Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

OUCH!

ŠIAME LEIDINYJE…

- Išankstinis pasiruošimas
- Pamesti ar pavogti įrenginiai
- Prieiga prie belaidžio tinklo
- Viešai prieinami kompiuteriai

Kaip likti saugiems keliaujant?

Apžvalga

Norime, kad technologijas galėtumėte maksimaliai išnaudoti bet kuriuo metu, net ir tada, kai keliaujate. Šiame naujienlaiškyje paaiškinsime, kaip keliaudami galite prisijungti prie interneto ir kaip saugiai naudotis įrenginiais.

Kviestinė redaktorė
Mark Williams, Tenesio įmonėje „BlueCross Blueshield“ dirbantis Įmonių saugos architektu. Taip pat jis yra SANS instituto paskaitų dėstytojas ir Informacinių sistemų saugumo asociacijos Čatanugos skyriaus prezidentas. Mark yra daug keliavęs ir puikiai supranta iškylančias problemas, kai į keliones kartu reikia pasiimti įvairius prietaisus.

Išankstinis pasiruošimas

Nors interneto tinklas namuose ar darbe greičiausiai yra visiškai saugus, tačiau keliaujant reikėtų suvokti, kad bet kuris tinklas, prie kurio jungiatės keliaudami, gali būti nepatikimas. Niekada nežinote, kas dar juo naudojasi ir ką jie jame veikia. Pateikiame keletą paprastų patarimų, kuriais vadovaudamiesi galite ne tik apsisaugoti, bet ir apsaugoti duomenis prieš išvykdami į kelionę.

- Saugiausia informacija yra ta, kurios su savimi neturite. Apgalvokite, kokių duomenų jums nereikės įrenginiuose, kuriuos imsite su savimi, ir tą informaciją iš jų pašalinkite. Taip žymiai sumažinsite žalą, jei įrenginius pamesite, juos kas nors pavogs, konfiskuos muitinė ar pasienio apsauga. Jei tai verslo kelionė, paklauskite savo vadovo ar jūsų organizacija suteikia įrenginių, kurie galėtų būti naudojami konkrečiai verslo kelionių metu.
- Apsaugokite savo mobiliuosius prietaisus ir/arba nešiojamą kompiuterį patikimu slaptažodžiu arba slaptu kodu. Tokiu būdu, kam nors pavogus įrenginį ar jums jį pametus, pašaliniai asmenys negalės prisijungti prie jame esančios informacijos. Be to, savo mobiliuosiuose prietaisuose ir nešiojamuose kompiuteriuose įjunkite arba įdiekite viso disko užšifravimą. Daugumoje mobiliųjų prietaisų jis pradeda veikti automatiškai vos tik įjungus ekrano užraktą.
- Įdiekite arba įjunkite savo įrenginyje programinę įrangą, kuria naudodamiesi galėsite nuotoliniu būdu nustatyti savo įrenginio buvimo vietą, o jį pametus ar pavogus, netgi pašalinti jame esančią informaciją.
- Prieš išvykdami atnaujinkite savo įrenginius, programas ir antivirusinę programinę įrangą, kad ji būtų naujausios versijos. Dažniausiai bandoma įsilaužti į sistemas, kuriose yra pasenusi programinė įranga.
- Padarykite išsamias, visuose įrenginiuose esančių duomenų, atsargines kopijas. Tokiu būdu, jei keliaujant jiems

Kaip likti saugiems keliaujant?

kažkas nutiks, visi jūsų originalūs duomenys bus laikomi saugioje vietoje.

- Prieš išvykdami į užsienį, savo mobiliojo ryšio paslaugų teikėjo pasiteiraukite, koks paslaugų planas šiuo metu užsakytas jūsų telefonui. Gana dažnai tokių paslaugų teikėjai užsienio teritorijoje naudojamiems duomenims nustato aukštus paslaugų įkainius, todėl keliaudami po užsienį galite pageidauti išjungti mobiliojo ryšio duomenis arba nuvykę į užsienį įsigyti tos vietos paslaugų teikėjo išankstinio papildymo SIM kortelę.

Norėdami likti saugūs keliaudami, apsaugokite savo įrenginius prieš išvykdami iš namų, laikykite jų duomenis fiziškai saugioje vietoje ir užšifruokite visą internete atliekamą veiklą.

Pamesti ar pavogti įrenginiai

Keliaudami pasirūpinkite fiziniu savo įrenginių saugumu. Pavyzdžiui, niekada nepalikite savo įrenginių automobilyje, kur žmonės gali juos lengvai matyti, nes nusikaltėliai paprasčiausiai išdauš jūsų automobilio stiklą ir pavogs viską, kas jame yra vertinga. Nors rizika patirti šį nusikaltimą išlieka, tačiau, remiantis naujausiais „Verizon“ tyrimo duomenimis, žymiai labiau tikėtina, jog žmonės savo įrenginį pames, nei kad jį kas nors pavogs. Tai reiškia, kad keliaudami visada turėtumėte keliskart pasitikrinti, ar su savimi vis dar tebeturite pasiimtus įrenginius, pavyzdžiui, eidami per oro uosto saugumo patikros zoną, išlipdami iš taksi automobilio ar išeidami iš restorano, išsiregistruodami iš viešbučio kambario ar išlipdami iš lėktuvo.

Prieiga prie belaidžio tinklo

Prieigos suteikimas prie interneto dažnai keliaujant reiškia, kad turėsite naudotis viešais belaidžio tinklo prieigos taškais, kuriuos galite rasti viešbutyje, vietinėje kavinėje ar oro uoste. Čia atsiranda dvi problemos, susijusios su belaidžiu tinklu: visų pirma, jūs nesate tikri, kas juos nustatė, o, visų antra, jūs nežinote, kas prie jų yra prisijungę. Todėl jie turėtų būti laikomi nepatikimais. Juk dėl šių priežasčių jūs ir atliekate visus šiuos veiksmus, kad apsaugotumėte savo įrenginius prieš išvykdami. Be to, belaidis tinklas naudoja radijo bangas, o tai reiškia, kad bet kas, esantis arti jūsų, gali įsiterpti ir šią informaciją stebėti. Dėl šių priežasčių, jei, visgi, pasirenkate naudoti belaidį tinklą, turite įsitikinti, jog visa jūsų internete atliekama veikla yra šifruojama. Pavyzdžiui, jungdamiesi prie interneto per naršyklę, įsitikinkite, kad jūsų lankomos interneto svetainės yra šifruojamos. Norėdami tai sužinoti, pažiūrėkite, ar interneto svetainės adresas prasideda trumpiniu „HTTPS://“

Kaip likti saugiems keliaujant?

ir/arba internetinio adreso juostoje yra užrakintos spynelės ženkliukas. Be to, galite naudotis VPN (virtualiuoju privačiu tinklu), kurį įjungus, užšifruojama visa jūsų internete atliekama veikla. Šią paslaugą jums gali suteikti darbe arba VPN funkcijas galite užsisakyti savo asmeniniam naudojimui. Jei nerimaujate, kad aplink nėra jokio patikimo belaidžio tinklo, apsvarstykite galimybę kompiuterį prijungti prie išmaniojo telefono, galinčio dalintis internetu (angl. tethering). Dėmesio: kaip minėjome anksčiau, išvykus į užsienį, ši paslauga gali brangiai kainuoti, todėl prieš tai pasikonsultuokite su savo mobiliojo ryšio paslaugų teikėju.

Viešai prieinami įrenginiai

Norėdami prisijungti prie kurios nors iš savo paskyrų ar konfidencialios informacijos, nenaudokite viešai prieinamų kompiuterių, kuriuos galite rasti viešbučių koridoriuose ar interneto kavinėse. Juk net nenumanote, kas prieš tai juo naudojosi, be to, tie asmenys galėjo jį netyčia ar sąmoningai užkrėsti. Kai tik įmanoma, naudokitės tik tais įrenginiais, kuriuos patys prižiūrite ir kuriais pasitikite. Geriausiu atveju, viešai prieinamus kompiuterius galite naudoti viešos informacijos paieškai, pavyzdžiui, orų prognozės ar naujienų skaitymui. Prisijungimas prie bet kurios paskyros (pvz., Google) gali prilygti jūsų veiklą stebinčio asmens kvietimui įsilaužti į jūsų įrenginį.

SUŽINOKITE DAUGIAU

Prenumeruokite kas mėnesinį OUCH! naujienlaiškį, gaukite prieigą prie archyvų, sužinokite daugiau apie SANS saugumo sprendimus apsilankę securingthehuman.sans.org/ouch/archives.

Šaltiniai

Slaptafrazės:	https://securingthehuman.sans.org/ouch/2015#april2015
Atsarginės kopijos:	https://securingthehuman.sans.org/ouch/2015#august2015
Kenkimo programa:	https://securingthehuman.sans.org/ouch/2016#march2016
Užšifravimas:	https://securingthehuman.sans.org/ouch/2016#june2016
„OUCH“ naujienlaiškių archyvas (su jų vertimais):	https://securingthehuman.sans.org/ouch/archives

Licencija

Redaktoriai: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Lietuvišką vertimą finansavo „Perlo“ įmonių grupė.

