Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadványban...

- **Előkészületek**
- **Elveszett vagy ellopott eszközök**
- **Wi-Fi hozzáférés**
- **Nyilvános számítógépek**

Biztonságban az utazás alatt

Áttekintés

Az OUCH! ehavi számának témája az utazások alatti biztonságos Internet kapcsolat és ügyintézés.

A szerzőről

Steve Armstrong a Logically Secure-nél a kiberbiztonsági események kezelését irányító technikai igazgató, a SANS minősített oktatója, illetve a SANS korábbi kurzusainak szerzője. A Twitter-en **@Nebulator**, a Google+ közösségi oldalon pedig **+SteveArmstrongSecurity** csatornán található meg.

Előkészületek

Amíg az otthoni vagy munkahelyi internetelérésünk valószínűleg biztonságos, utazás közben mindig azt kell feltételeznünk, hogy olyan hálózatokhoz kapcsolódunk, amelyek nem biztonságosak. Soha nem tudhatjuk, hogy ki kapcsolódik még az általunk használt hálózathoz, illetve milyen veszélyt jelenthet ez számunkra. Azonban néhány egyszerű intézkedés megtételével utazás közben is sikeresen megvédhetjük az adatainkat. Az utazás előtt 1-2 héttel:

- Döntsük el, milyen adatra nem lesz szükségünk az utazás alatt, és az ilyet töröljük le az összes eszközről, amit magunkkal viszünk. Ez nagymértékben csökkenti a lehetséges károkat abban az esetben, ha ellopnák, vagy csak egyszerűen eltűnne az adott eszköz, illetve ha például valamiért lefoglalnák azt a határon. Ha munkával kapcsolatos utazásról van szó, akkor kérdezzük meg a felettesünket, hogy a munkáltató biztosít-e alternatív eszközöket az út idejére.
- Külföldi utazás előtt nézzünk utána, hogy az adott országban milyen konnektorokat használnak, mert lehetséges, hogy csak átalakítóval tudjuk majd feltölteni az eszközöket. Utána kell nézni annak is, hogy a mobil szolgáltató milyen plusz költségeket számít fel a szolgáltatás külföldről történő adatforgalom igénybevétele miatt. Ilyen esetben érdemes lehet kikapcsolni az adatforgalmat esetleg új szerződést kötni az utazás idejére.
- Telepítsünk olyan alkalmazást, amivel távolról nyomon lehet követni az eszközt. Ellopás vagy elvesztés esetén ennek segítségével törölni is lehet róla minden adatot. Sok mobil eszközben eleve benne van ez a funkció, és csak engedélyezni kell. (Tartsuk észben, hogy ennek a funkciónak az igénybevételéhez internetelérés szükséges.)

1-2 nappal az utazás előtt:

- Frissítsük az eszközt, az alkalmazásokat és az antivírus szoftvert a legújabb verzióra.
- Engedélyezzük a megfelelő biztonsági beállításokat (például tűzfal).
- Állítsunk be egy erős jelszót. Ezzel meg tudjuk akadályozni, hogy az eszköz ellopása vagy elvesztése esetén

Biztonságban az utazás alatt

hozzá lehessen férni a rajta lévő információkhoz.

- Titkosítsuk az eszközt, így az eszköz ellopása vagy elvesztése esetén ne lehessen hozzáférni a rajta lévő információkhoz. Bizonyos készülékek (például iPhone) ezt automatikusan megteszik, ha beállítunk valamilyen jelszót.
- Készítsünk egy teljes mentést az eszközről. Ha valami történik az eszközzel, akkor is megmarad minden adat egy biztonságos helyen.

Az utazás alatti biztonság kulcsa az, hogy még indulás előtt tegyünk óvintézkedéseket az eszközeinkkel kapcsolatban. Ne veszítsük eszközeinket szem elől és kizárólag titkosított csatornát használjunk az online ügyek intézéséhez.

Elveszett vagy ellopott eszközök

Utazás alatt mindig gondoskodjunk a készülék fizikai értelembe vett biztonságáról! Például soha ne hagyjuk az autóban olyan helyen, ahol más is láthatja, mivel a bűnözők simán betörik miatta az autó üvegét, és elemelik azt, ami megtetszik nekik. Meg kell fontolni a kábel-zár használatát, amelynek segítségével fizikailag is tudjuk rögzíteni például a laptop-ot. Bár a bűnözés komoly kockázatot jelent az értékeinkre, még mindig nagyobb eséllyel veszítjük el azokat, mintsem hogy ellopnák tőlünk. A Verzion egy 10 éves tanulmánya szerint nagyjából 15-ször nagyobb a kockázata annak, hogy elhagyjuk valahol az eszközeinket, mint annak, hogy ellopják azt. Emiatt mindig duplán ellenőrizzük, hogy megvan-e minden eszközünk, például a reptéri biztonsági ellenőrzéskor, amikor kiszállunk a taxiból, kijelentkezünk a hotelből, vagy éppen elhagyjuk a repülőgépet.

Wi-Fi hozzáférés

Utazás közbeni Internet elérés általában nyilvános Wi-Fi használatot jelent, ami lehet például a hotelben, a repülőtéren vagy egy kávézóban. A nyilvános Wi-Fi-vel nem csak az a gond, hogy nem tudjuk, ki helyezte üzembe, hanem az is, hogy nem tudjuk, ki más csatlakozik még hozzá. Emiatt ezekre úgy kell tekinteni, mint nem megbízható hálózatokra, és emiatt kell a korábban említett intézkedéseket megtenni. Továbbá vegyük figyelembe, hogy a Wi-Fi rádióhullámokat használ a mi eszközünk és a Wi-Fi hozzáférési pont közötti adatátvitelre. Ez pedig azt eredményezi, hogy bárki, aki a közelünkben van, képes lehallgatni ezt a kommunikációt.

Emiatt rendkívül fontos, hogy minden nyilvános Wi-Fi használat esetén titkosított adatátvitelt használjunk. Például ha a böngészőben megnyitunk egy weboldalt, akkor győződjünk meg arról, hogy az titkosított csatornát használ (ha a cím https:// karakterekkel kezdődik, és egy zárt lakat van a címsorban, akkor ilyen oldalról van szó). Ezen kívül használhatunk meg VPN-t is (Virtual Private Network), amely minden online aktivitásunkat titkosítani fogja. Ezt például igénybe vehetjük a saját munkáltatónkon keresztül, vagy akár vehetünk is ilyen szolgáltatást saját használatra. Ha nem áll rendelkezésre

Biztonságban az utazás alatt

megbízható Wi-Fi elérés, akkor még mindig van lehetőség arra, hogy okostelefonon keresztül érjük el az Internetet (ezt nevezik idegen szóval tethering-nek). (Ahogy korábban említettük, ennek komoly költségei lehetnek külföldön, aminek érdemes előzetesen utánajárni.)

Nyilvános számítógépek

Ne használjunk semmilyen nyilvánosan elérhető számítógépet például a hotelekben, könyvtárakban, kávézókban, mivel nem tudhatjuk, hogy ki használta előzőleg, és hogy nem fertőzte-e meg valamilyen káros szoftverrel véletlenül vagy szándékosan. Amikor csak lehetséges, olyan eszközt használjunk bármilyen online aktivitásra, amelyet csak mi használunk. Ha elkerülhetetlen, hogy nyilvánosan elérhető számítógép használata, akkor csak olyan szolgáltatást vegyünk igénybe, amely nem igényli a bejelentkezés és jelszó használatát.

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

Jelszavak:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201305_hu.pdf
Kétfaktoros hitelesítés:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_hu.pdf
Titkosítás:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201408_hu.pdf
Új tablet biztonságossá tétele:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201312_hu.pdf
Verizon DBIR 2014:	http://www.verizonenterprise.com/DBIR/2014/

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

