OUCH! | 2015. május

Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadványban...

Generációs különbségek

Áttekintés

Többségünk magabiztosan és biztonságosan kezeli a modern technológiákat. Azonban a családban lehetnek olyan emberek, akik számára nem annyira természetes a számítógépek és egyéb eszközök használata, főleg akkor, ha ők nem az Internettel együtt nőttek fel. Az alábbi tanácsokat megfogadva sikeresen és biztonságosan át lehet hidalni a generációs szakadékból adódó problémákat, valamint lépéseket tehetünk annak érdekében, hogy biztonságosabbá tegyük a gyerekek számára az Internet használatát, de tartsuk észben, hogy ismerősök vagy családtagok meglátogatása esetén nem biztos, hogy ugyanaz a biztonsági környezet rendelkezésre fog állni. Ezért megmutatjuk azt is, hogy milyen lépéseket tehetünk annak érdekében, hogy biztonságosabb online környezetet teremtsünk akkor is, hogy a gyerekünk látogatóba megy valakihez.

A szerzőről

Brian Honan (Twitter **@brianhonan**) egy Dublinban élő, független biztonsági szakértő, az első írországi CERT alapítója és vezetője, az Europol Cybercrime Centre (EC3) tanácsadója, előadásokat tart a dublin-i egyetemen, valamint számos könyv és publikáció szerzője.

Az alapok

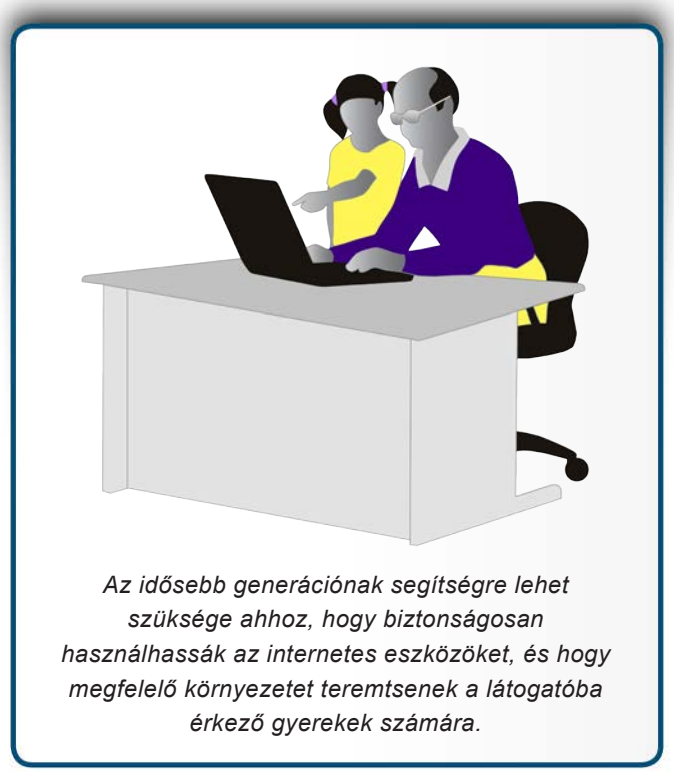
Kezdésnek érdemes megfontolni néhány egyszerű lépést a család minden tagjának, amelyekkel nagyban hozzá lehet járulni bárki biztonságos digitális életéhez. Azonban ha tudjuk, hogy valaki a családból nem képes önmaga végigmenni ezen az úton, akkor azzal érdemes közösen megtenni az utat, vagy pedig személyesen intézkedni a lépések megtételéről.

- **Pszichológiai manipuláció (social engineering)**: olyan példán kell bemutatni a pszichológiai manipuláció működését, amelyet mindenki képes megérteni. A csalók és szélhámosok már több ezer éve közöttünk élnek, így az ilyen támadások nem újak. Az egyetlen újítás az, hogy a régi módszereket az Internethez igazítják. Mutassunk olyan példákat, amelyekkel az elmúlt évtizedekben sok embert át tudtak már verni (klasszikus adathalász email-ek vagy a Microsoft ügyfélszolgálat telefonhívása). Ha mást nem is, azt mindenképpen érjük el, hogy a családtagok senkinek ne adják ki a jelszavukat, vagy ne engedélyezzék, hogy bárki hozzáférjen távolról a számítógépükhöz. Végezetül pedig nagyon fontos az is, hogy meggyőzzük őket, ha problémájuk vagy kérdésük van bármilyen email-lel vagy telefonhívással kapcsolatban, akkor nyugodtan forduljanak hozzánk.
- **Otthoni Wi-Fi hálózat**: ügyeljünk arra, hogy az otthoni Wi-Fi hálózat biztonságos legyen. A legalapvetőbb, hogy megváltoztatjuk a router adminisztrátori jelszavát, beállítjuk, hogy csak egy megfelelően erős jelszó megadása után lehessen csatlakozni, illetve hogy a legújabb titkosítást használjuk. Érdemes azt is megfontolni, hogy a Wi-Fi router-en beállítjuk az www.opendns.org biztonságos DNS szolgáltatást (vagy hasonlót). Az ehhez hasonló szolgáltatások nem csak abban segítenek, hogy elkerüljük a káros szoftverrel fertőzött

Generációs különbségek

weboldalakat, hanem azt is beállíthatjuk, hogy milyen oldalakat lehessen, vagy ne lehessen megnyitni, ami nagyon értékes lehet, ha a gyerek például látogatóba megy valahova.

- **Biztonsági frissítések telepítése**: ez az egyik legalapvetőbb lépés, amit megtehetünk annak érdekében, hogy biztonságban legyenek az internetes eszközök. Ezért győződjünk meg arról, hogy az összes hálózatra kapcsolódó számítógép és mobil eszköz, illetve az azokon használt alkalmazások mindig naprakész állapotban vannak, vagyis az összes biztonsági frissítés legyen letöltve és feltelepítve. Ennek legegyszerűbb módja, hogy engedélyezzük az automatikus frissítési funkciót.
- **Anti-vírus**: az emberek hibáznak, és néha olyan hivatkozásra kattintanak, vagy olyan alkalmazást telepítenek, amit nem kellett volna. Bár az anti-vírus szoftverek nem képesek minden káros szoftvert felismerni, a leggyakoribb fenyegetéseket azért meg tudják állítani. Ezért győződjünk meg arról, hogy minden eszközön van futó és naprakész anti-vírus szoftver.
- **Jelszavak**: az erős jelszó kulcsfontosságú abban, hogy meg tudjuk védeni mind az internetes eszközöket, mind pedig az online felhasználói fiókokat. Mutassuk be a családnak, hogy tudnak erős jelszavakat készíteni. Érdemes megfontolni a jelmondatok használatát, mert könnyebb emlékezni és használni is, illetve mutassuk meg a családtagoknak a jelszókezelő programok használatát. amennyiben erre nincs lehetőség, akkor írassuk le a jelszavakat, majd egy olyan biztonságos helyre tegyük el, ahol később hozzáférhetnek. A fontosabb online felhasználói fiókokhoz érdemes kétlépcsős hitelesítést használni.
- **Mentések**: amikor minden más elromlott, akkor a mentések menthetik meg a napunkat. Győződjünk meg arról, hogy minden családtagnak van egyszerű, megbízható, könnyen hozzáférhető fájlrendszer mentése.



Az idősebb generációnak segítségre lehet szüksége ahhoz, hogy biztonságosan használhassák az internetes eszközöket, és hogy megfelelő környezetet teremtsenek a látogatóba érkező gyerekek számára.

Havonta vagy maximum negyedévente győződjünk meg arról, hogy a fentieket mindenki betartja. Végső esetben fontoljuk meg egy távoli adminisztrációs szoftver telepítését a különböző eszközökre, de ilyenkor is használjunk erős titkosítást és egyedi jelszót.

Látogató gyerekek

Gyakran megesik, hogy ha a gyerekek látogatóba mennek - például a nagyszülőkhöz - akkor az otthon felállított szabályok nem lesznek érvényesek – ide értve azokat is, amelyeket kimondottan a gyerekek védelmében léptettünk életbe. Az alábbi tanácsok ezen a helyzeten tudnak segíteni.

Generációs különbségek

- **Szabályok**: győződjünk meg arról, hogy minden családtag ismeri azokat a szabályokat és elvárásokat, amelyek a gyerekekre vonatkoznak. Például van szabályunk arra, hogy a gyerekek mennyit játszhatnak online játékkal, vagy mikor használhatják a mobil eszközeiket? Ne számítsunk arra, hogy a gyerekek el fogják magyarázni az erre vonatkozó szabályokat a nagyszülőknek vagy más családtagnak. A legjobb módszer erre, hogy készítünk egy táblázatot, és megosztjuk azokkal, akikhez a gyerekek gyakran mennek látogatóba.
- **Irányítás**: ha a gyerekeink jobban értenek az Internethez, mint a nagyszülők, akkor azt ki is fogják használni. Például ha a gyerek rendszergazdai hozzáférést kér és kap a nagyszülők számítógépéhez, akkor lehet, hogy olyan játékokat fognak telepíteni, amiket mi nem engednénk meg. Győződjünk meg arról, hogy a családtagok tisztában vannak ezzel, és nem fognak további jogokat adni a gyerekeknek azon túl, mint ami eredetileg meg lett állapítva.

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a http://www.securingthehuman.org weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További információ a http://www.nisz.hu oldalon olvasható.

Hivatkozások

Pszichológiai manipuláció:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_hu.pdf
Az otthoni hálózat védelme:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201401_hu.pdf
A jelmondatokról:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_hu.pdf
A vírusvédelemről:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201412_hu.pdf
Online gyermekvédelem:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201304_hu.pdf
Telefonhívásos átverések (angolul):	http://www.onguardonline.gov/articles/0346-tech-support-scams
Internetbiztonság otthon:	http://www.securingthehuman.org/media/resources/STH-Poster-CyberSecureHome-Hungarian.pdf

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Fordította: Birkás Bence, Árvai Gábor, Pál Benyó