

Kas patiesībā ir VPN

Tas maina to, kurš tevi var redzēt, nevis to, vai kāds var.

Vienkāršiem vārdiem: VPN liedz tavam interneta pakalpojumu sniedzējam vai lidostas Wi-Fi redzēt, kur tu pieslēdzies. Šī informācija nepazūd: tā tiek nodota VPN uzņēmumam, kurš to tagad redz. Tas, kas jau ceļoja šifrēts, piemēram, e-pasts vai banka, bija šifrēts arī iepriekš. Tas kalpo dažiem konkrētiem mērķiem, un to bieži pārdod tā, it kā tas atrisinātu daudz ko vairāk.

Gadiem ilgi es dzirdēju par VPN un nepievērsu tam uzmanību, tāpat kā antivīrusu programmām: es nelietoju antivīrusu, vai gandrīz nekad. Man ir reāllaika kopijas visam trīs vietās, un es ļoti uzmanos ar to, ko lejupielādēju, uz kādām saitēm spiežu un kādas vietnes apmeklēju. Tā nav simtprocentīga drošība, bet man tas der. Kādu dienu es ieraudzīju VPN piedāvājumu par nedaudz vairāk kā diviem eiro mēnesī un aiz ziņkārības to iegādājos. Tas darbojas labi, bet man tas ir noderējis maz: piemēram, lai izmēģinātu pakalpojumu, kas toreiz darbojās tikai Amerikas Savienotajās Valstīs. Vai es jūtos drošāk? Nē. Ja man to atkal piedāvās par šo cenu, varbūt atjaunošu; ja ne, tad nē. Tā ir tikai mana pieredze, tā neko nepierāda. Tāpēc es sev pajautāju, ko tieši dara VPN. Lūk, kā es to sapratu.

Iedomājies, ka iemet vēstuli pastkastītē ar skaidri redzamu saņēmēja adresi. Pastnieks redz, kam tu to sūti, pat ja nevar to izlasīt, ja tā ir aizzīmogota. Šis pastnieks ir tavs interneta pakalpojumu sniedzējs. VPN ievieto tavu vēstuli citā aploksnē, kas adresēta starpniekam, kurš to atver un pārsūta tālāk. Tavs ierastais pastnieks vairs neredz īsto adresi. Viņš redz tikai to, ka tu raksti šim starpniekam.

Tas, kurš kontrolē tīklu, no kura tu pieslēdzies, piemēram, lidostas Wi-Fi, vairs neredz, kurp tu dodies. Bet starpnieks tagad redz to, ko iepriekš redzēja tavs operators, un dažreiz vairāk, jo visa tava datplūsma iet caur viņu. Uzraudzība nepazūd: tā maina īpašnieku. No tā arī cēlies nosaukums.

Turklāt gandrīz viss, ko tu dari šodien, piemēram, atver e-pastu vai ieej bankā, jau ceļo šifrēts līdz galamērķa serverim, pateicoties pārlūkprogrammas piekaramajai slēdzenei. Tas notiek gan ar VPN, gan bez tā. VPN pievieno aizsardzību tikai pirmajā posmā, līdz pat savam serverim. No turienes ceļš ir tāds pats kā parasti.

Tāpēc ir lietas, ko tas tev nevar apsolīt, lai gan dažreiz to tā pārdod. Ja esi ielogojies savā e-pastā vai bankā, šis pakalpojums zina, ka tas esi tu, ar VPN vai bez tā. Tas arī negarantē, ka neviens neskatās tavu datplūsmu: tas tikai maina to, kurš skatās. Ja uzņēmums apgalvo, ka tas «neuzglabā žurnālus», tas ir solījums, gluži tāpat kā tad, kad liela platforma saka «tavas ziņas ir šifrētas, mēs tās nelasām». Audits to var apstiprināt noteiktā brīdī, taču tā joprojām ir lieta, kuras izpildei tu uzticies, nevis kaut kas tāds, ko pēc uzbūves nebūtu iespējams pārkāpt.

Un sarunas saturs paliek tāds pats. Ja tava ziņapmaiņas lietotne jau šifrē no gala līdz galam, VPN neko nepievieno. Ja tā to nedara, VPN to arī neizlabo: tas aizsargā ziņas ceļu, nevis to, ko lietotne vai tās serveris ar to dara pēc ierašanās.

Nekas no tā nepadara to bezjēdzīgu. Paslēpt savu pieslēgšanās vietu no publiskā Wi-Fi, no operatora, kurš vēlētos pārdot šo vēsturi, vai no valsts, kas bloķē kādu pakalpojumu, ir reāls darbs, un tas tiek paveikts labi. Tomēr mārketinga parasti sola vairāk, nekā šis slānis spēj dot.

Jautājums, ko vērts sev uzdot saistībā ar VPN vai jebkuru pakalpojumu, kas sola tevi aizsargāt, nav «vai tas ir šifrēts?». Droši vien jā, vismaz vienā posmā. Tas ir šis cits: kam es uzticu to uzticību, ko esmu atņēmis citam? Un kas man paliek pāri, ja tā izrādās nepamatota?

VPN, kad tas labi veic savu darbu, tikai maina to, kurš ir tavas savienojuma starpnieks. Tāda lietotne kā Solo2, kuras ziņojumi neiet caur nevienu serveri, pilnībā izslēdz starpnieku no sarunas. Tās nekonkurē: tās risina dažādas problēmas.

To jaukšana ir ļoti izplatīts veids, kā noticēt, ka esi pasargātāks, nekā patiesībā esi.

Redaktora piezīme: kad šajos Cuadernos tiek minēti uzņēmumi vai produkti, tas nav domāts kā apsūdzība. Tie, kas tos veido, dara darbu, ko miljoniem cilvēku izmanto un novērtē. Tas, uz ko mēs norādām, ir strukturāls — modelis, nevis zīmols. Zīmoli parādās kā piemēri, jo tos lasītājs atpazīst.

Avoti un papildu literatūra

- HTTPS protokols un transporta šifrēšana ir atvērti standarti, ko publiski dokumentējusi IETF.
- Šajā pašā krājumā: «Kad vidū neviena nav» un «Tu neesi anonīms» no citiem skatupunktiem attīsta to pašu atšķirību starp struktūru un solījumu.

[← Iepriekšējais Tu neesi anonīms](#)

Jaunākie lasījumi

- [Pārdomas · 2026. gada 29. jūnijs Tu neesi anonīms](#)
- [Pārdomas · 2026. gada 27. maijs Tas, ko paraksts nevar atrisināt](#)
- [Analīze · 2026. gada 26. maijs Patiesa vs šķietama konfidencialitāte: jautājumi, ko vērts sev uzdot](#)

Paņem šo rakstu līdzī tur, kur tev nepieciešams.

[↓ Markdown](#) [↓ Parasts teksts](#) [↓ PDF](#)

Fails tiks lejupielādēts tavā ierīcē. No turienes vari to saglabāt, importēt Solo2 vai kopīgot jebkur. Cuadernos nepieņem lēmumu par galamērķi tavā vietā.

Vaska zīmogs · SHA-256 99869d62dd25681620e22454be3e5d3629d498e1d96cbc107c499e6f5bf52d3a

[Funkcijas](#) [Cenas](#) [Instalēt](#) [Jaunami](#) [Blogs](#) [Pro](#) [Palīdzība](#) [Par mums](#) [Kontakti](#)
[Pārredzamība](#) [Verifikācija](#) [Privātums](#) [Noteikumi](#) [Sīkdatnes](#)

Cuadernos Lacre · [Menzuri Gestión S.L.](#) publikācija ·
autors R.Eugenio · rediģējusi [Solo2](#) komanda.

Šī vietne neizmanto sīkfailus. Viss, ko ielādē tavs pārlūks, ir mūsu rakstīts vai pārraudzīts un izvietots uz mūsu Eiropas serveriem: anonīms apmeklējumu skaitītājs (Umami, pašizmitināts) un minimālais JavaScript, kas nepieciešams valodas selektoram un tavam gaišās/tumšās tēmas iestatījumam, kurš tiek saglabāts tavā pašā ierīcē. Bez trešo pušu resursiem, bez trekeriem, bez profilēšanas, bez datu kopīgošanas. Ja vēlies mums sekot: [RSS](#).