egy jól ismert márka valódi webhelyének tűnnek, azonban ezek sok esetben hamisak. Legyünk óvatosak azokkal a webhelyekkel, amelyekkel semmilyen módon nem lehet kapcsolatba lépni, vagy amelyek nem működő kapcsolatfelvételi űrlapokkal vagy magán e-mailes elérhetőséggel rendelkeznek! Írjuk be az online áruház nevét vagy webcímét a keresőbe, hogy megtudjuk, mit mondtak róla mások! Keressünk olyan kifejezéseket, mint például: "csalás", "átverés", "soha többé" és "hamis"! Legyünk különösen óvatosak az olyan online hirdetésekkel és ajánlatokkal, amelyek túl jónak tűnnek ahhoz, hogy igazak legyenek! Sokkal biztonságosabb olyan termékeket vásárolni, amelyek lehet, hogy egy kicsivel drágábbak, azonban elérhetőek olyan megbízható oldalakon keresztül, ahonnan mi – vagy ismerőseink – már vásároltunk.

A jó hír az, hogy mi magunk vagyunk a legjobb védelmünk. Nálunk van az irányítás. Csupán figyeljünk oda ezekre az átverésekre, és így biztonságosan hozhatjuk ki a legtöbbet a közösségi médiából!

A szerzőről

Chris Elgee (@chriselgee) sérülékenységvizsgáló, aki a @CounterHackSec számára alkot kihívásokat, emellett az amerikai Nemzeti Gárda kiberzászlóalj parancsnoka, és tanúsított SANS instruktor. Chris számára az nyújtja az igazi élvezetet, ha az apró technikai részletekkel foglalkozhat, amelyekből egy egész szervezet számára hasznos tudást építhet, amit azután diákokkal és partnerekkel is megoszthat.

Források

Better Business Bureau Scam Tracker: https://www.bbb.org/ScamTracker
Pszichológiai manipulációs támadások: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Biztonságos online vásárlás: https://www.sans.org/newsletters/ouch/shopping-online-securely-nov-21/
Vishing - Telefonos csaló hívások: https://www.sans.org/newsletters/ouch/vishing

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