

Kaj je v resnici VPN

Spremeni, kdo te lahko vidi, ne pa, ali te kdo lahko.

Preprosto povedano: VPN poskrbi, da tvoj ponudnik interneta ali letališki Wi-Fi ne vidita več, kam se povezuješ. Te informacije ne izginejo: prenesejo se na podjetje za VPN, ki jih zdaj vidi. Kar je že prej potovalo šifrirano, kot e-pošta ali banka, je bilo šifrirano tudi prej. Služi nekaj konkretnim namenom, pogosto pa se prodaja tako, kot da bi reševal veliko več.

Leta sem poslušal o VPN-jih in se zanje nisem zmenil, ravno tako kot za protivirusne programe: ne uporabljam protivirusnega programa, ali skoraj nikoli. Imam sprotne kopije vsega na treh mestih in zelo pazim, kaj prenašam, na katere povezave klikam in katere spletne strani obiskujem. To ni stoodstotna varnost, a zame deluje. Nekega dne sem videl ponudbo za VPN za nekaj več kot dva evra na mesec in jo sklenil iz radovednosti. Deluje dobro, vendar mi je malo koristil: na primer za preizkus storitve, ki se je takrat odpirala le v Združenih državah. Se počutim bolj varno? Ne. Če mi jo znova ponudijo po tej ceni, jo morda podaljšam; če ne, ne. To je le moja izkušnja, ničesar ne dokazuje. Zato sem se vprašal, kaj točno počne VPN. Tako sem to razumel sam.

Predstavlja si, da vržeš pismo v nabiralnik z jasno vidnim naslovom prejemnika. Pismonoša vidi, komu ga pošiljaš, čeprav ga ne more prebrati, če je zaprto. Ta pismonoša je tvoj internetni operater. VPN vstavi tvoje pismo v drugo ovojnico, naslovljeno na posrednika, ki jo odpre in posreduje naprej. Tvoj običajni pismonoša ne vidi več pravega naslova. Vidi le to, da pišeš temu posredniku.

Tisti, ki nadzoruje omrežje, iz katerega se povezuješ – na primer letališki Wi-Fi –, ne vidi več, kam greš. Toda posrednik zdaj vidi tisto, kar je prej videl tvoj operater, včasih pa še več, saj ves tvoj promet poteka prek njega. Nadzor ne izgine: zamenja roke. Od tod ime.

Poleg tega skoraj vse, kar počneš danes – kot je odpiranje pošte ali vstop v banko –, že potuje šifrirano do ciljnega strežnika po zaslugi ključavnice v brskalniku. To se dogaja z VPN-jem in brez njega. VPN doda zaščito le na prvem odseku, do svojega strežnika. Od tam naprej je pot enaka kot običajno.

Zato so stvari, ki ti jih ne more obljubiti, čeprav se včasih tako prodaja. Če si se prijavil v svojo pošto ali banko, ta storitev ve, da si to ti, z VPN-jem ali brez njega. Prav tako ne zagotavlja, da nihče ne gleda tvojega prometa: spremeni le, kdo gleda. To, da podjetje trdi, da «ne hrani dnevnikov», je obljuba – natanko tako, kot ko velika platforma pravi «vaša sporočila so šifrirana, ne beremo jih». Revizija lahko to potrdi v določenem trenutku, vendar ostaja nekaj, v kar zaupaš, da bo izpolnjeno, ne nekaj, česar po sami zasnovi ne bi bilo mogoče prekršiti.

In vsebina pogovora ostane enaka. Če tvoja aplikacija za sporočanje že šifrira od konca do konca, VPN ne doda ničesar. Če tega ne počne, VPN tega tudi ne reši: zaščiti pot sporočila, ne pa tega, kar aplikacija ali njen strežnik z njim storita ob prihodu.

Nič od tega ga ne dela neuporabnega. Skriti to, kam se povezuješ, pred javnim Wi-Fi-jem, pred operaterjem, ki bi želel to zgodovino prodati, ali pred državo, ki blokira določeno storitev, je pravo delo in to opravlja dobro. Trženje pa običajno obljublja več, kot lahko ta plast da.

Vprašanje, ki si ga velja zastaviti ob VPN-ju ali katerikoli storitvi, ki obljublja, da te bo zaščitila, se ne glasi «ali je šifrirano?». Verjetno da, vsaj na enem delu. Glasi se drugače: v koga polagam zaupanje, ki sem ga odvezel

drugemu? In kaj mi ostane, če se izkaže za neutemeljeno?

VPN, ko dobro opravlja svoje delo, le spremeni posrednika tvoje povezave. Aplikacija, kot je Solo2, katere sporočila ne gredo skozi noben strežnik, posrednika povsem umakne iz pogovora. Ne tekmujeta: rešujeta različne težave.

Zamenjevati ju je zelo pogost način, da se človek počuti bolj zaščenega, kot je v resnici.

Opomba uredništva: ko ti Cuadernos navajajo podjetja ali izdelke, to ni namenjeno obtoževanju. Tisti, ki jih gradijo, opravljajo delo, ki ga milijoni ljudi uporabljajo in cenijo. To, na kar opozarjamo, je strukturno — model, ne blagovna znamka. Blagovne znamke se pojavljajo kot primer, ker jih bralec prepozna.

Viri in nadaljnje branje

- Protokol HTTPS in transportno šifriranje sta odprta standarda, ki ju javno dokumentira IETF.
- V tej isti zbirki: «Ko vmes ni nikogar» in «Nisi anonimen» z drugih zornih kotov razvijata isto razlikovanje med strukturo in obljubo.

[← Prejšnji Nisi anonimen](#)

Zadnja branja

- [Razmislek · 29. junij 2026 Nisi anonimen](#)
- [Razmislek · 27. maj 2026 Česa podpis ne more popraviti](#)
- [Analiza · 26. maj 2026 Dejanska vs. navidezna zasebnost: vprašanja, ki si jih je smiselno zastaviti](#)

Vzemi ta članek s seboj, kamor koli ga potrebuješ.

[↓ Markdown](#) [↓ Navadno besedilo](#) [↓ PDF](#)

Datoteka bo prenesena v tvojo napravo. Od tam jo lahko shraniš, uvoziš v Solo2 ali deliš z drugimi, kakor želiš. Brez sledenja, brez registracije, brez povezave, ki te spremlja.

Voščeni pečat · SHA-256 b3bfef6b3e89314f1f120d4f00706c2fcb14889a26b7e4a4290b6f70d939cd88

[Funkcije](#) [Cene](#) [Namesti](#) [Novosti](#) [Blog](#) [Pro](#) [Pomoč](#) [O nas](#) [Kontakt](#)
[Preglednost](#) [Verifikacija](#) [Zasebnost](#) [Pogoji](#) [Piškotki](#)

Cuadernos Lacre · Publikacija podjetja [Menzuri Gestión S.L.](#) ·
napisal R.Eugenio · uredila ekipa [Solo2](#).

To spletno mesto ne uporablja piškotkov. Vse, kar naloži tvoj brskalnik, smo napisali ali nadzorujemo mi in je gostovano na naših evropskih strežnikih: anonimen števec obiskov (Umami, samostojno gostovan) in minimalni JavaScript, potreben za izbirnik jezika in tvojo izbiro svetle/temne teme, ki se shrani v tvoji lastni napravi. Brez virov tretjih oseb, brez sledilnikov, brez profiliranja, brez deljenja podatkov. Če nas želiš spremljati: [RSS](#).