Mėnesinis informacinio saugumo naujienlaiškis Tau

Virtualieji privatieji tinklai (VPN)

Apžvalga

Sėdint vietiniame restorane ar kavinėje, o kelionių metu būnant viešbutyje ar oro uoste, gali reikėti pasinaudoti interneto prieiga per viešąjį belaidį tinklą. Bet ar šie viešieji tinklai yra saugūs ir kas stebi arba registruoja jūsų internetinę veiklą? Galbūt jūs net namie nepasitikite savo IPT (interneto paslaugų teikėju) ir norite būti užtikrinti, kad tokių paslaugų teikėjai negalės stebėti, ką veikiate internete. Apsaugokite savo internetinę veiklą ir privatumą, naudodami VPN (virtualųjį privatųjį tinklą). VPN tai technologija, internetinei veiklai sukurianti privatų, šifruotąjį tunelį, pašaliniams asmenims apsunkinantį jūsų internetinės veiklos stebėjimą ar sekimą. Be to, VPN padeda paslėpti jūsų buvimo vietą, todėl jūsų lankomoms svetainėms yra žymiai sudėtingiau nustatyti iš kokios vietos jūs prie jų jungiatės.

Kaip tai veikia?

VPN veikia, sukurdamas privatų, šifruotąjį tunelį, jungiantį jus su pasirinktu VPN paslaugų teikėju. Šiuo tuneliu keliauja visi jūsų internetinės veiklos duomenys, kurie iš jūsų VPN paslaugų teikėjo tinklo yra nukreipiami jūsų pasirinkta kryptimi. Pavyzdžiui, jeigu esate Tampoje, Floridos valstijoje ir jungiatės prie Miunchene, Vokietijoje esančio VPN serverio, bet kokia svetainė, prie kurios jungsitės, laikys kad jungiatės iš Miuncheno, Vokietijos. VPN yra lengva naudoti. Pirmasis žingsnis būtų rasti VPN paslaugų teikėją, kuriuo galėtumėte pasitikėti ir tuomet susikurti paskyrą jo svetainėje (tam įprastai reikia įsigyti jo teikiamą paslaugą). Susikūrę paskyrą, turite parsisiųsti, įsidiegti ir nustatyti jo VPN programinę įrangą. Ją įdiegę ir nustatę, prisijunkite prie interneto kaip tai įprastai darote. VPN programinė įranga nepastebimai sukurs šifruotą tunelį ir pradės saugoti jūsų privatumą to net nesuvokiant.

VPN paslaugų teikėjo pasirinkimas

Jūsų internetinė veikla yra saugi ir privati tiek, kiek saugus ir privatus yra jūsų VPN paslaugų teikėjas. Įsitikinkite, kad pasirinkote tokį paslaugų teikėją, kuriuo galite pasitikėti. Toliau aprašome pagrindinius etapus, renkantis VPN paslaugų teikėją.

Prisijungimas. Ieškokite tokios paslaugos, kuri nekauptų jokių veiklos žurnalų ir pagrindinį dėmesį skirtų jūsų privatumui. Jei jūsų VPN paslaugų teikėjas nekaups jokių veiklos žurnalų, pašaliniams asmenims bus žymiai sudėtingiau prisijungus peržiūrėti, ką veikėte internete.

Įmonės buveinės vieta. Skirtingi VPN paslaugų teikėjai yra įsikūrę skirtingose šalyse. Įsitikinkite, kad jūsų VPN paslaugų teikėjas yra įsikūręs šalyje, kurioje galioja griežti privatumo įstatymai. VPN paslaugų teikėjai, įsikūrę šalyse, kuriose nėra daug privatumo įstatymų arba jie nėra griežti, gali būti priversti atskleisti apie jus renkamą informaciją.

Serveriai. Ieškokite tokios VPN paslaugos, kuri turėtų serverių jums reikiamose šalyse ar miestuose. Kai kurie VPN paslaugų teikėjai turi tūkstančius serverių ir buveinių visame pasaulyje. Jei norite, jog atrodytų, kad jungiatės iš konkrečios šalies, pasidomėkite ar jūsų VPN paslaugų teikėjas teikia tokią paslaugą.

Suderinamumas. Ieškokite tokių paslaugų, kurios veiktų skirtinguose kompiuteriuose ir mobiliuosiuose įrenginiuose. Pavyzdžiui, įprastai naudojate „Windows“ operacinę sistemą turintį nešiojamąjį kompiuterį, planšetinį kompiuterį ir „iPhone“ telefoną. Tokiu atveju, jums reikia tokios VPN paslaugos, kuri veiktų visuose šiuose įrenginiuose.

Venkite nemokamų paslaugų. Būkite itin atsargūs, susidūrę su „nemokamomis” VPN paslaugomis – kaip jie tada uždirba pinigus ir sugeba išlikti versle? Naudojantis nemokamomis paslaugomis, gali būti kaupiama ir parduodama jūsų informacija.

VPN tai puikus būdas apsaugoti savo internetinį privatumą. Tačiau VPN neužtikrins jūsų kompiuterio, kitų įrenginių ar internetinių paskyrų saugumo. Taigi net naudodamiesi VPN, įsitikinkite, kad visuomet atliekate pagrindinius saugumo veiksmus, užtikrindami, kad jūsų įrenginių sistema yra visada atnaujinta, nustatydami ekrano užraktą ir visose savo paskyrose naudodami patikimus ir unikalius slaptažodžius.

Kviestinis redaktorius

Phil Johnsey *(@peakreflections) yra Palm Bičo apygardoje dirbantis IT specialistas, turintis patirties saugumo, ekspertizės ir audito srityse. Jis turi SANS sertifikatą skaitmeninės ekspertizės ir saugumo pagrindų srityse bei yra „OUCH“ bendruomenės peržiūros tarybos narys. Taip pat jam labai patinka žmonėms paprasčiau pateikti su saugumu susijusius dalykus.*

Šaltiniai

Paprastas slaptažodžių kūrimas: https://www.sans.org/u/Sd8
Mobiliųjų prietaisų apsauga: https://www.sans.org/u/Sdd
Sustabdykime kenkėjiškas programas: https://www.sans.org/u/Sdi