Ikmēneša Informācijas drošības izdevums Tev

Virtuālie privātie tīkli (VPN)

Pārskats

Jums varētu rasties nepieciešamība izmantot publisko WiFi interneta pieslēgumu, esot projām no mājām, kad apmeklējat vietējo restorānu vai kafejnīcu, vai arī atrodoties ceļojumā viesnīcā vai lidostā. Bet cik droši ir šādi publiskie tīkli, un kas novēro vai ieraksta to, ko darāt tiešsaistē? Iespējams, jūs neuzticaties pat IPS (interneta pakalpojumu sniedzējam) savās mājās, un vēlaties būt droši, ka tas nevar novērot, ko darāt tiešsaistē. Aizsargājiet savas tiešsaistes aktivitātes un privātumu ar VPN (Virtual Private Network) jeb virtuālo privāto tīklu. VPN ir tehnoloģija, kas izveido privātu šifrētu tuneli jūsu tiešsaistes aktivitātēm, padarot jūsu tiešsaistes darbību novērošanu daudz sarežģītāku. Papildus tam, VPN palīdz noslēpt jūsu atrašanās vietu, apgrūtinot tīmekļa vietņu, kuras apmeklējat, iespēju noteikt jūsu atrašanos.

Kā tas strādā?

VPN darbojas, izveidojot privātu šifrētu tuneli uz VPN nodrošinātāju, kuru jūs izvēlaties. Visas jūsu tiešsaistes aktivitātes tiek virzītas caur šo tuneli, un tad, atstājot jūsu VPN nodrošinātāja tīklu, nonāk jūsu izvēlētajā galamērķī. Piemēram, ja atrodaties Jelgavā, un pieslēdzaties caur VPN no Minhenes Vācijā, visas tīmekļa vietnes, kuras apmeklēsiet, domās, ka pieslēdzaties no Minhenes, Vācijas. VPN ir vienkārši lietojams. Pirmais solis ir atrast VPN nodrošinātāju, kuram uzticaties, un tad izveidot pie viņiem kontu (tas parasti ietver pakalpojuma iegādi). Kad jums ir konts, jūs lejuplādējat, uzstādāt un konfigurējat viņu VPN programmatūru. Pēc uzstādīšanas un konfigurēšanas jūs pieslēdzaties internetam kā parasti. VPN programmatūra nemanāmi izveidos jūsu šifrēto tuneli un sāks sargāt jūsu privātumu, jums to nemaz nemanot.

VPN nodrošinātāja izvēle

Jūsu tiešsaistes aktivitātes ir tikai tik privātas un drošas, cik ir jūsu VPN nodrošinātājs. Pārliecinieties, ka izvēlaties kādu, kam varat uzticēties. Šeit būs daži punkti, kuri jāņem vērā, izvēloties VPN pakalpojuma sniedzēju:

Žurnalēšana (logging): Izvēlieties servisu, kurš neveic nekādus pierakstus un fokusējas uz privātumu. Ja jūsu VPN nodrošinātājs neuzkrāj nekādus žurnalēšanas pierakstus (logs), ir daudz grūtāk kādam iet un pētīt, ko jūs esat darījuši tiešsaistē.

Kompānijas atrašanās vieta: Dažādi VPN nodrošinātāji atrodas dažādās valstīs. Pārliecinieties, ka jūsu izvēlētais VPN nodrošinātājs atrodas valstī ar spēcīgu privātuma aizsardzību. VPN nodrošinātāji, kas atrodas valstīs ar vāju vai neesošu privātuma likumdošanu var tikt piespiesti atklāt informāciju, ko ir ievākuši par jums.

Serveri: Meklējiet VPN nodrošinātāju, kura serveri ir izvietoti jums nepieciešamajās valstīs vai pilsētās. Dažiem VPN nodrošinātājiem ir tūkstošiem serveru, kas izvietoti dažādās pasaules vietās. Vai jums ir nepieciešams, lai izskatās, ka jūsu pieslēgums nāk no konkrētas valsts, vai izvēlētais VPN nodrošinātājs to spēj nodrošināt?

Savietojamība: Pārliecinieties, ka serviss darbojas uz dažādiem datoriem un mobilajām iekārtām. Piemēram, ja izmantojat Windows portatīvo datoru, planšetdatoru un iPhone, jūs vēlēsieties, lai VPN pakalpojums darbojas uz visām šīm iekārtām.

Izvairieties no bezmaksas: Esiet ļoti piesardzīgi "bezmaksas" VPN pakalpojuma gadījumā, kā viņi gūst peļņu un turpina biznesu? Bezmaksas servisi var vākt un pārdot jūsu informāciju.

VPN ir lielisks veids kā pasargāt jūsu tiešsaistes privātumu. Taču VPN nepadara jūsu datoru, iekārtas vai tiešsaistes kontus drošākus. Tādēļ, pat ja izmantojat VPN, pārliecinieties, ka vienmēr ievērojat drošības pamatprasības, ieskaitot pārliecināšanos, ka iekārtas ir atjauninātas, ekrānu bloķētāju lietošanu un drošas, unikālas paroles visiem jūsu kontiem.

CERT.LV ir Latvijas Republikas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā. Uzziniet vairāk https://www.cert.lv vai sekojiet mums Twiterī @certlv.

Viesredaktors

Phil Johnsey *(@peakreflections) ir IT profesionālis Palmbičas apgabalā, kuram ir pieredze drošības jautājumos, kriminālistikā un auditēšanā. Viņš ir izgājis SANS sertifikāciju digitālajā kriminālistikā un security essentials un ir OUCH recenzentu padomes biedrs. Viņa aizraušanās ir censties padarīt drošību vienkāršu priekš citiem.*

Resursi

Kā padarīt paroles vieglāk iegaumējamas:	https://www.sans.org/u/Sd8
Mobilo ierīču drošība:	https://www.sans.org/u/Sdd
Stop Malware:	https://www.sans.org/u/Sdi

Redakcija: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Tulkojums: CERT.LV