

Hvad en VPN egentlig er

Den ændrer, hvem der kan se dig, ikke om nogen kan.

Kort fortalt: En VPN forhindrer din internetudbyder eller et lufthavns-Wi-Fi i at se, hvor du forbinder dig hen. De oplysninger forsvinder ikke; de sendes til VPN-firmaet, som nu kan se dem i stedet. Det, der allerede var krypteret, som e-mails eller bankforretninger, var det også i forvejen. Den tjener nogle få konkrete formål, men sælges ofte, som om den løste langt mere.

I årevis hørte jeg om VPN og ignorerede det, ligesom med antivirus: Jeg bruger ikke antivirus, eller næsten aldrig. Jeg har realtidsskoplere af alt tre steder, og jeg passer meget på, hvad jeg downloader, hvilke links jeg klikker på, og hvilke hjemmesider jeg besøger. Det er ikke hundrede procent sikkerhed, men det virker for mig. En dag så jeg et VPN-tilbud til lidt over to euro om måneden og købte det af nysgerrighed. Det fungerer fint, men har nyttet mig meget lidt: for eksempel til at teste en tjeneste, der dengang kun var åben i USA. Føler jeg mig mere sikker? Nej. Hvis de tilbyder mig det til den pris igen, fornyer jeg måske; hvis ikke, så nej. Det er bare min erfaring, det beviser ingenting. Så jeg spurgte mig selv, hvad en VPN egentlig gør. Her er, hvordan jeg forstod det.

Forestil dig, at du putter et brev i postkassen med modtagerens adresse tydeligt synlig. Postbuddet ser, hvem du sender det til, selvom vedkommende ikke kan læse brevet, når det er lukket. Det postbud er din internetudbyder. En VPN lægger dit brev ind i en anden konvolut, adresseret til en mellemmand, der åbner det og sender det videre. Dit vante postbud ser ikke længere den rigtige adresse. Han ser kun, at du skriver til den mellemmand.

Den, der kontrollerer det netværk, du forbinder fra – for eksempel et lufthavns-Wi-Fi –, ser ikke længere, hvor du surfer hen. Men mellemmanden ser nu det, din udbyder plejede at se, og somme tider mere, fordi al din trafik passerer igennem ham. Overvågningen forsvinder ikke: Den skifter hænder. Heraf navnet.

Desuden rejser næsten alt, hvad du gør i dag – som at åbne din mail eller gå i banken –, allerede krypteret frem til destinationsserveren takket være hængelåsen i browseren. Det sker med og uden VPN. En VPN tilføjer kun beskyttelse på det første stykke vej, frem til dens egen server. Derfra er vejen den sædvanlige.

Derfor er der ting, den ikke kan love dig, selvom den somme tider markedsføres sådan. Hvis du er logget ind på din mail eller din bank, ved den tjeneste, hvem du er, med eller uden VPN. Den garanterer heller ikke, at ingen kigger på din trafik: Den ændrer kun, hvem der kigger. Når firmaet siger, at det «ikke gemmer logfiler», er det et løfte, fuldstændig ligesom når en stor platform siger «dine beskeder er krypterede, vi læser dem ikke». En revision kan bekræfte det på et givet tidspunkt, men det forbliver noget, du stoler på overholdes – ikke noget, der er umuligt at bryde per design.

Og indholdet af en samtale forbliver det samme. Hvis din beskedapp allerede krypterer fra ende til anden, tilføjer VPN intet. Hvis den ikke gør det, løser VPN det heller ikke: Den beskytter beskedens vej, ikke hvad appen eller dens server gør med den, når den er fremme.

Intet af dette gør den ubrugelig. At skjule, hvor du forbinder dig hen for et offentligt Wi-Fi, for en udbyder, der gerne vil sælge den historik, eller for et land, der blokerer en tjeneste, er et reelt stykke arbejde, og det gør den godt. Markedsføringen lover dog som regel mere, end det lag kan levere.

Det spørgsmål, man bør stille sig selv ved en VPN eller enhver tjeneste, der lover at beskytte dig, er ikke «er det krypteret?». Det er det formentlig, i hvert fald på en strækning. Det er derimod dette: Hvem placerer jeg den tillid hos, som jeg har frtaget en anden? Og hvad har jeg tilbage, hvis den viser sig ubegrundet?

En VPN ændrer, når den gør sit arbejde godt, kun hvem der er mellemmand på din forbindelse. En app som Solo2, hvis beskeder ikke passerer gennem nogen server, fjerner mellemmanden helt fra samtalen. De konkurrerer ikke: De løser forskellige problemer.

At forveksle dem er en meget udbredt måde at bilde sig ind, at man er mere beskyttet, end man i virkeligheden er.

Redaktionel note: Når disse Cuadernos nævner virksomheder eller produkter, er det ikke for at anklage. De, der bygger dem, udfører et stykke arbejde, som millioner bruger og værdsætter. Det, vi påpeger, er strukturelt — modellen, ikke brandet. Brands optræder som eksempler, fordi det er dem, læseren genkender.

Kilder og yderligere læsning

- HTTPS-protokollen og transportkryptering er åbne standarder, offentligt dokumenteret af IETF.
- I denne serie belyser «Når der ikke er nogen imellem» og «Du er ikke anonym» fra andre vinkler den samme sondring mellem struktur og løfte.

[← Forrige Du er ikke anonym](#)

Seneste læsning

- [Refleksion · 29. juni 2026 Du er ikke anonym](#)
- [Refleksion · 27. maj 2026 Hvad en underskrift ikke kan løse](#)
- [Analyse · 26. maj 2026 Reelt vs. tilsyneladende privatliv: De spørgsmål, man bør stille sig selv](#)

Tag denne artikel med dig, hvor du har brug for den.

[↓ Markdown](#) [↓ Almindelig tekst](#) [↓ PDF](#)

Filen downloades til din enhed. Derfra kan du gemme den, importere den til Solo2 eller dele den, hvor du vil. Cuadernos beslutter ikke destinationen for dig.

Laksegl · SHA-256 4a3567f49a4886d520b63508be548686561b5f049c65a58d0c2e45143c7ed516

[Funktioner](#) [Priser](#) [Installer](#) [Nyheder](#) [Blog](#) [Pro](#) [Hjælp](#) [Om](#) [Kontakt](#)
[Gennemsigthed](#) [Verifikation](#) [Privatliv](#) [Vilkår](#) [Cookies](#)

Cuadernos Lacre · En udgivelse fra [Menzuri Gestión S.L.](#) · skrevet af R.Eugenio · redigeret af holdet bag [Solo2](#).

Dette websted bruger ikke cookies. Alt, hvad din browser indlæser, er skrevet eller overvåget af os og hostet på vores europæiske servere: den anonyme besøgstæller (Umami, selvhøstet) og den mindst mulige JavaScript, der er nødvendig for sprogvalgeren og din præference for lyst/mørkt tema, som gemmes på din egen enhed. Ingen ressourcer fra tredjeparter, ingen trackere, ingen profilering, ingen deling af data. Hvis du vil følge os: [RSS](#).