

Hva et VPN egentlig er

Det endrer hvem som kan se deg, ikke om noen kan.

Kort forklart: Et VPN gjør at internettleverandøren din eller flyplass-Wi-Fi-en slutter å se hvor du kobler deg til. Denne informasjonen forsvinner ikke; den sendes til VPN-selskapet, som nå ser den i stedet. Det som allerede var kryptert, som e-post eller nettbank, var kryptert fra før også. Det tjener noen få konkrete formål, men selges ofte som om det løste langt mer.

I årevis hørte jeg snakk om VPN og brydde meg ikke, akkurat som med antivirus: Jeg bruker ikke antivirus, eller nesten aldri. Jeg har sanntidskopier av alt på tre steder, og er veldig forsiktig med hva jeg laster ned, hvilke lenker jeg klikker på, og hvilke nettsider jeg besøker. Det er ikke hundre prosent sikkerhet, men det fungerer for meg. En dag så jeg et VPN-tilbud til litt over to euro i måneden og kjøpte det av nysgjerrighet. Det fungerer fint, men har vært til lite nytte: for eksempel for å teste en tjeneste som den gangen bare var tilgjengelig i USA. Føler jeg meg tryggere? Nei. Hvis de tilbyr meg det til den prisen igjen, fornyer jeg kanskje; hvis ikke, nei. Det er bare min erfaring, det beviser ingenting. Så jeg spurte meg selv hva et VPN egentlig gjør. Slik har jeg forstått det.

Se for deg at du legger et brev i postkassen med mottakerens adresse godt synlig. Postbudet ser hvem du sender det til, selv om han ikke kan lese det når det er lukket. Det postbudet er internettleverandøren din. Et VPN legger brevet ditt inn i en ny konvolutt, adressert til et mellomledd som åpner det og videresender det. Det vanlige postbudet ditt ser ikke lenger den egentlige adressen. Han ser bare at du skriver til det mellomleddet.

Den som kontrollerer nettverket du kobler deg til fra, for eksempel Wi-Fi på en flyplass, slutter å se hvor du går. Men mellomleddet ser nå det operatøren din pleide å se, og noen ganger mer, fordi all trafikken din går gjennom det. Overvåkingen forsvinner ikke: Den skifter hender. Derav navnet.

Dessuten reiser nesten alt du gjør i dag, som å sjekke e-post eller gå i banken, allerede kryptert frem til målserveren takket væreengelåsen i nettleseren. Det skjer med og uten VPN. Et VPN legger bare til beskyttelse på det første strekket, frem til sin egen server. Derfra er veien den vanlige.

Derfor er det ting det ikke kan love deg, selv om det noen ganger markedsføres slik. Hvis du er logget inn på e-posten din eller i banken din, vet den tjenesten hvem du er, med eller uten VPN. Det garanterer heller ikke at ingen ser på trafikken din: Det endrer bare hvem som ser. Når selskapet sier at det «ikke lagrer logger», er det et løfte, akkurat som når en stor plattform sier «meldingene dine er kryptert, vi leser dem ikke». En revisjon kan bekrefte det på et gitt tidspunkt, men det forblir noe du stoler på at overholdes – ikke noe som er umulig å bryte etter selve designet.

Og innholdet i en samtale forblir det samme. Hvis meldingsappen din allerede krypterer ende-til-ende, tilfører ikke VPN noe som helst. Gjør den ikke det, løser ikke VPN det heller: Det beskytter veien meldingen tar, ikke hva appen eller serveren gjør med den når den kommer frem.

Ingenting av dette gjør det ubrukelig. Å skjule hvor du kobler deg til for et offentlig Wi-Fi, for en operatør som ønsker å selge den historikken, eller for et land som blokkerer en tjeneste, er en reell oppgave, og det gjør det godt. Markedsføringen lover derimot ofte mer enn det dette laget kan levere.

Spørsmålet man bør stille seg med et VPN eller enhver tjeneste som lover å beskytte deg, er ikke «er det kryptert?». Sannsynligvis ja, i det minste på et strekk. Det er dette andre: Hvem plasserer jeg tilliten hos, som jeg har frattatt en annen? Og hva sitter jeg igjen med hvis den viser seg uberettiget?

Et VPN endrer, når det gjør jobben sin godt, bare hvem som er mellomledd for tilkoblingen din. En app som Solo2, der meldingene ikke går gjennom noen server, fjerner mellomleddet fra samtalen helt. De konkurrerer ikke: De løser ulike problemer.

Å forveksle dem er en svært vanlig måte å tro at man er mer beskyttet enn man faktisk er.

Redaksjonell note: når disse Cuadernos nevner selskaper eller produkter, er det ikke for å anklage. De som bygger dem, gjør en jobb som millioner av mennesker bruker og verdsetter. Det vi påpeker er strukturelt — modellen, ikke merkevaren. Merkevarene vises som eksempler fordi det er disse leseren kjenner til.

Kilder og videre lesing

- HTTPS-protokollen og transportkryptering er åpne standarder, offentlig dokumentert av IETF.
- I samme serie: «Når ingen er i midten» og «Du er ikke anonym» belyser fra andre vinkler det samme skillet mellom struktur og løfte.

[← Forrige](#)[Du er ikke anonym](#)

Siste lesninger

- [Refleksjon · 29. juni 2026 Du er ikke anonym](#)
- [Refleksjon · 27. mai 2026 Det en signatur ikke kan fikse](#)
- [Analyse · 26. mai 2026 Reelt vs. tilsynelatende personvern: Spørsmålene man bør stille seg selv](#)

Ta med deg denne artikkelen dit du trenger den.

[↓ Markdown](#) [↓ Klartekst](#) [↓ PDF](#)

Filen lastes ned til enheten din. Derfra kan du lagre den, importere den til Solo2 eller dele den hvor du vil. Cuadernos bestemmer ikke destinasjonen for deg.

Lakksegl · SHA-256 ef8a840c8efb2a0ac8678eb39561833e44027736a4ac426b04d9f39cc5a23edd

[Egenskaper](#) [Priser](#) [Installer](#) [Nyheter](#) [Blogg](#) [Pro](#) [Hjelp](#) [Om](#) [Kontakt](#)
[Åpenhet](#) [Verifisering](#) [Personvern](#) [Vilkår](#) [Informasjonskapsler](#)

Cuadernos Lacre · En utgivelse fra [Menzuri Gestión S.L.](#) · skrevet av R.Eugenio · redigert av teamet bak [Solo2](#).

Dette nettstedet bruker ikke informasjonskapsler. Alt som nettleseren din laster inn, er skrevet eller overvåket av oss og plassert på våre europeiske servere: den anonyme besøkstelleren (Umami, selvhostet) og det minimale JavaScript som kreves for språkvelgeren og innstillingen din for lyst eller mørkt tema, som lagres på din egen enhet. Ingen ressurser fra eksterne selskaper, ingen trackere, ingen profilering, ingen deling av data. Hvis du vil følge oss: [RSS](#).