Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

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

Biztonságban az utazás alatt

Áttekintés

A legtöbbet akarjuk kihozni a velünk élő technológiákból, így van ez utazás alatt is. Az OUCH! ehavi számának témája az utazások alatti biztonságos Internet kapcsolat és eszközhasználat.

A szerzőről

Mark Williams a tennessee-i BlueCross Blueshield vállalati biztonsági rendszertervezője. Továbbá, SANS oktató és a chattanooga-i ISSA tagozat elnöke. Rengeteget utazik, így tisztában van a műszaki kütyüket érintő problémákkal.

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.

- A legbiztonságosabb információ az, amivel nem is rendelkezünk. 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 eszközöket kifejezetten az út idejére.
- Zárjuk mobil eszközeinket vagy laptopunkat erős képernyőzárral. Ezzel meg tudjuk akadályozni, hogy az eszköz ellopása vagy elvesztése esetén hozzá lehessen férni a rajta lévő információkhoz. Továbbá, állítsunk be vagy töltsünk le teljes tárhely titkosítást. A legtöbb mobil eszközön ez automatikusan aktiválódik a képernyőzár használatával.
- Állítsunk be vagy töltsünk le olyan szoftvert, ami lehetővé teszi az eszköz távoli követését, akár távoli törlését, az eszköz elvesztése vagy ellopása esetére.
- Frissítsük az eszközt, az alkalmazásokat és az antivírus szoftvert a legújabb verzióra.
- Végezzünk egy teljes biztonsági mentést minden eszközre. Így ha bármi történik út közben, biztonságos helyen lesznek az eszköz adatairól a másolatok.
- Nemzetközi utazásánál érdeklődjünk a szolgáltatónk külföldön elérhető csomagjairól. Gyakran magasabb díjat

Biztonságban az utazás alatt

számolnak a szolgáltatók a külföldi adatforgalomra, így érdemes lehet kikapcsolni az adatforgalmat vagy egy helyi eldobható SIM kártyát beszerezni a külföldi út idejére.

Elveszett vagy ellopott eszközök

Utazás alatt mindig gondoskodjunk a készülék fizikai értelemben 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. Amíg a lopás nyilván egy kockázat marad, a Verzion egy friss tanulmánya szerint nagyjából 100-szor nagyobb a kockázata annak, hogy elhagyjuk valahol az eszközeinket, mint annak, hogy ellopják azokat. 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.

Az utazás alatti biztonság kulcsa az, hogy még indulás előtt tegyünk óvintézkedéseket az eszközeinkkel kapcsolatban. Ne veszítsük eszközeinket szem elől és használjunk titkosítást az eszközökön.

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

Biztonságban az utazás alatt

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 a nyilvánosan elérhető számítógép használata, akkor csak olyan szolgáltatást vegyünk igénybe, amin publikus információ található, pl. időjárás vagy napi hírek. Bármilyen saját fiókba való bejelentkezéssel (pl. Google) csak a hackereket kísértjük.

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

A jelmondatokról:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_hu.pdf
A biztonsági mentésről:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_hu.pdf
A káros szoftverekről:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_hu.pdf
A titkosításról:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201606_hu.pdf
Az OUCH! archívum:	https://securingthehuman.sans.org/ouch/archives

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