

Cos'è davvero una VPN

Cambia chi può vederti, non se qualcuno può farlo.

In parole semplici: una VPN impedisce al tuo fornitore internet o al Wi-Fi di un aeroporto di vedere dove ti colleghi. Questa informazione non scompare: passa all'azienda della VPN, che ora la vede. Ciò che viaggiava già cifrato, come la posta o la banca, lo era anche prima. Serve a pochi scopi precisi e viene spesso venduta come se servisse a molto di più.

Per anni ho sentito parlare di VPN e non me ne sono curato, proprio come con gli antivirus: non uso antivirus, o quasi mai. Ho copie di tutto in tre posti diversi, in tempo reale, e sto molto attento a cosa scarico, ai link su cui clicco e ai siti che visito. Non è una sicurezza al cento per cento, ma per me funziona. Un giorno ho visto un'offerta per una VPN a poco più di due euro al mese e l'ho attivata per curiosità. Funziona bene, ma mi è servita a poco: ad esempio, per provare un servizio che all'epoca era accessibile solo negli Stati Uniti. Mi sento più sicuro? No. Se me la riufrissero a quel prezzo, forse la rinnoverei; altrimenti no. È solo la mia esperienza, non dimostra nulla. Così mi sono chiesto cosa faccia esattamente una VPN. Ecco come l'ho capita io.

Immagina di imbucare una lettera con l'indirizzo del destinatario ben visibile. Il postino vede a chi la invii, anche se non può leggerla se è sigillata. Quel postino è il tuo operatore internet. Una VPN infila la tua lettera dentro un'altra busta, indirizzata a un intermediario che la apre e la rispedisce. Il tuo postino abituale non vede più l'indirizzo reale. Vede solo che stai scrivendo a quell'intermediario.

Chi controlla la rete da cui ti colleghi, ad esempio il Wi-Fi di un aeroporto, non vede più dove vai. Ma l'intermediario vede ora ciò che vedeva il tuo operatore, e talvolta di più, perché tutto il tuo traffico passa attraverso di lui. La sorveglianza non scompare: cambia di mano. Da qui il nome.

Inoltre, quasi tutto ciò che fai oggi, come aprire l'email o accedere alla banca, viaggia già cifrato fino al server di destinazione grazie al lucchetto del browser. Questo accade con e senza VPN. La VPN aggiunge protezione solo nel primo tratto, fino al proprio server. Da lì in poi, la strada è quella di sempre.

Per questo ci sono cose che non può prometterti, anche se a volte viene venduta così. Se hai effettuato l'accesso alla tua posta o alla tua banca, quel servizio sa chi sei, con o senza VPN. Non garantisce nemmeno che nessuno guardi il tuo traffico: cambia solo chi guarda. Quando l'azienda afferma di «non conservare registri», è una promessa, esattamente come quando una grande piattaforma dice «i tuoi messaggi sono cifrati, non li leggiamo». Un audit può certificarlo in un dato momento, ma resta qualcosa che confidi venga rispettato, non un'impossibilità garantita dalla struttura.

E il contenuto di una conversazione resta identico. Se la tua app di messaggistica cifra già end-to-end, la VPN non aggiunge nulla. Se non lo fa, la VPN non risolve il problema: protegge il tragitto del messaggio, non ciò che l'app o il suo server ne fanno una volta arrivato.

Nulla di tutto questo la rende inutile. Nascondere dove ti colleghi da un Wi-Fi pubblico, da un operatore che vorrebbe vendere quella cronologia o da uno Stato che blocca un servizio è un lavoro concreto, e lo fa bene. Il marketing, invece, promette spesso più di quanto questo livello possa dare.

La domanda da porsi, con una VPN o con qualsiasi servizio che promette di proteggerti, non è «è cifrato?». Probabilmente sì, almeno per un tratto. È questa: in chi sto riponendo la fiducia che ho tolto a un altro? E cosa mi resta se si rivela ingiustificata?

Una VPN, quando lavora bene, cambia soltanto l'intermediario della tua connessione. Un'app come Solo2, i cui messaggi non passano attraverso alcun server, toglie del tutto l'intermediario dalla conversazione. Non competono: risolvono problemi diversi.

Confonderle è un modo comunissimo di credersi più protetti di quanto non si sia davvero.

Nota editoriale: quando questi Cuadernos menzionano aziende o prodotti, non è per accusare. Chi li costruisce fa un lavoro che milioni di persone usano e apprezzano. Ciò che segnaliamo è strutturale — il modello, non il marchio. I marchi appaiono come esempio perché sono quelli che il lettore riconosce.

Fonti e letture aggiuntive

- Il protocollo HTTPS e la cifratura del trasporto sono standard aperti, documentati pubblicamente dall'IETF.
- In questa stessa raccolta: «Quando non c'è nessuno in mezzo» e «Non sei anonimo» approfondiscono, da altri punti di vista, la stessa distinzione tra struttura e promessa.

[← Precedente](#)[Non sei anonimo](#)

Letture recenti

- [Riflessione · 29 giugno 2026 Non sei anonimo](#)
- [Riflessione · 27 maggio 2026 Ciò che una firma non può risolvere](#)
- [Analisi · 26 maggio 2026 Privacy reale vs apparente: le domande da porsi](#)

Porta questo articolo dove ne hai bisogno.

[↓ Markdown](#) [↓ Testo semplice](#) [↓ PDF](#)

Il file viene scaricato sul tuo dispositivo. Da lì puoi salvarlo, importarlo in Solo2 o condividerlo come preferisci. Cuadernos non decide la destinazione per te.

Sigillo di cera · SHA-256 829be5eaa537b6230df98590b8b25ed140ff11f9c610f719d5d217f43eab150a

[Funzionalità](#) [Prezzi](#) [Installa](#) [Novità](#) [Blog](#) [Pro](#) [Aiuto](#) [Chi siamo](#) [Contatti](#)
[Trasparenza](#) [Verifica](#) [Privacy](#) [Condizioni](#) [Cookie](#)

Cuadernos Lacre · Una pubblicazione di [Menzuri Gestión S.L.](#) ·
scritta da R.Eugenio · a cura del team di [Solo2](#).

Questo sito non utilizza cookie. Tutto ciò che il tuo browser carica è scritto o supervisionato da noi e ospitato sui nostri server europei: il contatore di visite anonimo (Umami, autoospitato) e il minimo JavaScript necessario per il selettore di lingua e la tua preferenza di tema chiaro/scuro, che viene salvata sul tuo dispositivo. Senza risorse di terze parti, senza tracker, senza profilazione, senza condivisione di dati. Se vuoi seguirci: [RSS](#).