Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

- **Mi, mint felhasználók**
- **Jelszavak**
- **Frissítések**
- **Biztonsági mentések**

A biztonság megőrzése négy lépésben

Áttekintés

A technológia nemcsak egyre fontosabb szerepet tölt be az életünkben, hanem egyre bonyolultabbá is válik. Figyelembe véve a technológia fejlődési sebességét, nincs könnyű dolgunk akkor, ha naprakészek akarunk lenni biztonsági szempontból. Úgy tűnik, hogy mindig jönnek újabb és újabb útmutatók, tanácsok, amelyek megmondják, hogy mit kellene, és mit nem kellene tennünk. Bár a részletek változnak, az internetes biztonság alapjai tulajdonképpen ugyanazok, mint korábban. Függetlenül attól, hogy milyen technológiát használunk, vagy éppen hol vagyunk, javasolt az alábbi négy fontos lépés megtétele. Ezekről a lépésekről bővebben olvashatunk még a hírlevél „Hivatkozások” részében említett linkek alatt.

A szerzőről

Ryan Johnson tevékenységének fő fókuszát arra helyezi, hogy a szervezetek fel legyenek készülve az elkerülhetetlen biztonsági események elleni fellépésre. Ezen kívül oktatja a SANS Intézet Advanced Network Forensics kurzusának. Ryan elérhető a Twitteren a **@ForensicRJ** cím alatt.

1. **Mi, mint felhasználók**: az első és legfontosabb, hogy mindig észben tartsuk, a technológia önmagában nem fog megvédeni bennünket, a támadók mindig találnak egy egyszerű módszert arra, hogy kijátsszák a biztonsági megoldásokat. Ha meg akarják szerezni a jelszavunkat vagy a hitelkártyaszámunkat, akkor különféle egyszerű trükkökkel el fogják érni, hogy mi magunk adjuk meg nekik. Például kapunk egy telefonhívást valakitől, aki azt állítja, hogy a Microsoft technikusa és úgy látja, hogy fertőzött a számítógépünk. A valóságban egy kiberbűnözőről van szó, aki így akar hozzáférést szerezni a rendszerünkhöz. Vagy ha kapunk egy email-t, amelyben azt állítják, hogy a megrendelt csomagunkat nem tudják kiszállítani, és ezért kattintsunk egy hivatkozásra, ahol meg tudjuk adni a címünket. Ezzel szemben a link egy hamis weboldalra vezet minket, amin keresztül káros szoftverek segítségével fel tudják törni a számítógépünket. A zsarolóvírusok és vezetői átverések is így kezdődnek. Végső soron a támadások elleni legjobb védelem mi magunk vagyunk. Legyünk óvatosak, használjuk a józan eszünket, és így felismerhetjük a legtöbb támadást.

2. **Jelszavak**: a védekezés következő lépése az, hogy egyedi, erős jelszót válasszunk minden egyes Internetre kapcsolódó eszköznek, online fióknak és alkalmazásnak. Nagyon fontos, hogy erős és egyedi jelszó legyen! Az erős azt jelenti, hogy a hacker-ek vagy az automatikus programjaik ne tudják könnyen megfejteni. Elegünk van már a bonyolult jelszavakból, amiket nehéz megjegyezni és beírni? Próbáljuk ki inkább a jelmondatokat. Egyetlen

A biztonság megőrzése négy lépésben

szóból álló jelszó helyett használjunk több szóból állót, könnyen megjegyezhető mondatot, mint pl. “Hol van a kávém?”. Minél hosszabb egy jelmondat, annál erősebb. Az egyedi azt jelenti, hogy minden eszközt és online fiókot saját jelszóval védjük. Ez azt jelenti, hogy ha valaki megszerzi a jelszavunkat, akkor más internetes szolgáltatások és eszközök nem kerülnek veszélybe. Nem emlékszel az erős, egyedi jelszavakra? Nem kell aggódni, néha mi sem. Ezért javasolt, hogy mindenki használjon egy jelszókezelő programot, amely képes titkosított formában tárolni a mobil eszközökön vagy számítógépen használt online fiókok jelszavait.

Az említett négy biztonsági lépés megtételével jó úton járunk ahhoz, hogy megvédjük magunkat, miközben felhasználjuk a legújabb technológiákat.

Végezetül pedig mindig kapcsoljuk be a kétlépcsős hitelesítést minden olyan felhasználói fiókhoz, amely erre lehetőséget ad. A jelszavak egyedül már nem elegendőek az online fiókjaink védelmére, valami erősebbre van szükség, mint pl. a képlépcsős hitelesítés. Szükség van a jelszavaink használatára, de mindamellett egy második lépcsőt is igényel, ami lehet valami személyes tulajdonság (biometria), valami birtoklás alapú (mint pl. egy okostelefonra küldött kód vagy a telefonon lévő kódgeneráló alkalmazás). Engedélyezzük ezt az opciót minden egyes fióknál, ahol elérhető, még a jelszókezelő programnál is. A kétlépcsős hitelesítés valószínűleg az egyetlen és legfontosabb lépés, amit biztonságunk érdekében megléphetünk, és használata sokkal egyszerűbb, mint gondolnánk.

3. **Frissítések**: mindig legyünk naprakészek, telepítsük a legfrissebb operációsrendszer frissítéseket, a legújabb alkalmazásokat minden számítógépre, mobil eszközre vagy bármire, amivel csatlakozunk az Internetre! A kiberbűnözők folyamatosan keresik az aktuálisan használt technológiákban lévő sebezhetőségeket. Ha találnak egy sérülékenységet, akkor speciális programok segítségével kihasználják azokat, hogy feltörjék az eszközeinket, bármilyen technológiát is használjunk. Eközben a szoftvergyártók is folyamatosan dolgoznak azon, hogy az ismertté vált sérülékenységeket kijavítsák, majd ezeket frissítések formájában nyilvánosságra hozzák. Azzal, hogy mindig telepítjük a szoftvergyártók által készített javításokat, megnehezítjük a kiberbűnözők a dolgát, hogy betörjenek a számítógépünkbe. Ennek érdekében - amikor lehetőségünk van rá - kapcsoljuk be az automatikus frissítést. Ezt a szabályt ne csak a számítógép és mobil készülék esetén tartsuk szem előtt, hanem minden olyan eszköz esetén, amely kapcsolódik az Internetre – TV, baba monitor, otthoni router, játékkonzol, vagy akár az autónk. Ha a számítógépünk operációs rendszere, mobil eszközünk, vagy egy általunk használt technológia már nem támogatott és nem érhető el hozzá új frissítés, javasolt olyan új verzió beszerzése, amin van támogatás.

A biztonság megőrzése négy lépésben

4. **Backups**: annak ellenére, hogy megteszünk minden óvintézkedést, előfordulhat, hogy mégis feltörik valamelyik eszközünket vagy fiókunkat. Az ilyen esetekben csak akkor lehetünk teljesen biztosak abban, hogy megszabadultunk a káros szoftver okozta fertőzéstől, ha teljesen töröljük az eszközön lévő rendszert, és újratelepítjük azt. Ha például a támadó megakadályozott bennünket abban, hogy hozzáférjünk a személyes állományainkhoz, képeinkhez, dokumentumainkhoz, stb., akkor az egyetlen lehetőségünk az, hogy egy korábbi biztonsági mentésből helyreállítjuk ezeket. Azért, hogy egy hasonló esetben cselekedni tudjunk, nagyon fontos, hogy rendszeresen készítsünk biztonsági mentést a személyes adatainkról, illetve hogy ellenőrizzük azt is, hogy a mentésből helyre tudjuk állítani azokat. Az operációs rendszerek és mobil eszközök többsége támogatja az automatikus mentést. Továbbá, javasolt, hogy biztonsági mentéseinket a felhőben vagy offline tároljuk, védve ezzel a kiberbűnözőktől.

További Információ

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

Az adathalászatról:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201512_hu.pdf
A jelszókezelőkről:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_hu.pdf
A kétlépcsős hitelesítésről:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_hu.pdf
A jelmondatokról:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_hu.pdf
A biztonsági mentésekről:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_hu.pdf

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Fordította: Birkás Bence