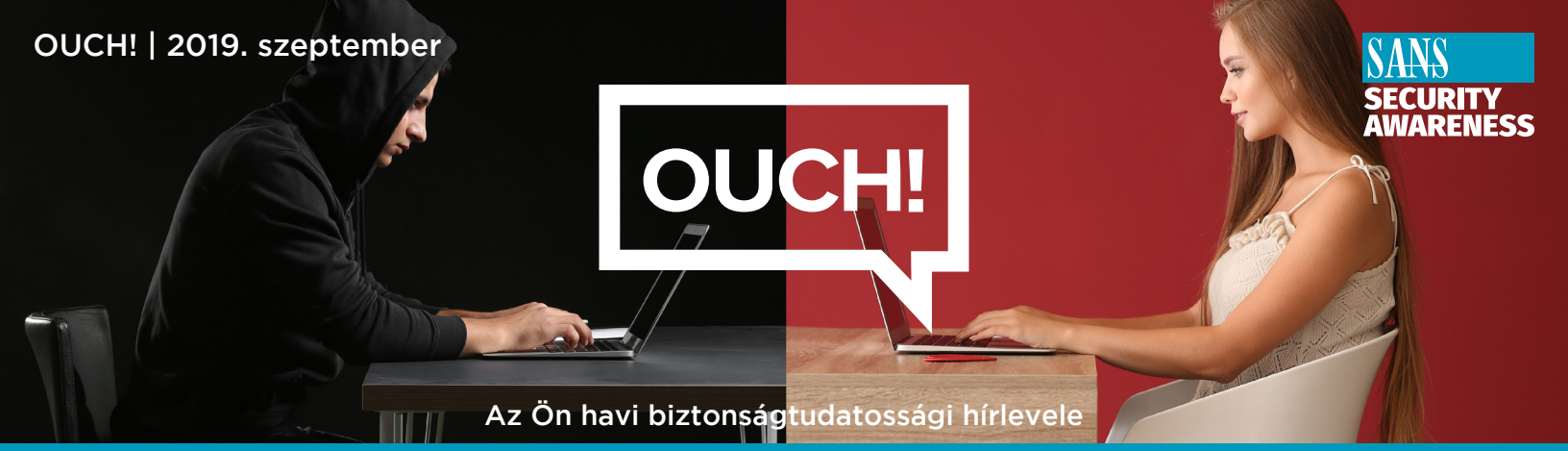
OUCH! | 2019. szeptember



SANS SECURITY AWARENESS

OUCH!

Az Ön havi biztonságtudatossági hírlevele

Átverés a közösségi médián keresztül

Áttekintés

Sokan kaptunk már adathalász e-maileket, akár a munkahelyünkön, akár otthon. Ezek olyan e-mailek, amelyek valósnak tűnnek, például mintha a bankjától, a főnökétől, vagy kedvenc webshopjától érkeztek volna. A valóságban azonban ezek támadások, amelyek sürgetéssel vagy megtévesztéssel arra próbálják rávenni, hogy olyat cselekedjen, amit nem kellene, mint például, hogy nyisson meg egy fertőzött mellékletet, ossza meg jelszavát, vagy hogy utaljon pénzt. A kihívás abban rejlik, hogy hiába tudjuk egyre jobban felismerni és megállítani ezeket a támadásokat, egyre több kiberbűnöző igyekszik újabb és újabb módokon kapcsolatot teremteni és csapdába csalni az embereket.

Átverési vagy becsapási kísérlet bármilyen Ön által használt kommunikációs formában megtörténhet, a Skype-tól, a WhatsApp-tól, a Slack-től egészen a Twitterig, Facebookig, Snapchatig, Instagramig, vagy akár a játék alkalmazásokig. A kommunikáció ezeken a platformokon, illetve csatornákon sokkal informálisabbnak, megbízhatóbbnak tűnik, éppen ezért használják őket a támadók mások becsapására. Ráadásul a mai technológiával a támadóknak sokkal könnyebbé vált a világ bármely pontjáról másvalakinek kiadni magukat. Fontos észben tartania, hogy bármely kommunikáció, amit folytat, talán nem is az, aminek látszik, és hogy a személyek nem mindig azok, akinek kiadják magukat.

Kulcspontok

Alább találhatók a leggyakoribb nyomok, amelyek arra utalnak, hogy az üzenet, amit éppen most kapott, vagy a poszt, amit éppen most olvasott, egy támadás részét képezhették.

Sürgetés: Olyan üzenet, ami a sürgetés érzetét kelti, azáltal, hogy azonnali cselekvésre buzdít, mielőtt bármi rossz történne, például egy felhasználói fiók bezárásával, vagy börtönbe jutással fenyegetve Önt. A támadó a siettetéssel azt akarja elérni, hogy hibázzon.

Nyomásgyakorlás: Arra próbálják rábírni Önt, hogy kerülje meg vagy hagyja figyelmen kívül a munkahelyi irányelveket vagy eljárásokat.

Kíváncsiság: Erőteljes kíváncsiságérzet keltése vagy egy ajánlat, ami túl jó ahhoz, hogy igaz legyen. Nem, nem nyert a lottón.

Érzékeny információ: Nagyon érzékeny információk kérése, mint például a bankkártyájának száma, jelszava, vagy bármilyen információ, amit nem szívesen osztana meg mással.

Hivatali üzenetek: Üzenetek, amelyek egy hivatalos szervezettől érkeznek, azonban helyesírási hibákat vagy elütéseket tartalmaznak. A legtöbb állami intézmény nem használja a közösségi médiát közvetlen hivatalos kapcsolattartásra. Ha nem biztos benne, hogy az üzenet valós, hívja vissza a szervezetet egy megbízható, például a weboldalukon elérhető telefonszámon.

Megszemélyesítés: Üzenetet kap egy barátjától vagy egy kollégájától, de a szavak használata, hangsúlya nem ismerős. Amennyiben gyanakszik, hívja fel a feladót, és ellenőrizze, hogy ő küldte-e az üzenetet. A kiberbűnözőknek egyszerű elkészíteni egy olyan üzenetet, ami úgy jelenik meg, mintha az egy ismerősétől érkezett volna. Bizonyos esetekben megszerezhetik az egyik barátja fiókját, majd úgy tesznek, mintha a barátjuk lenne, és kapcsolatba lépnek Önnel. Különösen vigyázni kell a szöveges üzenetekkel, a Twitterrel és egyéb rövid üzenetformátumokkal, amelyeknél nehezebb megállapítani a feladó személyiségét.

Az ilyen csalások, átverések és támadások ellen Ön jelenti a legjobb védelmet. Ha egy poszt vagy üzenet furcsa vagy gyanúsnak tűnik, egyszerűen hagyja figyelmen kívül vagy törölje azt. Amennyiben ez olyan valakitől származik, akit személyesen is ismer, hívja fel telefonon, hogy ellenőrizze, valóban ő küldte-e.

Magyar Kiadás

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. Az NKI rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a https://nki.gov.hu oldalon olvasható.

A szerzőről

Dr. Jessica Barker *(@drjessicabarker) a kiberbiztonság emberi oldalának vezető személyisége. Társ ügyvezető a Cygentánál, ahol követi szenvedélyét, hogy pozitívan befolyásolja a kiberbiztonsági tudatosságot, viselkedést és kultúrát szerte a világon. A ClubCISO elnöke és népszerű előadó.*

Források

Pszichológiai befolyásolás:	https://www.sans.org/u/Uz6
Telefonos átverés:	https://www.sans.org/u/Uzb
Adathalászat megállítása:	https://www.sans.org/u/Uzg
Megszemélyesítéses átverések:	https://www.sans.org/u/Uzl