otpbanka

Čuvajte se besplatnih Wi-Fi mreža!

Kad Internetu pristupate putem besplatnih, bežičnih, Wi-Fi mreža izlažete se tome da netko, tko ne bi trebao imat pristup onome što radite – vidi sve što na svojim uređajima gledate i što na njima pišete...

Sjedite opušteno u kafiću, u kojem imaju besplatni Wi-Fi pristup Internetu. Pojeli ste solidan ručak i sad, uz kavu ili pivo, ne možete odoljeti i krenete prčkati po mobitelu ne biste li vidjeli je li vas tko zvao, imate li novih poruka, što se događa na Facebooku i, općenito, što je novo u svijetu. Kao da je to sad bitno. Na zimskom odmoru ste! Međutim, ne možete izdržati. Uz to, besplatno je. Wi-Fi u kafiću (hotelu, parku, aerodromu, autobusu,) je otvoren za sve. I tako, prvo bacite oko na e-poštu. Imate poruka. Izvadite svoj laptop i s njime se spojite na Internet, putem iste, besplatne, svima dostupne Wi-Fi mreže. „Prelistate" stranice novina koje inače čitate, bacite oko na Twitter, pogledate neki video na YouTubeu i dignete fotke koje ste jučer snimili, na svoj Instagram. Pa, zašto ne? Svi oko vas to rade, a Wi-Fi mreža koju koristite čini se sigurnom. No, je li to baš tako?

Prva linija obrane

Kad Internetu pristupate putem besplatnih, bežičnih, Wi-Fi mreža izlažete se tome da netko, tko ne bi trebao imat pristup onome što radite – vidi sve što na svojim uređajima gledate i što na njima pišete. Može čitati vašu elektroničku poštu, SMS poruke i poruke koje razmjenjujete s obitelji i prijateljima putem internetskih aplikacija za trenutno dopisivane, može gledati što radite na društvenim mrežama, prepisati lozinke koje koristite za pristup svom računu u banci i još štošta drugog. Zato, prije nego što vam padne na pamet da Internetu pristupite putem neke besplatne Wi-Fi mreže morate podići svu raspoloživu sigurnosnu obranu. Antivirusna aplikacija i firewall dvije su apsolutno nezaobilazne sigurnosne mjere koje bi vaši (mobitel i laptop) uređaji „po defaultu" morali imati u sebi i koji moraju biti stalno u funkciji. Provjerite to. Zatim, lozinke. Počevši od one s kojom pristupate svojim prijenosnim uređajima do onih kojima pristupate svojim društvenim mrežama i drugim online uslugama, moraju biti jedinstvene, dugačke i komplicirane, kako bi ih bilo što teže provaliti. Jasno je samo po sebi: istu lozinku ne smijete koristiti za pristup do više od jedne od usluga, a nikad nije previše ponoviti i ovo: vašem računu u banci nikad ne smijete pristupati putem Wi-Fi mreže, ma kako se ona činila sigurnom, a tvrtka koja njome upravlja pouzdanom. Nikad. Ili – učinite to. Na svoju štetu i sramotu. I nemojte poslije reći da vas nitko na to nije upozorio.

Ništa ne pretpostavljajte

Drugi sigurnosni korak - ako baš morate surfati Internetom dok ste na odmoru ili uživate u znamenitostima Pariza ili blagodatima neke egzotične lokacije uz more - provjerite koliko je sama Wi-Fi mreža na koju ćete se priključiti sa svojim uređajima – sigurna. Iako se čini očevidnim, provjerite je li ime bežične mreže kafića ili hotela u kojoj joj pristupate – točno. Nemojte pretpostaviti da je točno. Pitajte nekoga tko tamo radi kako glasi naziv njihove Wi-Fi mreže i usporedite to s onim što piše na ekranu vašeg uređaja. Zatim provjerite je li mreža zaštićena – to znači da joj se mora pristupiti putem posebne lozinke i da prefiks u adresnoj liniji internetskog preglednika počinje slovima htpps (ako nema s – nije sigurno). Još jedan savjet: čim se vratite doma, ili do neke druge sigurne veze na Internet, promijenite sve lozinke koje ste koristili dok ste surfali preko Wi-Fi mreža. Želite li još veću razinu sigurnosti kad pristupate Internetu putem besplatnih, javno dostupnih Wi-Fi mreža, koristite se uslugom pristupa putem neke virtualne privatne mreže (VPN). To je tehnologija koja stvara mrežu u mreži - hajmo tako reći - stvara mrežu samo za vas i dostupna je za manje od sto kuna. Pisali smo o tome već, na ovoj stranici, a jedan od alata kojim to možete učiniti je OpenDNS.

Pozornost je pola sigurnosti

I za kraj najvažnije. Iako se opet radi o nečemu što bi moralo biti jasno po sebi, prva stvar u samo-zaštiti dok Internetu pristupate putem javnih Wi-Fi mreža je: pozornost. Ako se, dok surfate takvim mrežama Internetom, pojavi neko sigurnosno upozorenje - nemojte ga ignorirati. Stanite i „skinite se" s te mreže. Možda je riječ samo o pogrešci administratora te mreže koji već dugo nije osvježio njen sigurnosni certifikat. Možda. A možda je riječ o hakeru koji čeka negdje u prikrajku baš na vas, još jednu naivnu, nepromišljenu žrtvu kojoj će sve lijepo što je doživjela na odmoru pokvariti šteta koju će pretrpjeti zbog puke lijenosti i nemara u pristupu Internetu putem besplatnih, javnih Wi-Fi mreža, bez nužne sigurnosne zaštite.