

OUCH!

Месечният бюлетин за Информационна Сигурност за вас

Виртуални частни мрежи (VPN)

Преглед

Може да се наложи да използвате обществена Wi-Fi връзка за достъп до Интернет, когато сте далеч от дома си, например когато сте в местния ресторант или кафене или когато пътувате, в хотел или на летище. Но колко сигурни са тези обществени мрежи и кой гледа или записва това, което правите онлайн? Може би дори не се доверявате дори на вашия ISP (доставчик на интернет услуги) у дома и искате да сте сигурни, че не могат да следят какво правите онлайн. Защитете своите онлайн дейности и поверителност с нещо, наречено VPN (виртуална частна мрежа). VPN е технология, която създава личен криптиран тунел за вашата онлайн дейност, който прави много по-трудно за който и да било да гледа или наблюдава това, което правите онлайн. В допълнение, VPN помага да скриете местоположението си, което прави много по-трудно за посещаваните от вас уебсайтове да определят къде се намирате.

Как работи?

VPN работи чрез създаване на личен криптиран тунел към избрания от вас VPN доставчик. Цялата ви онлайн дейност минава през този тунел, след което напуска мрежата на вашия доставчик на VPN до желаната дестинация. Например, ако се намирате в Тампа, Флорида и се свързвате с VPN сървър в Мюнхен, Германия, всеки уебсайт, към който се свързвате, ще мисли, че се свързвате от Мюнхен, Германия. VPN е лесна за използване. Първата стъпка е намирането на доверен доставчик на VPN и създаване на акаунт при тях (това обикновено изисква да закупите услугата им). След като имате акаунт, изтеглете, инсталирайте и конфигурирайте VPN софтуер. Веднъж инсталирали и конфигурирали това, се свързвате с интернет, както винаги. Софтуерът сам ще създаде вашия криптиран тунел и ще започнете да защитавате личните си данни, без дори да го забелязвате.

Избор на доставчик на VPN

Вашите онлайн дейности са толкова сигурни и лични, колкото и вашият доставчик на VPN. Не забравяйте да изберете такъв, на който можете да се доверите. Ето ключовите моменти при избора на доставчик на VPN услуги.



Създаване на регистри: Потърсете услуга, която не съхранява регистри и се фокусира върху неприкосновеността на личния живот. Ако вашият доставчик на VPN услуги не води никакви регистри, е много по-трудно за някой да се върне и да види това, което сте правили онлайн.



Къде се намира компанията: Различните доставчици на VPN са базирани в различни страни. Уверете се, че сте избрали доставчик на VPN, който е базиран в страна, която има силни закони за поверителност. Доставчиците на VPN, разположени в страни, които имат много малко или слаби закони за поверителност, могат да бъдат принудени да предадат информацията, която събират за вас.



Сървъри: Потърсете VPN услуга, чиито сървъри се намират в нужните ви страни или градове. Някои доставчици на VPN имат хиляди сървъри и местоположения по целия свят. Имате ли необходимост връзките ви да изглеждат така, сякаш идват от конкретна страна и може ли вашият доставчик на VPN да осигури това?



Съвместимост: Потърсете услуги, които работят на различни компютри и мобилни устройства. Например, може да използвате лаптоп с Windows, таблет и iPhone. Съответно ще искате VPN услуга, която ще работи на всички тези устройства.



Избягвайте безплатното: Бъдете много предпазливи по отношение на безплатните VPN услуги - как тези фирми печелят пари и остават в бизнеса? Безплатните услуги може да събират и продават вашата информация.

Радослава Несторова (лингвист) и Николай Дачев (технически експерт) са екип, доказал се в областта на техническите преводи. Повече за нас можете да научите на нашите страници в LinkedIn:

<https://www.linkedin.com/pub/radoslava-nestorova/6/6a2/962>

<https://www.linkedin.com/pub/nikolay-dachev/7b/5bb/96b>

Гост-редактор

Фил Джонси (@peakreflections) е ИТ специалист в окръг Палм Бийч с опит в областта на сигурността, разследванията и одитирането. Той е SANS сертифициран в областта на дигиталните разследвания, основните изисквания за сигурност и член на OUCH общността. Неговата страст прави сигурността лесна за другите.



Ресурси

Лесен наръчник за пароли: <https://www.sans.org/u/Sd8>

Сигурност на мобилни устройства: <https://www.sans.org/u/Sdd>

Борба с вируси: <https://www.sans.org/u/Sdi>

OUCH! се публикува от SANS Security Awareness и се разпространява под лиценза на [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Имате право да разпространявате този бюлетин или да го използвате във вашата информационна кампания, при условие че не го модифицирате. За преводи или повече информация моля пишете на www.sans.org/security-awareness/ouch-newsletter. Редакторски колектив: Уолт Scrivens, Фил Хофман, Алън Уагонър, Черил Конли | Превод: Николай Дачев и Радослава Несторова