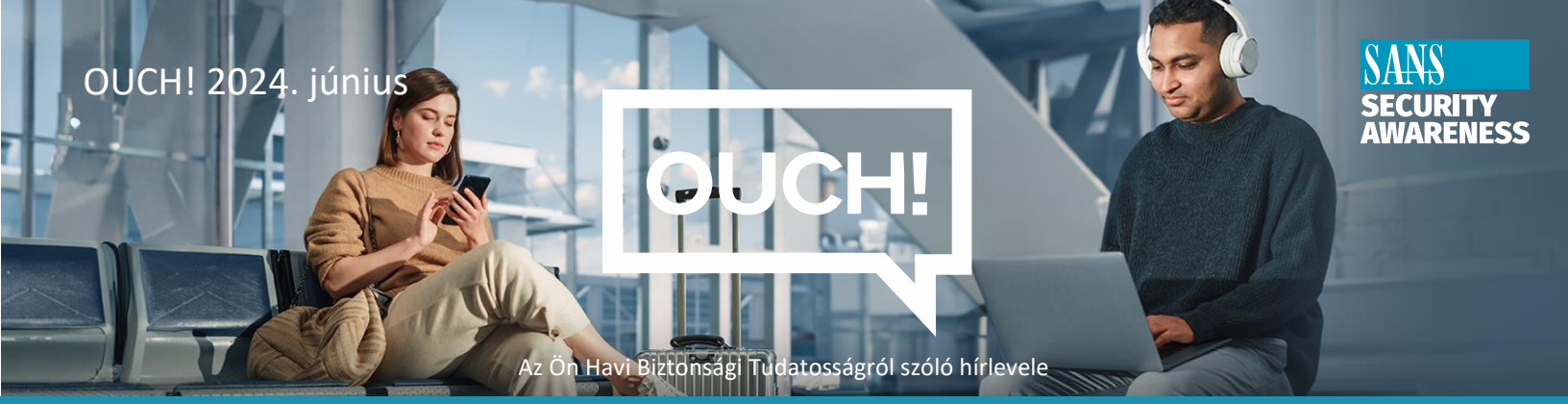
OUCH! 2024. június



SANS SECURITY AWARENESS

Nyaralni megy? Tippek, hogy utazása „kiberbiztonságban” teljen

Áttekintés

Nyakunkon a nyaralási szezon és hamarosan több millió ember utazik majd világszerte. Amennyiben mi is ezt fontolgatjuk, íme néhány tipp, amelyek segítenek megőrizni "kiberbiztonságunkat" az utazás alatt is.

Mobileszközök

Ne pakoljunk túl sok mindent: Csak azokat a mobileszközeinket vigyük magunkkal, amelyekre feltétlen szükségünk lehet a nyaralás során. „Mobileszközök” alatt értjük a laptopokat, tableteket, okostelefonokat, okosórákat, e-book olvasókat és a hordozható játékkonzolokat is. Minél kevesebb eszköz van nálunk, annál kevesebbet veszíthetünk el, vagy lophatnak el tőlünk. Ha már itt tartunk, tudta, hogy sokkal több esély van arra, hogy elveszíti a mobiltelefonját, mint hogy ellopnák azt? Sokszor a legnagyobb kihívás folyamatosan számon tartani a saját készülékeinket. Amikor elhagyjuk a szállodai szobát, éttermet, taxit, vonatot vagy repülőt, minden esetben tartsunk egy gyors ellenőrzést, és győződjünk meg arról, hogy minden készülékünk megvan. Ne felejtsük el duplán ellenőrizni a velünk utazó barátok vagy családtagok eszközeit sem. Különös tekintettel a gyermekekre figyeljünk, akik sokszor az ülésen vagy az étteremben felejtik a náluk lévő készülékeket.

Azokon az eszközökön, amelyeket magunkkal viszünk, frissítsük az operációs rendszert és alkalmazásokat a legújabb verzióra. Ennek a legegyszerűbb módja, ha engedélyezzük az automatikus frissítések telepítését. Ezáltal biztosak lehetünk abban, hogy a eszközünkön lévő sérülékenységek javításra kerülnek, és a legújabb biztonsági funkciók futnak majd rajta. Mindig használjunk képernyőzárat és ha lehetséges, győződjünk meg arról, hogy valamilyen módon távolról nyomon tudjuk követni készülékeink tartózkodási helyét. Ezen felül hasznos, ha van lehetőségünk arra, hogy távolról törölni tudjuk az eszköz tartalmát. Így ha egy eszközt elveszítünk vagy ellopják tőlünk, távolról nyomon követhetjük annak helyzetét, és/vagy törölhetjük róla személyes adatainkat. Végül pedig készítsünk biztonsági másolatot minden magunkkal vitt eszközről, így a rajtuk tárolt adataink probléma esetén visszaállíthatóak lesznek.

Wi-Fi kapcsolatok

Utazás közben előfordulhat, hogy csatlakozni szeretnénk egy nyilvános Wi-Fi hálózathoz. Ilyen például az ingyenes Wi-Fi hálózat a reptereken, kávézókban vagy éttermekben. Ne feledjük, hogy általában fogalmunk sincs arról, ki konfigurálta az adott nyilvános Wi-Fi hálózatot, így azt sem tudhatjuk, figyelik-e, és ha igen, hogyan teszik azt, valamint, hogy rajtunk kívül még ki csatlakozott hozzá. Lehetőleg kerüljük a nyilvános Wi-Fi hálózatokhoz történő csatlakozást, és inkább használjuk saját mobilinternetünket, a családtagok eszközei számára pedig hozzunk létre személyes hotspotot. Ezáltal biztosak lehetünk abban, hogy az eszközök megbízható Wi-Fi hálózathoz kapcsolódnak.

Annak érdekében pedig, hogy csökkentsük az utazás alatt használt mobiladat mennyiségünket, töltsük le előre azokat a tartalmakat, amikről tudjuk, hogy szükségünk lesz rájuk. Ezek lehetnek például térképek különböző verziói, hogy offline is könnyedén el tudjunk jutni a célunkhoz, vagy szórakoztató tartalmak, mint például hangoskönyvek, eBookok, játékok vagy filmek.

Nyilvános számítógépek

Kerüljük a nyilvános – például szállodai előcsarnokokban vagy kávézókban lévő - számítógépek használatát online fiókjainkba történő bejelentkezéshez, vagy más érzékeny adatainkhoz való hozzáféréshez. Sosem tudhatjuk, ki használta a számítógépet előttünk, és könnyen előfordulhat, hogy az eszközt véletlenül vagy szándékosan valaki korábban megfertőzte egy rosszindulatú - például billentyűleütéseket rögzítő - programmal. Ragaszkodjunk a saját, általunk ellenőrzött, megbízható eszközökhöz.

Közösségi média

Mindenki szereti megosztani a kalandjait ismerőseivel, de nem tudhatjuk, hogy ki olvassa még a bejegyzéseinket az egyes közösségi platformokon. Amennyire csak lehetséges, kerüljük a túl sok információ megosztását utazásunkról, inkább várjunk ezzel addig, amíg haza nem érünk. Ezenkívül soha ne tegyünk közzé képeket beszállókártyákról, vezetői engedélyekről vagy útlevelekről, mivel ez személyazonosság lopáshoz vezethet.

Vámeljárások és helyi törvények

Tanulmányozzuk át a célország(ok) törvényeit, mivel a jogaink országonként eltérőek lehetnek. Bizonyos tartalmak, amelyek itthon elfogadhatóak, más országokban akár illegálisak is lehetnek. Ezekkel legyünk tisztában, mielőtt útnak indulunk.

Ne feledjük, a vakáció a pihenés, a felfedezés és a szórakozás ideje. A fenti egyszerű lépések segítenek abban, hogy ezt biztonságban és biztonságosan tölthessük.

A szerzőről

Marisa Midler, Kiberbiztonsági szakember a Carnegie Mellon Egyetem Szoftverfejlesztői Intézet CERT részlegén. Marisa elismert Információbiztonsági Szakértő (CISSP), diplomáját a Carnegie Mellon (MsC) és a Pittsburgh-i Egyetemen (BsC/BA) szerezte.

Források

A Frissítés Ereje: https://www.sans.org/newsletters/ouch/power-updating/
Érzelmi triggerek – Így csapnak be minket a kibertámadók: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Egy Egyszerű Lépés Fiókjaink Biztonságossá Tételéért: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)