Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

A legjobb kiberbiztonsági tippek az ünnepi szabadság idejére

Áttekintés

Az ünnepi szezon közeledtével emberek milliói terveznek nagyobb utazást. Ha mi is ezt fontolgatjuk, íme néhány tipp, amelyek segítenek megőrizni kiberbiztonságunkat.

- **Mobileszközök**: A lehető legkevesebb eszközt vigyük magunkkal! Minél kevesebb eszköz van nálunk utazásaink során, annál kevesebbet veszíthetünk el, vagy lophatnak el tőlünk. Sokan nem is tudják, hogy sokkal nagyobb valószínűséggel veszítünk el egy mobileszközt, mint hogy azt ellopják tőlünk. Amikor elhagyunk egy szállodai szobát, éttermet, taxit, vonatot vagy repülőt, minden esetben tartsunk egy gyors eszközellenőrzést, és győződjünk meg arról, hogy minden készülékünk megvan! Ne felejtsünk el figyelmet fordítani a velünk utazó barátok vagy családtagok eszközeire sem. Különösen a gyermekekre figyeljünk, akik sok esetben az ülésen vagy az étteremben felejtik a náluk lévő telefonokat vagy játékokat.
  Azokat a digitális eszközöket, amiről úgy döntünk, hogy fontos magunkkal vinnünk, mindenképpen frissítsük, hogy a legújabb operációs rendszer és alkalmazások fussanak rajtuk! A képernyőzár mindig legyen aktiválva! Ha lehetséges, győződjünk meg arról, hogy valamilyen módon távolról nyomon tudjuk követni eszközeink tartózkodási helyét! Továbbá hasznos, ha van lehetőségünk arra is, hogy amennyiben szükséges, 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, készítsünk biztonsági másolatot minden magunkkal vitt eszközről, így a rajtuk tárolt adataink probléma esetén visszaállíthatóak lesznek!

- **Wi-Fi kapcsolatok:** Utazás közben előfordulhat, hogy csatlakoznunk kell egy nyilvános Wi-Fi hálózathoz. Ne feledjük azonban, hogy általában fogalmunk sincs arról, hogy ki konfigurálta az adott nyilvános Wi-Fi-hálózatot, így azt sem tudhatjuk, megfigyelik-e azt, valamint hogy rajtunk kívül még ki csatlakozott hozzá! Ezért lehetőleg kerüljük a nyilvános Wi-Fi hálózatokhoz történő csatlakozást, és inkább használjuk saját mobilnetünket, a családtagok eszközei számára pedig hozzunk létre személyes hotspot hálózatot! Ezáltal biztosak lehetünk abban, hogy az eszközök megbízható Wi-Fi hálózathoz kapcsolódnak. Ha ez nem lehetséges, és mindenképp egy nyilvános Wi-Fi hálózathoz kell csatlakoznunk (például repülőtéren, szállodában vagy kávézóban), használjunk virtuális magánhálózatot, amelyet gyakran VPN-nek neveznek. Ez egy olyan szoftver, amelyet laptopunkra vagy mobileszközeinkre is telepíthetünk, hogy segítsen megvédeni és anonimizálni a Wi-Fin keresztüli internetes forgalmunkat. Egyes VPN-megoldások olyan beállításokat is tartalmaznak, amelyek automatikusan bekapcsolják a VPN-t, amikor egy nem megbízható Wi-Fi hálózatokhoz csatlakozunk.

- **Nyilvános számítógépek**: Kerüljük a nyilvános számítógépek például a szállodai előcsarnokokban vagy kávézókban található számítógépek - használatát online fiókjainkba történő bejelentkezéshez, vagy más érzékeny adatokhoz történő hozzáféréshez! Sosem tudhatjuk, ki használta a számítógépet előttünk, és könnyen előfordulhat, hogy az eszközt véletlenül vagy szándékosan valaki korábban megfertőzte rosszindulatú - például billentyűleütést-figyelő - programmal. Ragaszkodjunk az általunk ellenőrzött, megbízható eszközökhöz!

- **Közösségi média**: Szeretünk másokat tájékoztatni utazásainkról és kalandjainkról a közösségi médián keresztül, de nem tudhatjuk, hogy mindenki a barátunk-e, aki online követ bennünket. 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!

- **Munka**: Ha szabadság alatt is dolgozunk (persze reméljük erre nem kerül sor!), feltétlenül ellenőrizzük a vonatkozó munkahelyi szabályzatot, beleértve azt is, hogy milyen eszközöket vagy adatokat vihetünk magunkkal, valamint, hogy hogyan tudunk biztonságosan csatlakozni távolról a munkahelyi rendszerekhez.

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

Princess Young a Southwest Airlines vezető elemzője, és a cég 60 000 alkalmazottja számára vezet kiberbiztonsági oktatást és képzést. Princess elkötelezett az alkalmazottak képzésével kapcsolatban, ezzel hatékonyan segítve őket abban, hogy részt vállaljanak a kiberbiztonsággal kapcsolatos közös felelősségből, beosztásuktól függetlenül.

Források

Mobilalkalmazások biztonságos használata: https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/
A frissítés ereje: https://www.sans.org/security-awareness-training/resources/power-updating/
Virtuális Magánhálózatok: https://www.sans.org/newsletters/ouch/Virtual-Private-Networks/
Biztonsági mentések: https://www.sans.org/security-awareness-training/resources/got-backups/

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