SANS Telekom Srbija

OUCH! | Februar, 2017

Mesečni bilten za podizanje svesti o bezbednosti informacija

OUCH!

U OVOM BROJU...



# Kako da budete bezbedni na putovanju

## Uvod

Želimo da budete u mogućnosti da koristite tehnologiju uvek u meri koja vam je potrebna, uključujući i dok ste na putovanju. U ovom tekstu naučićete kako da se na putovanjima povežete na Internet i koristite svoje uređaje na bezbedan način.

### Gost urednik

Mark Williams je projektant informacione bezbednosti (enterprise security architect) u kompaniji „BlueCross Blueshield of Tennessee“. On je i SANS instruktor i predsednik ISSA Chattanooga ogranka. Mark je često putovao i svestan je svih pitanja koja se javljaju kada sa sobom nosimo naše visokotehnološke spravice.

## Pre polaska

Dok vaša mreža kod kuće ili na poslu može biti bezbedna, trebalo bi da, kada putujete, mreže na koje se povezujete smatrate mrežama kojima se ne može verovati. Nikada ne možete znati ko se sve nalazi na mreži i šta on radi. U nastavku vam dajemo nekoliko jednostavnih saveta pre polaska na put koji mogu značajno zaštiti vas lično i vaše podatke.

- Najbezbednija je informacija koju nemate kod sebe. Utvrdite koji podaci vam neće trebati na uređajima koje nosite sa sobom i uklonite te informacije. Ovim značajno smanjujete eventualnu štetu u slučaju da su vaši uređaji izgubljeni, ukradeni ili ih je zaplenila carina ili bezbednosne službe na granici. Ako putujete službeno proverite sa svojim nadređenim da li postoji mogućnost da vam vaša organizacija dodeli neki od uređaja namenjenih za rad zaposlenih dok su na putovanju.
- Zaključajte vaše mobilne uređaje i/ili laptop jakim lozinkama ili šifrom (passcode, PIN). Na ovaj način neće svako moći da pristupi vašim informacijama u slučaju da uređaj bude izgubljen ili ukraden. Dodatno, omogućite ili instalirajte enkripciju diska (full disk encryption) na vašim mobilnim uređajima ili laptopu. Za većinu mobilnih uređaja, enkripcija je automatski omogućena kada koristite zaključavanje ekrana.
- Instalirajte ili aktivirajte softver na vašem uređaju tako da možete udaljeno da pratite lokaciju vašeg uređaja, pa i da ga udaljeno obrišete (tzv. wipe-ovanje) ako je izgubljen ili ukraden.
- Pre polaska na put ažurirajte vaše uređaje, aplikacije i antivirusni softver na najnovije verzije. Mnogi napadi su usmereni na sisteme sa zastarelim softverom.
- Kreirajte kompletne bekape svih vaših uređaja. Na taj način ćete, čak i ako se na putovanju nešto dogodi vašim

## Kako da budete bezbedni na putovanju

uređajima, vi i dalje imati vaše podatke na bezbednom mestu.

- Za putovanja van zemlje, proverite sa vašim provajderom mobilnih usluga kakav servisni plan imate na raspolaganju. Često provajderi skupo naplaćuju prenos podataka u romingu, pa ćete možda želeti da onemogućite prenos podataka putem mobilne mreže (isključite cellular data funkcionalnost) ili kupite lokalnu SIM karticu koju ćete korisititi u zemlji u kojoj boravite.

*Da biste bili bezbedni dok putujete, zaštitite vaše uređaje pre nego što krenete na put, čuvajte ih fizički zaštićene i neka sve vaše online aktivnosti budu enkriptovane.*

## Izgubljeni / ukradeni uređaji

Kada započnete vaše putovanje brižljivo se starajte o fizičkoj zaštiti vaših uređaja. Na primer, nikada ne ostavljajte uređaje u vašem automobilu tako da ih prolaznici mogu lako uočiti, jer lopovi mogu jednostavno razbiti prozor i pokupiti sve što ima neku vrednost. Iako kriminal zaista predstavlja rizik, prema poslednjem istraživanju kompanije Verizon, 100 puta je verovatnije da će osoba izgubiti svoj uređaj nego da će on biti ukraden. To znači da uvek treba dvaput proveriti da li je vaš uređaj još uvek uz vas dok putujete, posebno kada prolazite bezbednosne provere na aerodromu, izlazite iz taksija ili restorana, odjavljujete se iz hotelske sobe ili iskrcavate iz aviona. Ne zaboravite da proverite džep na sedištu ispred vas!

## Wi-Fi pristup

Pristup Internetu za vreme putovanja često znači upotrebu javnih Wi-Fi pristupnih tačaka, poput onih u hotelu, lokalnim kafeterijama ili na aerodromu. Postoje dva problema sa javnim Wi-Fi uslugama: nikada ne možete biti sigurni ko ih je zapravo omogućio niti možete znati ko je sve konektovan na njih. Zato im ne treba verovati. U suštini one su glavni razlog zbog koga ste pre polaska preduzeli prethodno navedene korake za zaštitu vaših uređaja. Pored toga, Wi-Fi koristi radio-talase, što znači da svako ko se nalazi u vašoj blizini može presresti ili nadzirati ove komunikacije. Iz navedenih razloga, ako koristite javni Wi-Fi, treba da se osigurate da su sve vaše online aktivnosti enkriptovane. Na primer, kada se konektujete koristeći pretraživač postarajte se da komunikacija sa veb sajtovima koje posećujete bude enkriptovana. U ovo se možete uveriti ako potražite 'HTTPS://' i/ili simbol zaključanog katanca u adresnom ili URL polju. Takođe, možda imate mogućnost da koristite VPN (Virtual Private Network) konfigurisanu tako da enkriptuje vašu celokupnu mrežnu aktivnost. Ova mogućnost vam može biti data zbog potreba vašeg posla ili možete kupiti VPN uslugu za vašu ličnu upotrebu. Jedna od opcija, kada

nemate poverenja u Wi-Fi, je i korišćenje mobilnog telefona kao pristupne tačke, vodeći računa o već pomenutoj činjenici da ovo može biti skupo na putovanjima van zemlje, te zahteva prethodnu proveru sa vašim provajderom mobilnih usluga.

## Javni računari

Ne koristite javne računare, poput onih u lobijima hotela ili u Internet kafeima, za prijavljivanje na ma koji nalog ili pristup osetljivim informacijama. Nemate pojma ko je pre vas koristio taj računar i da li ga je slučajno ili namerno zarazio. Kad god je to moguće, koristite samo uređaje nad kojima imate kontrolu i kojima verujete. U najboljem slučaju javni računari su korisni za pristup javnim informacijama kao što je vremenska prognoza ili najnovije vesti. Prijavljivanje na ma koji nalog, na primer na vaš Google nalog, može biti pozivnica za hakere koji možda čekaju u „zasedi“.

## Saznajte više

Prijavite se na OUCH! mesečni bilten za podizanje svesti o bezbednosti informacija namenjen svima, pročitajte prethodne brojeve OUCH!-a i saznajte više o SANS-ovim rešenjima za unapređenje svesti o bezbednosti informacija na našoj internet prezentaciji securingthehuman.sans.org/ouch/archives.

## Verzija na srpskom

Telekom Srbija kao društveno odgovorna telekomunikaciona kompanija pomaže prevođenje i distribuciju ovog biltena kako bi se unapredila svest korisnika informaciono-komunikacionih tehnologija o bezbednosti informacija.

## Dodatne informacije

| | |
|---|---|
| Propusne fraze: | https://securingthehuman.sans.org/ouch/2015#april2015 |
| Rezervne kopije i oporavak: | https://securingthehuman.sans.org/ouch/2015#august2015 |
| Šta je malver: | https://securingthehuman.sans.org/ouch/2016#march2016 |
| Enkripcija: | https://securingthehuman.sans.org/ouch/2016#june2016 |
| Arhive OUCH biltena: | https://securingthehuman.sans.org/ouch/archives |



Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis Cheryl Conley
Preveli: Dragan Ristić i Gordana Živanović