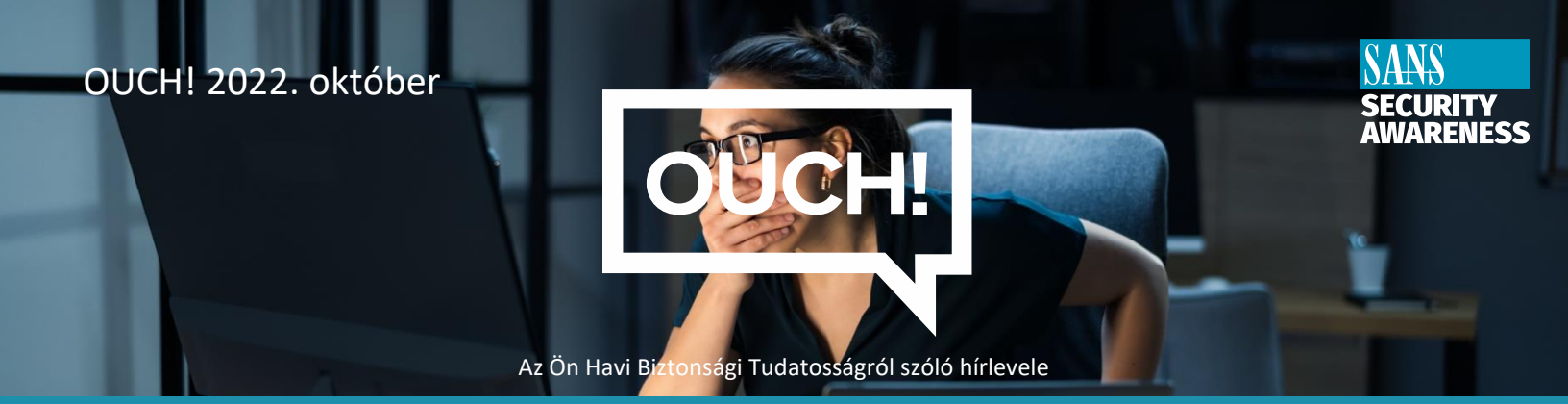
OUCH! 2022. október



Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Érzelmi triggerek – Így csapnak be minket a kibertámadók

Áttekintés

A kibertámadók folyamatosan új módszereket dolgoznak ki annak érdekében, hogy olyan dolgokra vegyenek rá bennünket, amelyeket nem szabadna megtennünk, mint például rákattintani a káros hivatkozásokra, megnyitni a fertőzött e-mail mellékleteket, ajándékutalványokat vásárolni vagy kiadni a jelszavainkat. Ráadásul gyakran különféle technológiákat és platformokat használnak a támadások során, például küldhetnek üzenetet e-mailben, SMS-ben, vagy a közösségi platformokon keresztül, illetve fel is hívhatnak minket telefonon. Noha mindez soknak tűnhet, a legtöbb ilyen támadás ugyanarról szól: az érzelmekről. Ha ismerjük, hogy a kibertámadók mivel próbálnak érzelmeket kiváltani, könnyebben ismerhetjük fel a támadásaikat, függetlenül attól, hogy épp melyik módszerrel próbálkoznak.

Minden az érzelmekről szól

Minden az érzelmekkel kezdődik. Mi, emberek, túl gyakran érzelmeink alapján hozunk döntéseket a tények helyett. Olyannyira jellemző ez, hogy egy egész kutatási terület foglalkozik az úgynevezett „viselkedési közgazdaságtannal”, olyan kutatók vezetésével, mint például Daniel Khaneman, Richard Thaler és Cass Sunstein. Szerencsénkre, ha tudjuk, hogy milyen érzelmi triggerekre (érzelmeket keltő tényezőkre) kell figyelmesnek lennünk, a legtöbb támadást észrevehetjük, sőt meg is állíthatjuk. Az alábbiakban sorra vesszük a leggyakoribb érzelmi triggereket, amelyekre figyelni kell. Előfordul, hogy a kibertámadók ugyanabban az e-mailben, szöveges üzenetben, közösségi média posztban vagy telefonhívásban az alábbi érzelmek különféle kombinációját alkalmazzák, még hatékonyabbá téve ezzel a támadást.

Sürgetés: A sürgetés az egyik leghatékonyabb érzelmi trigger, ennélfogva ez a leggyakoribb. A kibertámadók gyakran félelmet, szorongást, vagy hiányérzetet próbálnak kiváltani, hogy hibás döntésre sarkalljanak bennünket. Megtörténhet például, hogy kapunk egy sürgető e-mailt a munkahelyi vezetőnktől, amelyben azt kéri tőlünk, hogy azonnal küldjünk el neki néhány bizalmas dokumentumot, holott valójában ő egy kibertámadó, aki a főnökünknek adja ki magát. Vagy szöveges üzenetet kapunk egy támadótól, aki egy hivatalos szervnek kiadva magát, arról tájékoztat minket, hogy lejárt az adófizetési határidő, most azonnal fizetnünk kell, különben börtönbe kerülünk.

Harag: Üzenetet kapunk egy számunkra fontos politikai, környezetvédelmi vagy társadalmi kérdés kapcsán, – valami olyasmit, hogy “nem fogja elhinni, mit csinál ez a politikai csoport vagy nagyvállalat!”

Meglepetés / Kíváncsiság: Néha a legszűkszavúbb támadások a legsikeresebbek. Egy meglepetés mindig felkelti a kíváncsiságunkat, ezért többet akarunk tudni. Ez egy nem várt dologra adott érzelmi reakció. Például, amikor üzenetet kapunk, hogy a csomagunkat nem tudták kézbesíteni, és egy linkre kattintva juthatunk több információhoz a kiszállításról, pedig valójában semmit sem rendeltünk. Arra csábítanak, hogy tudjunk meg többet erről. Sajnos valójában nincs is ilyen csomag, csupán károkozási szándék vár ránk a link túloldalán.

Bizalom: Amikor a támadók olyan nevet vagy márkát használnak, amiben megbízunk, és ezáltal cselekvésre késztetnek. Például az üzenet látszólag a bankunktól, egy ismert jótékonysági szervezettől, egy megbízható kormányzati szervtől vagy akár egy ismerősünktől érkezik. Csak azért, mert egy e-mail vagy szöveges üzenet egy általunk ismert szervezet nevét és logóját használja, még nem jelenti azt, hogy az üzenet valóban tőlük származik.

Izgalom: SMS-üzenetet kapunk a bankunktól vagy a szolgáltatónktól, amelyben megköszönik, hogy időben teljesítettük a befizetéseket. A szöveges üzenet ezután tartalmaz egy linket, ahol ezért cserébe jutalom vár ránk – például egy új iPad – milyen izgalmas! Ez a hivatkozás egy olyan weboldalra vezet, amely bár hivatalosnak tűnik, azonban minden személyes adatunkat elkéri, vagy meg kell adnunk bankkártya adatainkat, hogy fedezni tudjuk a szállítási/kezelési költségeket. Az üzenet küldője valójában egy kibertámadó, aki egyszerűen ellopja a pénzünket vagy a személyazonosságunkat.

Empátia / Együttérzés: A kibertámadók kihasználják jóindulatunkat. Például miután egy katasztrófáról számolnak be a hírekben, általában hamis e-mailek milliói kerülnek kiküldésre, amelyekben a kiberbűnözők az áldozatokat segítő jótékonysági szervezetnek adják ki magukat, és pénzt kérnek tőlünk.

Ha jobban megértjük ezeket az érzelmi triggereket, sokkal felkészültebben vesszük majd észre és állítjuk meg a kibertámadókat, függetlenül attól, hogy azok milyen csalit, technológiát vagy platformot használnak.

A szerzőről

My-Ngoc Nguyen a Secured IT Solutions vezérigazgatója. 20 éves tapasztalattal rendelkezik kiberbiztonsági és kockázatkezelési programok irányításában és kidolgozásában az amerikai szövetségi kormányzat, valamint a magánszektor számára egyaránt. Emellett rendszeresen oktat a SANS MGT512 kurzuson. https://www.linkedin.com/in/menop, My-Ngoc Nguyen | SANS Institute @MenopN.

Források

Pszichológiai manipuláción alapuló támadások: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Vishing – csaló telefonhívások: https://www.sans.org/newsletters/ouch/vishing/
A három leggyakoribb közösségi média csalás: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Így ismerjük fel, és kezeljük az üzenetküldéses támadásokat!: https://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
Egyre trükkösebbek az adathalász támadások: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/

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