

Co je ve skutečnosti VPN

Mění to, kdo tě může vidět, ne jestli tě někdo vidět může.

Jednoduše řečeno: VPN zabrání tvému poskytovateli internetu nebo letištní Wi-Fi vidět, kam se připojuješ. Tyto informace nezmizí: předají se firmě provozující VPN, která je teď vidí. To, co už putovalo šifrovaně, jako e-mail nebo bankovníctví, putovalo šifrovaně i dříve. Slouží k několika konkrétním účelům a často se prodává tak, jako by řešila mnohem víc.

Celé roky jsem o VPN slýchal a ignoroval to, stejně jako s antiviry: nepoužívám antivirus, nebo téměř nikdy. Mám kopie všeho na třech místech v reálném čase a dávám velký pozor na to, co stahuji, na jaké odkazy klikám a jaké weby navštěvuji. Není to stoprocentní bezpečnost, ale mně to funguje. Jednoho dne jsem viděl nabídku VPN za o něco málo přes dvě eura měsíčně a ze zvědavosti jsem si ji pořídil. Funguje dobře, ale posloužila mi málo: například k vyzkoušení služby, která se tehdy otevírala pouze ve Spojených státech. Cítím se bezpečněji? Ne. Pokud mi ji znovu nabídnou za tuto cenu, možná ji obnovím; pokud ne, tak ne. Je to jen má zkušenost, nic to nedokazuje. Zeptal jsem se tedy sám sebe, co přesně VPN dělá. Takhle jsem to pochopil já.

Představ si, že házíš dopis do schránky s dobře viditelnou adresou příjemce. Pošťák vidí, komu ho posíláš, i když ho nemůže přečíst, pokud je zalepený. Tím pošťákem je tvůj internetový operátor. VPN vloží tvůj dopis do další obálky, adresované zprostředkovateli, který ji otevře a přepošle. Tvůj obvyklý pošťák už skutečnou adresu nevidí. Vidí pouze to, že píšeš tomuto zprostředkovateli.

Ten, kdo ovládá síť, ze které se připojuješ – například letištní Wi-Fi –, přestává vidět, kam chodíš. Ale zprostředkovatel nyní vidí to, co dříve viděl tvůj operátor, a někdy i víc, protože veškerý tvůj provoz prochází přes něj. Sledování nemizí: mění majitele. Odtud ten název.

Kromě toho téměř vše, co dnes děláš – jako otevření e-mailu nebo vstup do banky –, už putuje šifrovaně až k cílovému serveru díky zámečku v prohlížeči. To se děje s VPN i bez ní. VPN přidává ochranu pouze na prvním úseku, až k vlastnímu serveru. Odtud je cesta stejná jako obvykle.

Proto jsou věci, které ti nemůže slíbit, i když se někdy takto prodává. Pokud ses přihlásil ke svému e-mailu nebo do banky, tato služba ví, že jsi to ty, s VPN nebo bez ní. Nezaručuje ani to, že nikdo nesleduje tvůj provoz: mění pouze to, kdo se dívá. To, že společnost tvrdí, že «neuchovává záznamy», je slib – stejně jako když velká platforma říká «vaše zprávy jsou šifrované, nečteme je». Audit to může v danou chvíli potvrdit, ale stále zůstává něčím, čemu věříš, že bude splněno, nikoli něčím, co by nebylo možné porušit ze samotného návrhu.

A obsah konverzace zůstává stejný. Pokud tvá aplikace pro zasílání zpráv již šifruje od začátku do konce, VPN nepřidává nic. Pokud to nedělá, VPN to také nespraví: chrání cestu zprávy, nikoli to, co s ní aplikace nebo její server udělají po doručení.

Nic z toho ji nečiní zbytečnou. Skrýt to, kam se připojuješ, před veřejnou Wi-Fi, před operátorem, který by chtěl tuto historii prodat, nebo před státem, který blokuje nějakou službu, je skutečná práce a odvádí ji dobře. Marketing však obvykle slibuje víc, než tato vrstva může nabídnout.

Otázka, kterou stojí za to si položit u VPN nebo jakékoli služby slibující tě ochránit, zní «je to šifrované?». Pravděpodobně ano, alespoň na jednom úseku. Zní jinak: do koho vkládám důvěru, kterou jsem odebral někomu

jinému? A co mi zbude, pokud se ukáže jako neopodstatněná?

VPN, když odvádí svou práci dobře, mění pouze to, kdo je zprostředkovatelem tvého připojení. Aplikace jako Solo2, jejíž zprávy neprocházejí žádným serverem, zprostředkovatele z konverzace zcela odstraňuje. Nekonkurují si: řeší různé problémy.

Jeich zaměňování je velmi běžný způsob, jak se domnívat, že je člověk chráněn více, než ve skutečnosti je.

Poznámka redakce: Pokud tyto Cuadernos zmiňují firmy nebo produkty, není to za účelem obviňování. Ti, kteří je vytvářejí, odvádějí práci, kterou miliony lidí používají a oceňují. To, na co poukazujeme, je strukturální — model, nikoliv značka. Značky uvádíme jako příklad, protože jsou pro čtenáře rozpoznatelné.

Zdroje a další čtení

- Protokol HTTPS a transportní šifrování jsou otevřené standardy, veřejně zdokumentované organizací IETF.
- V této stejné sbírce: «Když není nikdo uprostřed» a «Nejste anonymní» rozvíjejí z jiných úhlů pohledu stejný rozdíl mezi strukturou a slibem.

[← Předchozí](#)[Nejste anonymní](#)

Nedávné čtení

- [Zamyšlení · 29. června 2026 Nejste anonymní](#)
- [Zamyšlení · 27. května 2026 Co podpis nemůže napravit](#)
- [Analýza · 26. května 2026 Skutečné vs. zdánlivé soukromí: otázky, které je vhodné si položit](#)

Vezmi si tento článek tam, kam potřebuješ.

[↓ Markdown](#) [↓ Prostý text](#) [↓ PDF](#)

Soubor se stáhne do tvého zařízení. Odtud si jej můžeš uložit, importovat do Solo2 nebo sdílet, kdekoli chceš. Cuadernos za tebe o cíli nerozhoduje.

Pečeť · SHA-256 ba55a8aec867c617ed1466efea8e24ad08574046bb61280a5d4ff5e842166f98

[Funkce](#) [Ceny](#) [Nainstalovat](#) [Novinky](#) [Blog](#) [Pro](#) [Nápověda](#) [O nás](#) [Kontakt](#)
[Transparentnost](#) [Ověření](#) [Soukromí](#) [Podmínky](#) [Cookies](#)

Cuadernos Lacre · Publikace [Menzuri Gestión S.L.](#) ·
napsal R.Eugenio · rediguje tým [Solo2](#).

Tento web nepoužívá cookies. Vše, co tvůj prohlížeč načítá, je napsané nebo námi dohlížené a umístěné na našich evropských serverech: anonymní počítadlo návštěv (Umami, vlastní hosting) a minimální nezbytný JavaScript pro výběr jazyka a tvoji předvolbu světlého nebo tmavého motivu, která se ukládá ve tvém vlastním zařízení. Žádné zdroje od externích společností, žádné trackery, žádné profilování, žádné sdílení dat. Pokud nás chceš sledovat: [RSS](#).