

Какво всъщност е VPN

Променя кой може да те вижда, а не дали някой може.

Казано просто: VPN прави така, че твоят интернет доставчик или Wi-Fi на летището да спрат да виждат къде се свързваш. Тази информация не изчезва: тя преминава към компанията за VPN, която сега я вижда. Онова, което вече пътуваше криптирано, като пощата или банката, беше криптирано и преди това. Служи за няколко конкретни неща и често се продава така, сякаш върши много повече.

С години чувах за VPN и не им обръщах внимание, точно както и за антивирусните: не ползвам антивирусна, или почти никога. Имам копия на всичко на три места в реално време и много внимавам какво тегля, какви връзки отварям и какви сайтове посещавам. Това не е стопроцентова сигурност, но при мен работи. Един ден видях оферта за VPN за малко над две евро на месец и я взех от любопитство. Работи добре, но ми послужи за малко: например да изпробвам услуга, която тогава беше достъпна само в САЩ. Чувствам ли се по-защитен? Не. Ако отново ми я предложат на тази цена, може и да я подновя; ако ли не — не. Това е само моят опит, той нищо не доказва. Затова се запитах какво точно прави един VPN. Ето как го разбрах аз.

Представи си, че пускаш писмо в пощенската кутия с ясно видим адрес на получателя. Пощальонът вижда на кого го изпращаш, въпреки че не може да го прочете, ако е запечатано. Този пощальон е твоят интернет доставчик. VPN слага писмото ти в друг плик, адресиран до посредник, който го отваря и го препраща. Твоят обичаен пощальон вече не вижда истинския адрес. Вижда само, че пишеш на този посредник.

Онзи, който контролира мрежата, от която се свързваш — например Wi-Fi на летище —, спира да вижда къде ходиш. Но посредникът сега вижда онова, което виждаше твоят доставчик, а понякога и повече, защото целият ти трафик минава през него. Наблюдението не изчезва: то сменя ръцете си. Оттам и името.

Освен това почти всичко, което правиш днес — като отваряне на пощата или вход в банката —, вече пътува криптирано до крайния сървър благодарение на катинара в брауъра. Това се случва с VPN и без него. VPN добавя защита само в първия участък, до собствения си сървър. Оттам нататък пътят е същият както винаги.

Затова има неща, които не може да ти обещае, макар че понякога се рекламира точно така. Ако си влязъл в пощата или в банката си, тази услуга знае, че това си ти, с VPN или без него. Не гарантира и че никой не наблюдава трафика ти: променя само кой наблюдава. Това, че компанията твърди, че «не пази логове», е обещание — точно както когато голяма платформа казва «съобщенията ви са криптирани, ние не ги четем». Един одит може да го потвърди в даден момент, но то остава нещо, на чието изпълнение разчиташ, а не нещо, което не може да бъде нарушено по проект.

И съдържанието на един разговор остава същото. Ако твоето приложение за съобщения вече криптира от край до край, VPN не добавя нищо. Ако не го прави, VPN също не решава проблема: той защитава пътя на съобщението, а не какво правят с него приложението или неговият сървър след пристигането.

Нищо от това не го прави безполезен. Да скриеш къде се свързваш от обществен Wi-Fi, от доставчик, който би искал да продаде тази история, или от държава, която блокира услуга, е реална задача и той я

върши добре. Маркетингът обаче обикновено обещава повече, отколкото този слой може да даде.

Въпросът, който си струва да си зададеш при VPN или всяка услуга, която обещава да те защити, не е «криптирано ли е?». Вероятно да, поне в един участък. Въпросът е друг: в кого влагам доверието, което отнех от друг? И какво ми остава, ако то се окаже неоправдано?

VPN, когато върши работата си добре, променя само кой е посредникът на твоята връзка. Приложение като Solo2, чиито съобщения не минават през никакъв сървър, премахва посредника от разговора напълно. Те не се конкурират: решават различни проблеми.

Да ги бъркаш е много разпространен начин да се смяташ за по-защитен, отколкото си в действителност.

Редакционна бележка: Когато тези Cuadernos споменават компании или продукти, това не е с цел обвинение. Хората, които ги създават, вършат работа, която милиони използват и ценят. Това, което посочваме, е структурно — моделът, а не марката. Марките се появяват като пример, защото са тези, които читателят разпознава.

Източници и допълнително четиво

- Протоколът HTTPS и транспортното криптиране са отворени стандарти, публично документирани от IETF.
- В същата поредица: «Когато няма никой по средата» и «Не сте анонимни» разглеждат от други ъгли същото разграничение между структура и обещание.

[← Предишна](#)[Не си анонимен](#)

Скорошни четива

- [Размисъл · 29 юни 2026 г. Не си анонимен](#)
- [Размисъл · 27 май 2026 г. Какво един подпис не може да поправи](#)
- [Анализ · 26 май 2026 г. Реална срещу привидна поверителност: въпросите, които е добре да си зададеш](#)

Вземи тази статия със себе си навсякъде, където ти е необходима.

[↓ Markdown](#) [↓ Обикновен текст](#) [↓ PDF](#)

Файлът се изтегля на твоето устройство. Оттам можеш да го запазиш, импортираш в Solo2 или споделиш където пожелаеш. Cuadernos не решава дестинацията вместо теб.

Восъчен печат · SHA-256 52c524da6a5fd1888f4d9d7d89166b7658160b1979a57f6d4185e89912fc40c2

[Функции](#) [Цени](#) [Инсталиране](#) [Новости](#) [Blog](#) [Pro](#) [Помощ](#) [Относно](#) [Контакт](#)
[Прозрачност](#) [Верификация](#) [Поверителност](#) [Условия](#) [Бисквитки](#)

Cuadernos Lacre · Публикация на [Menzuri Gestión S.L.](#) ·
написана от R.Eugenio · редактирана от екипа на [Solo2](#).

Този уебсайт не използва бисквитки. Всичко, което зарежда твоят браузър, е написано или контролирано от нас и се съхранява на нашите европейски сървъри: анонимният брояч на посещения (Umami, самостоятелно хостван) и минималният необходим JavaScript за избора на език и твоята настройка за светла/тъмна тема, която се запазва на собственото ти устройство. Без ресурси от трети страни, без тракери, без профилиране, без споделяне на данни. Ако искаш да ни последваш: [RSS](#).