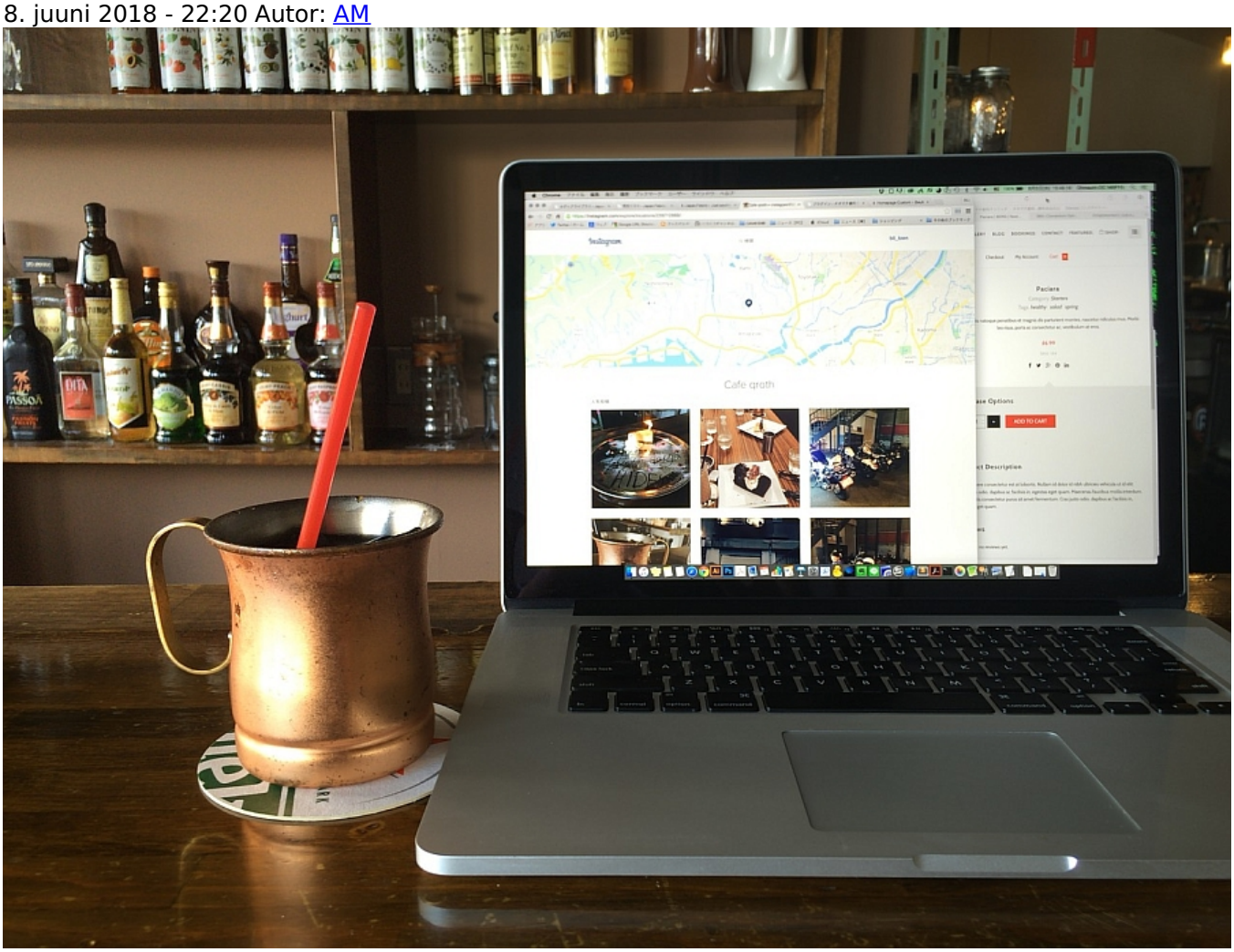
Hoiatus: suvel kolivad nutipetturid avalikesse WiFi võrkudesse

8. juuni 2018 - 22:20 Autor: AM



Suvepuhkusel avaliku WiFi kasutamine hotellis või kohvikus tähendab, et võid üsna lihtsalt sattuda nutipetturite ohvriks, kes kaaperdavad su kontod mõne lihtsa liigutusega.

„Avaliku WiFi kasutamisesse, eriti, kui seda pakutakse tasuta, peab suhtuma väga ettevaatlikult," rääkis Tele2 Eesti raadiovõrgu juht Tanel Sarri. „Kindlasti ei tohi mitte kunagi avalikus WiFis sisse logida oma pangakontodele või teistesse suuremat turvalisust nõudvatele kontodele," hoiatas Sarri.

Selleks, et veenduda, kas WiFi võrk on piisavalt turvaline, et veebis ringi liikuda, andis Tanel Sarri kolm lihtsat soovitust, mida meeles pidada.

1. Jälgi SSL ühenduse olemasolu ehk kas veebiaadress algab https-iga.

SSL ehk *Secure Sockets Layer* on standard, mis loob privaatse krüpteeritud ühenduse sinu arvuti veebibrauseri ja veebiserveri vahel. SSL vähendab oluliselt riski, et keegi saab avalikus WiFi võrgus sinu ühendusele ligi ja andmed kätte.

Sama ebaturvaline võib olla telefonist hotspoti abil jagatav internetivõrk, seega soovitame kasutada hotspoti võimalust vaid turvalises keskkonnas.

2. Ära sisesta ühelgi lehel tundlikku personaalset infot avalikus WiFi-s.

See, et ühendus on turvaline, ei tähenda, et leht ise on 100 protsenti turvaline. Seega ära kunagi sisesta oma personaalseid või krediitkaardiandmeid lehekülgedele, millega sa pole kursis või varasemast tuttav.

3. Kasuta äppide jaoks pigem 3G või 4G võrku.

Nutitelefonis äppe kasutades ei saa kontrollida SSL ühendust ning paljud äpid ei krüpteeri infot. Sestap

peab äppide kaudu kontodel käies, mobiilipanka kasutades või krediitkaardiga oste sooritades olema ettevaatlik ning soovitus on kasutada taolisteks tegevusteks oma telefoni andmeside ühendust ehk 3G või 4G võrku, mis on oluliselt turvalisem.

4. Kasuta VPNi.

On mitmeid viise, et end veebikurjamite eest kaitsta, kuid üks viis ületab kõik eelnevad – see on VPN-i kasutamine. Iga kord läbi VPN-i ühendust luues krüpteeritakse turvalisuse ja privaatsuse tagamiseks internetiühendus, kuhu ei pääse sisse ei interneti pakkuja, võrgu omanik kui ka häkker. Kui kasutad VPN-iga WiFi ühendust, on privaatsus ja turvalisus alati kaitstud. Soovitav oleks kasutada VPNi pakkujaid nagu näiteks Private Internet Access, TorGuard, IPVanish, CyberGhost või TunnelBear. On ka tasuta pakkujaid, kuid need ei pruugi olla alati kõigi vajalike sertifikaatidega või on suure kasutajate hulga tõttu aeglase ühendusega.

Uudised
Andmeside
Turvalisus
Võrguseadmed