Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

SMS-támadások: Egy smishing történet

Márk SMS-t kapott az Amazontól, amit értetlenül olvasott: „A kézbesítési kísérlet meghiúsult! Kattintson az alábbi linkre, hogy újraütemezze a kézbesítést, ellenkező esetben csomagját visszaküldjük a feladónak.” Márk nem emlékezett rá, hogy mostanában rendelt volna bármit is online, de őszintén szólva annyi mindent rendelt már az interneten, hogy elképzelhetőnek tartotta, hogy megfeledkezett róla. Nem akart lemaradni semmilyen csomagról, ezért rákattintott a linkre, és egy oldal töltött be, amely a kapcsolattartási adatait kérte "a megfelelő újraütemezés biztosítása érdekében". Az üzenet először kissé furcsának tűnt, de Márk végül úgy gondolta, jobb félni, mint megijedni. Beírta az otthona címét, majd további információkat kértek tőle, beleértve a bankkártya adatait is. Bízva a cégben, mindent megadott, amit kértek, hogy biztosítsa a kézbesítést. Az oldal ezután azt írta, hogy csomagja hamarosan kézbesítésre kerül. Márk tizenöt percen belül telefonhívást kapott. A bankja kereste őt, a hívásban pedig arról értesítették, hogy bankkártyáját világszerte számos online tranzakcióhoz használták. Márk megdermedt, amikor rájött, hogy valójában semmilyen csomagról sem volt szó, az üzenet pedig nem volt más, csak egy átverés, aminek a célja a személyes adatainak – beleértve a bankkártyája adatait – megszerzése volt.

Mik azok az üzenetküldéses támadások? (Smishing)

Az üzenetküldéses támadások, amelyeket Smishingnek is neveznek (az SMS és a Phishing szavak kombinációja), akkor fordulnak elő, amikor a kiberbűnözők SMS-t, szöveges üzeneteket vagy hasonló üzenetküldési technológiákat használnak arra, hogy megtévesszenek minket, és olyan cselekvésre vegyenek rá, amit nem lenne szabad megtennünk, például bank- vagy hitelkártya-adataink megadására vagy rosszindulatú alkalmazások telepítésére. Az e-mailes adathalász támadásokhoz hasonlóan a kiberbűnözők gyakran próbálnak az érzelmeinkre hatni, például sürgetéssel, vagy kíváncsiságkeltéssel. Az üzenetküldéses támadásokat azonban az teszi igazán veszélyessé, hogy a szövegben sokkal kevesebb információ és nyom található, mint az e-mailekben, így azt is sokkal nehezebb észlelni, hogy valami nincs rendben.

A kiberbűnözők néha kombinálják a telefonos és üzenetküldéses támadásokat. Például először egy szöveges üzenetet küldenek – mintha az a bankunktól érkezne – amelyben egy sürgős kifizetés engedélyezésére kérnek. Az üzenetben azt kérik, hogy válaszoljunk IGEN-nel vagy NEM-mel. Ha válaszolunk, a kiberbűnözők tudni fogják, hogy „horogra akadtunk”, és fel fognak hívni, mintha a bankunk csalásmegelőzési osztályáról telefonálnának. Ezután megpróbálnak rávenni bennünket arra, hogy eláruljuk pénzügyi és hitelkártya adatainkat, vagy megadjuk netbankos fiókunk bejelentkezési felhasználónevét és jelszavát.

A támadások felismerése és megállítása

A támadások leggyakoribb jelei az alábbiak:

- **Sürgősség**: Bármilyen üzenet, amely hatalmas sürgősség érzetét kelti, amikor valaki megpróbál siettetni vagy nyomást gyakorolni ránk, hogy cselekedjünk, például azt állítva, hogy a fiókjainkat lezárják vagy börtönbe kerülünk.
- **Kapzsiság:** Túl jól hangzik az üzenet ahhoz, hogy igaz legyen? Nem, sajnos nem nyertél egy új, ingyen iPhone-t.
- **Kíváncsiság**: Ha olyan üzenetet kapunk, amelyről azt állítják, rossz számra küldték, vagy egy ismeretlen személy csak annyit ír, hogy "szia", ne válaszoljunk rá, és ne próbáljuk meg felvenni a kapcsolatot a küldővel; egyszerűen csak töröljük az üzenetet. Ezek a kiberbűnözők kísérletei arra, hogy beszélgetésbe bonyolódjanak velünk, például egy romantikus csalás érdekében.
- **Személyes** információ**:** Az üzenet olyan webhelyre mutat, amely személyes – például bankkártya – adatokat, jelszavakat vagy egyéb bizalmas információkat kér, amelyekhez másoknak nem szabadna hozzáférnie**?**
- **Fizetések**: Legyünk nagyon gyanakvóak a szokatlan fizetési kérelmekkel szemben, mint például azok, amik a Western Union-on vagy a Bitcoin-on keresztül történnek.

Ha látszólag egy hivatalos szervezettől kaptunk üzenetet, amelyben figyelmeztetnek bennünket, akkor közvetlenül a szervezettel vegyük fel velük a kapcsolatot! Ne az üzenetben szereplő telefonszámot használjuk, inkább egy megbízható számot hívjunk! Például, ha szöveges üzenetet kapunk a bankunktól, amelyben jelzik, hogy probléma van a bankszámlánkkal vagy a hitelkártyánkkal, vegyük fel a kapcsolatot közvetlenül a bankkal vagy a hitelkártya-társasággal, felkeresve az adott pénzintézet hivatalos weboldalát, vagy közvetlenül tárcsázva őket a bankkártya vagy hitelkártya hátulján lévő telefonszám alkalmazásával. Ne feledjük továbbá, hogy a legtöbb kormányzati szerv, például az adó- vagy bűnüldöző szervek soha nem szöveges üzenetben, hanem inkább levélben keresnek meg minket.

Az üzenetalapú smishing támadások ellen mi magunk vagyunk a legfőbb védelmünk.

A szerzőről

Destiney Plaza a Carnegie Mellon Egyetem Szoftverfejlesztési Intézetének kiberbiztonsági mérnöke. Szeret inspiráló előadásokat tartani különböző közönségeknek, a kezdőktől egészen a kiberbiztonsági szakemberekig. CISSP minősítéssel, számítástechnikai alapképzéssel (BS) és információs rendszerek menedzsmentjében szerzett mesterfokozattal (MS) rendelkezik.

Források

Üzenetküldés: mit tegyünk és mit ne: https://www.sans.org/newsletters/ouch/messaging-dos-and-donts/
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)