Sajber bezbednost na putovanju

Uvod

Sezona praznika se bliži i uskoro će milioni ljudi krenuti na put. Ako ste i vi među njima, u nastavku ovog teksta pronaći ćete savete kako da na putovanju ostanete bezbedni u sajber prostoru.

- **Mobilni uređaji**: Ne preterujte sa brojem mobilnih uređaja koje nosite na put. Što manje uređaja nosite na put, manje su i šanse da neki izgubite ili da vam ga ukradu. Možda toga niste bili svesni, ali mnogo se češće dešava da mobilni uređaji budu izgubljeni nego da budu predmet krađe. Zbog toga ne zaboravite da, svaki put kada napuštate hotelsku sobu, restoran, taksi, voz ili avion, proverite da li kod sebe imate sve svoje uređaje. Ukoliko sa vama putuju prijatelji ili članovi porodice podsetite i njih da obave ovu proveru. Naročito obratite pažnju na decu jer ona često ostave uređaj na svom sedištu ili u restoranu.

  Uređaje koje odlučite da ponesete na put obavezno ažurirajte tako da koriste najnoviju verziju operativnog sistema i aplikacija. Uključite opciju zaključavanja ekrana. Ukoliko je moguće, postarajte se da imate na raspolaganju način da udaljeno pratite svoje uređaje za slučaj da se izgube. Pored toga, može vam od koristi biti i opcija za udaljeno brisanje podataka na uređaju. Na taj način, možete da pratite i pronađete uređaj ili da sa njega udaljeno obrišete sve svoje osetljive podatke i naloge u slučaju da uređaj bude izgubljen ili ukraden. Konačno, napravite rezervnu kopiju (bekap) za sve uređaje koje nosite sa sobom, kako biste lako mogli da povratite svoje podatke u slučaju gubitka ili krađe.

- **Bežične mreže**: U toku putovanja možda ćete morati da se povežete na neku javnu bežičnu (Wi-Fi) mrežu. Imajte na umu da vi ne možete znati ko je i kako konfigurisao tu bežičnu mrežu, ko je nadgleda i ko je sve osim vas na nju povezan. Umesto da se povezujete na javnu bežičnu mrežu, kad god je to moguće povežite se na mrežu putem vašeg pametnog telefona i funkcije lične pristupne tačke (eng. *personal hotspot*). Takav način bežičnog povezivanja je bezbedniji i pouzdaniji. Ako to nije moguće i morate da se povežete na javnu bežičnu mrežu (na aerodromu, u hotelu, kafiću ili negde drugde), onda obavezno koristite virtuelnu privatnu mrežu (VPN). VPN zapravo predstavlja softver koji instalirate na vašem laptopu ili na mobilnom uređaju, a koji vam pomaže da zaštitite i anonimizujete vašu bežičnu vezu. Pojedina VPN rešenja poseduju i podešavanja za automatsko uključivanje VPN-a kad god se povezujete na nepouzdane bežične mreže.

© SANS Institute 2021

- **Javni računari**: Izbegavajte da se sa javnih računara, poput onih u hotelskim predvorjima ili u kafićima, prijavljujete na bilo koje svoje naloge ili pristupate osetljivim informacijama. Ne možete znati ko je taj računar koristio pre vas i da li ga je možda slučajno ili namerno zarazio malverom, kao što je na primer program koji beleži sve što se otkuca na tastaturi. Držite se onih uređaja koje vi kontrolišete i u koje imate poverenje.

- **Društvene mreže**: Svi mi volimo da putem društvenih mreža obaveštavamo prijatelje i rođake o našim putovanjima i avanturama, ali ne znamo uvek ko su sve osobe koje to prate na mreži. Izbegavajte objavljivanje informacija sa putovanja dok niste kod kuće. Razmislite o tome da utiske sa putovanja podelite tek kad se vratite kući. Osim toga, nikada nemojte objavljivati (postovati) slike propusnica za ukrcavanje, vozačkih dozvola ili pasoša jer to može dovesti do krađe identiteta.

- **Rad sa udaljene lokacije**: Ako planirate da radite dok ste na odmoru (nadamo se da ne!), obavezno unapred proverite kakva je politika vašeg poslodavca u vezi sa tim, uključujući i koje uređaje ili informacije vam je dozvoljeno da ponesete sa sobom, kao i kako da se bezbedno udaljeno povežete sa sistemima poslodavca.

Odmor bi trebalo da bude vreme za opuštanje, istraživanje i zabavu. Ovi jednostavni koraci će vam pomoći da to postignete na bezbedan način.

Gost urednik

Princes Jang je viša analitičarka u kompaniji Southwest Airlines. Bavi se edukacijom i obukama o sajber bezbednosti za oko 60.000 zaposlenih. Pomaže zaposlenima da razumeju da svi oni dele odgovornost za sajber bezbednost, bez obzira na ulogu ili titulu koju imaju.

Dodatni materijal

Bezbedno korišćenje mobilnih aplikacija: https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/
Moć ažuriranja: https://www.sans.org/newsletters/ouch/the-power-of-updating/
Virtuelne privatne mreže (VPN): https://www.sans.org/newsletters/ouch/Virtual-Private-Networks/
Imate li bekap: https://www.sans.org/security-awareness-training/resources/got-backups

Preveli za zajednicu: Dragan Ristić i Gordana Živanović
OUCH! Bilten objavljuje SANS Security Awareness program i distribuira se pod Creative Commons BY-NC-ND 4.0 license. Biltene je dozvoljeno deliti ili distribuirati pod uslovom da se sadržaj ne prodaje i ne modifikuje. Redakcija: Walter Scrivens, Phil Hoffman, Alan Waggoner, Les Ridout, Princess Young.