SANS SECURING THE HUMAN
NEMZETI KIBERVÉDELMI INTÉZET

OUCH! | 2017. Október

Havi biztonság tudatossági hírlevél mindenkinek

OUCH!

ebben a kiadásban...

Segítsünk másoknak biztonságuk megteremtésében

Áttekintés

Sokan magabiztosan mozognak a technológia világában, tudják hogyan használják azt biztonsággal és biztonságosan. Mások, barátok vagy családtagok nem ennyire magabiztosak. Valójában zavarodottak, ijedtek vagy félnek tőle, mely nagyon sérülékennyé teszi őket a mai támadók számára. A kiberbiztonságnak nem kell ijesztőnek lennie, tulajdonképpen elég egyszerű, ha egyszer megértik az alapokat. Valószínűleg szükségük van az útmutatásunkra, hogy segítsünk megérteni nekik az alapokat.

A szerzőről

Randy Marchany (Twitter: **@randymarchany**) a Virginia Tech informatikai biztonsági vezetője (CISO) valamint a SANS Intézet minősített oktatója.

Öt egyszerű lépés

Íme öt egyszerű lépés amivel segíthetünk másoknak, hogy túllépjenek ezen félelmeken és biztonságosan használhassák napjaink technológiáinak nagy részét. Még több információ található a pontokhoz a hírlevél végén lévő hivatkozásokon.

1. **Pszichológiai befolyásolás**: A pszichológiai manipuláció egy bevált módszer, amit a kibertámadók használnak, hogy átverjenek vagy rávegyenek embereket arra, hogy olyat tegyenek, amit nem kellene, például a jelszavuk megosztása, a számítógépük megfertőzése vagy érzékeny adatok megosztása. Ebben nincs semmi újdonság, csalók és szemfényvesztők évezredek óta léteznek. Az egyetlen különbség, hogy a bűnözők most ugyanazokat a módszereket az interneten keresztül alkalmazzák. Segíthetünk másokon, ha elmagyarázzuk nekik a leggyakoribb jeleit a pszichológiai befolyásolásos támadásoknak, mint amikor valaki sürgető hangnemet használ, amikor valami túl jól hangzik, hogy igaz legyen, vagy amikor a kibertámadó azt színleli, hogy olyasvalaki, akit jól ismerünk, de az üzenetei mégsem úgy hangzanak, mint ha a barátod írta volna. Hozzunk példákat a leggyakoribb pszichológiai befolyásolásos támadásra, mint az adathalász e-mailek, vagy a hírhedt Microsoft technikai támogatásos telefonhívások. Végül bizonyosodjuk meg róla, hogy a családtagjaink megértették, hogy soha ne adják meg jelszavukat senkinek vagy senkinek ne biztosítsanak távoli hozzáférést a számítógépükhöz.
2. **Jelszavak**: Az erős jelszavak kulcsfontosságúak ahhoz hogy megvédjük az eszközeinket és az online felhasználó fiókjainkat Családtagjainkkal együtt menjünk végig a biztonságos jelszó létrehozásának folyamatán. Javasoljuk a jelmondatok alkalmazását, mivel azt a legegyszerűbb begépelni és megjegyezni. A jelmondatok nem mások, mint több szóból álló jelszavak. Továbbá segítsünk nekik, a jelszókezelő program telepítésében és használatában. Nagyon fontos hogy egyedi jelszavunk legyen minden egyes eszközünkhöz és felhasználói fiókunkhoz. Ha a jelszókezelő használata nehéznek bizonyul, akkor javasoljuk, hogy írják le a jelszavaikat, melyeket biztonságos helyen tároljanak.Végül a fon-

Segítsünk másoknak biztonságuk megteremtésében

tosabb felhasználói fiókoknál segítsünk, a kétlépcsős hitelesítést (gyakran két faktoros hitelesítésnek nevezett) beállítani. A két lépcsős hitelesítés az egyik leghatékonyabb megoldás, amit tehetünk bármely felhasználói fiók biztonságáért.

3. **Javítások**: A rendszerek naprakészen tartása egy olyan alapvető lépés melyet bárki meg tud csinálni az eszközeik biztonságossá tételéhez. Ez nem csak a számítógépünk és mobil eszközeink esetében igaz, hanem bármire, ami kapcsolódik az internethez, mint a játék konzolok, hőmérők vagy akár a világítás és a hangszórók. A legegyszerűbb módja az eszközeink naprakészen tartásának, hogy engedélyezzük az automatikus frissítéseket, amikor csak lehetséges.
4. **Vírusirtó szoftverek**: Az emberek hibáznak, így néha rákattintunk vagy telepítünk olyan dolgokat, amikre nem kellett volna, így rendszerünk megfertőződhet. A vírusirtó szoftvereket arra tervezték, hogy megvédjen minket ezektől a hibáktól. A vírusirtó nem tud megállítani minden kártevőt, de segít azonosítani és megállítani a leggyakoribb támadásokat. Ezért bizonyosodjuk meg róla, hogy az összes otthoni számítógépünkön van telepítve, aktiválva és frissítve vírusirtó szoftver. Továbbá számos mai Vírusirtó szoftver már tartalmaz egyéb biztonsági technológiákat is, mint például tűzfalat vagy böngészőbe épülő biztonsági megoldást.
5. **Biztonsági mentések**: Amikor minden egyéb megoldás kudarcot vallott, gyakran a biztonsági mentések nyújtják az egyetlen megoldást arra, hogy visszaállítsunk olyan fájlokat, amiket önhibánkból veszítettünk el - például amikor rossz fájlt törlünk ki - vagy esetleg egy olyan kibertámadás miatt, mint a zsarolóvírus. Bizonyosodjuk meg róla, hogy a családunk és barátaink automatikus fájl mentést használnak. Gyakran a legegyszerűbb megoldások a felhő alapúak, melyek mentik fájljainkat óránként vagy bármikor, amikor módosítjuk azokat. Ezen megoldások nem csak az adataink mentését, hanem visszaállítását is megkönnyítik.

Segítsünk másoknak a technológia biztonságos használatában, osszuk meg velük ezt az öt egyszerű lépést.

Gyerekek biztonsága vendégségben

Ha otthonosan mozgunk a technológia világában, akkor nem csak magunkat tesszük biztonságossá, hanem segítünk gyerekeinknek is a biztonságuk megőrzésében. Amikor gyerekek meglátogatnak egy olyan rokont, aki nem járatos a technológia világában, mint például a nagyszülők, ezek a barátok vagy rokonok nem fognak úgy odafigyelni gyermekeink online biztonságára, mint ahogy azt mi magunk tennénk. Íme, néhány tanács , amit megtehetünk, hogy elősegítsük gyermekeink biztonságát akkor is, amikor meglátogatnak valakit, különösen ha ez a családon belül van.

- **Szabályok**: Bizonyosodjunk meg róla, hogy a gyerekek biztonságára vonatkozó szabályainkról, elképzeléseinkről tudnak az ismerőseink. Például hogy van e bármi szabály, hogy mennyi időt tölthetnek a gyerekek online, kivel beszélhetnek vagy milyen játékokkal szabad játszaniuk? Ne bízz abban, hogy a gyerekek elmondják ezen

Segítsünk másoknak biztonságuk megteremtésében

szabályokat a családtagoknak. Az egyik javaslat, hogy csináljunk egy „szabálylapot”, amit osszunk meg minden olyan rokonnal, akit gyakran meglátogatnak a gyerekek.

- **Kontorollok**: Ha a gyerek jobban ért a technológiához, mint az őt felügyelők, akkor ezt ki is használhatja. Például, ha, a gyerek adminisztrátori jogokat kér vagy szerez a nagyszülők számítógépéhez akkor azt tesz amit akar, például olyan játékot tölt le amivel nem akarjuk hogy játsszon. Győződjünk meg róla, hogy a rokonok megértik, hogy a gyerekeknek nem kell további hozzáféréseket adni azon túl, amivel már rendelkeznek.

Végül javasoljuk az embereknek, hogy iratkozzanak fel olyan forrásokra, mint az OUCH! hírlevél, hogy tovább képezhessék magukat. Ez egy minden hónapban több, mint 20 nyelven megjelenő ingyenes hírlevél. Iratkozzon fel a https://securingthehuman.sans.org/ouch -on.

További információ

Iratkozzon fel a havi OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a securingthehuman.sans.org/ouch/archives weboldalon.

Magyar Kiadás

A Nemzeti Kibervédelmi Intézet (NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. A Nemzeti Kibervédelmi Intézet 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 http://www.govcert.hu/ és a http://neih.gov.hu oldalon olvasható.

Hivatkozások

Pszichológiai befolyásolás:	https://securingthehuman.sans.org/ouch/2017#january2017
Jelmondatok:	https://securingthehuman.sans.org/ouch/2017#april2017
Jelszókezelő:	https://securingthehuman.sans.org/ouch/2017#september2017
Két-lépcsős hitelesítés:	https://www.securingthehuman.org/ouch/2015#september2015
Biztonsági mentés és helyreállítás:	https://securingthehuman.sans.org/ouch/2017#august2017
A mai online gyerekek biztonsága:	https://securingthehuman.sans.org/ouch/2017#may2017
Kiberhónap Magyarországon:	https://kiberhonap.hu/

Szerkesztette: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Fordította: Tikos Anita