

OUCH!

Publicația dumneavoastră lunară de sensibilizare asupra securității informatice

Rețele Virtuale Private (VPN)

Prezentare generală

Este posibil ca la un moment dat, când sunteți departe de casă, să fiți nevoiți să utilizați o rețea publică de Wi-Fi pentru a accesa Internetul, de exemplu când vă aflați la un restaurant, o cafenea sau când călătoriți, la hotel sau aeroport. Dar cât de sigure sunt aceste rețele publice și cine urmărește sau înregistrează ceea ce faceți online? Sau poate că nu aveți încredere nici în furnizorul dvs. de Internet de acasă și doriți să fiți siguri că nu va monitoriza activitatea online. Vă puteți proteja activitățile și confidențialitatea online cu ceea ce se numește VPN (Virtual Private Network – rețea virtuală privată). Un VPN este o tehnologie care creează un tunel privat, criptat pentru activitatea dvs. online, ceea ce face mult mai dificil pentru oricine să vadă sau să monitorizeze ceea ce faceți online. În plus, un VPN vă ajută să vă ascundeți locația, ceea ce face mult mai greu pentru site-urile vizitate să își dea seama unde vă aflați.

Cum funcționează?

Un VPN funcționează prin crearea unui tunel privat, criptat către furnizorul VPN pe care îl alegeți. Toată activitatea dvs. online trece prin acest tunel, apoi părăsește rețeaua furnizorului VPN spre destinația dorită. De exemplu, dacă vă aflați în Tampa, Florida și vă conectați la un server VPN din München, Germania, orice site pe care vă conectați va crede că vă conectați din München, Germania. Un VPN este simplu de utilizat. Primul pas este găsirea unui furnizor VPN care să vă inspire încredere și apoi crearea unui cont la acest furnizor (de obicei, acest lucru necesită achiziționarea serviciului). Odată ce aveți un cont, descărcați, instalați și configurați software-ul VPN. Odată făcuți acești pași, vă puteți conecta la Internet cum faceți de obicei. Software-ul VPN va rula pe fundal, creându-vă un tunel criptat protejându-vă intimitatea fără să vă dați seama.

Alegerea unui furnizor de VPN

Siguranța și confidențialitatea activităților dvs. online depinde de furnizorul VPN. Asigurați-vă că selectați unul în care puteți avea încredere. Iată câteva puncte cheie de luat în considerare atunci când selectați un furnizor de servicii VPN.



Înregistrări: Căutați un serviciu care nu înregistrează conexiunile și se concentrează pe confidențialitate. Dacă furnizorul dvs. de servicii VPN nu tine astfel de evidențe, este mult mai greu pentru oricine să vadă ce ați făcut online.



Locația companiei: Furnizori diferiți se află în țări diferite. Asigurați-vă că selectați un furnizor VPN aflat într-o țară cu legi clare și puternice privind confidențialitatea. Furnizorii de VPN situați în țări fără legi sau cu legi slabe privind confidențialitatea, pot fi forțați să comunice informațiile pe care le colectează despre dvs.



Servere: Căutați un serviciu VPN care are serverele situate în țările sau orașele de care aveți nevoie. Unii furnizori de VPN au mii de servere și locații pe tot globul. Aveți nevoie ca conexiunile dvs. să pară ca provin dintr-o anumită țară, poate furnizorul de VPN să ofere acest lucru?



Compatibilitate: Căutați servicii care funcționează pe diferite computere și dispozitive mobile. De exemplu, poate aveți un laptop Windows, o tabletă și un iPhone. Atunci, aveți nevoie de un serviciu VPN care să funcționeze pe toate aceste dispozitive.



Evitați serviciile gratis: Fiți foarte precauți față serviciile VPN gratuite, cum fac furnizorii bani și nu dau faliment? Serviciile gratuite pot colecta și vinde informațiile dvs.

VPN-ul este o modalitate fantastică de a vă proteja confidențialitatea online. Cu toate acestea, VPN-ul nu vă protejează computerul, dispozitivele sau conturile online. Deci, chiar dacă utilizați o rețea VPN, asigurați-vă întotdeauna că urmați regulile de securitate de bază, că dispozitivele dvs. sunt actualizate, că utilizați un sistem de blocare a acestor dispozitive și că întotdeauna folosiți parole puternice și unice pentru toate conturile dvs.

Versiunea în limba română

Ubisoft este o companie de jocuri. Un creator de lumi, dedicat îmbogățirii vieților jucătorilor cu experiențe de joc originale și memorabile. Alflați mai multe la: <https://www.ubisoft.com/en-us/>.

Editor invitat

Phil Johnsey (@peakreflections) lucrează în IT la Palm Beach County și are experiență în domeniul securității, criminalisticii și auditului. Este certificat SANS în domeniul criminalisticii digitale, elementelor esențiale de securitate și este membru al consiliului de evaluare a publicației OUCH. Pasiunea lui este să facă securitatea cibernetică pe înțelesul tuturor.



Resurse

Simplificarea parolelor: <https://www.sans.org/u/Sd8>
Securizarea dispozitivului mobil personal: <https://www.sans.org/u/Sdd>
Opriti programele Malware: <https://www.sans.org/u/Sdi>

Ouch! este publicat de SANS Security Awareness și este distribuit sub licența [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Sunteți liber să distribuiți acest buletin informativ sau să-l utilizați în programul dumneavoastră de instruire atâta vreme cât nu îl modificați. Pentru traducere sau informații suplimentare, vă rugăm să contactați www.sans.org/security-awareness/ouch-newsletter. Echipa editorială: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Tradus de: Sorana Costache