

Vad en VPN egentligen är

Den ändrar vem som kan se dig, inte om någon kan det.

Kort sagt: En VPN gör att din internetleverantör eller flygplatsens Wi-Fi slutar se vart du ansluter. Den informationen försvinner inte; den skickas vidare till VPN-företaget, som nu ser den i stället. Det som redan reste krypterat, som e-post eller bankärenden, var krypterat även innan. Den tjänar några få konkreta syften och säljs ofta som om den löste mycket mer.

I flera år hörde jag talas om VPN och brydde mig inte om det, precis som med antivirus: Jag använder inget antivirus, eller nästan aldrig. Jag har realtidskopior av allt på tre platser och är mycket försiktig med vad jag laddar ner, vilka länkar jag klickar på och vilka webbplatser jag besöker. Det är inte hundra procentig säkerhet, men det fungerar för mig. En dag såg jag ett VPN-erbjudande för drygt två euro i månaden och skaffade det av ren nyfikenhet. Det fungerar bra, men har varit till ringa nytta: till exempel för att prova en tjänst som då bara var öppen i USA. Känner jag mig säkrare? Nej. Om de erbjuder mig det till det priset igen förnyar jag kanske; om inte, nej. Det är bara min egen erfarenhet, det bevisar ingenting. Så jag frågade mig vad en VPN egentligen gör. Så här har jag förstått det.

Föreställ dig att du lägger ett brev på brevlådan med mottagarens adress fullt synlig. Brevbäraren ser vem du skickar det till, även om han inte kan läsa det om det är förseglat. Den brevbäraren är din internetleverantör. En VPN stoppar ditt brev i ett annat kuvert, adresserat till en mellanhand som öppnar det och skickar det vidare. Din vanliga brevbärare ser inte längre den verkliga adressen. Han ser bara att du skriver till den mellanhanden.

Den som kontrollerar nätverket du ansluter ifrån, till exempel ett flygplats-Wi-Fi, slutar se vart du surfar. Men mellanhanden ser nu det din operatör brukade se, och ibland mer, eftersom all din trafik passerar genom denne. Övervakningen försvinner inte: Den byter ägare. Därav namnet.

Dessutom reser nästan allt du gör idag, som att öppna e-post eller logga in på banken, redan krypterat fram till målservern tack vare webbläsarens hänglås. Det sker med och utan VPN. En VPN lägger bara till skydd på den första delsträckan, fram till sin egen server. Därifrån är vägen den vanliga.

Därför finns det saker den inte kan lova dig, även om den ibland marknadsförs så. Om du har loggat in på din e-post eller din bank vet den tjänsten vem du är, med eller utan VPN. Den garanterar inte heller att ingen granskar din trafik: Den ändrar bara vem som tittar. Att företaget säger att det «inte sparar loggar» är ett löfte, precis som när en stor plattform säger «dina meddelanden är krypterade, vi läser dem inte». En revision kan bekräfta det vid ett givet tillfälle, men det förblir något du litar på efterlevs – inte något som är omöjligt att bryta genom själva konstruktionen.

Och innehållet i en konversation förblir detsamma. Om din meddelandeapp redan krypterar ände till ände tillför en VPN ingenting. Om den inte gör det lagar VPN inte heller saken: Den skyddar meddelandets väg, inte vad appen eller dess server gör med det när det kommer fram.

Inget av detta gör den värdelös. Att dölja vart du ansluter för ett offentligt Wi-Fi, för en operatör som vill sälja den historiken eller för ett land som blockerar en tjänst är ett verkligt arbete, och det gör den väl. Marknadsföringen lovar dock oftast mer än vad detta skikt kan ge.

Frågan man bör ställa sig med en VPN eller vilken tjänst som helst som lovar att skydda dig är inte «är det krypterat?». Förmodligen ja, åtminstone på en sträcka. Frågan är denna andra: Vem placerar jag det förtroende hos som jag har tagit ifrån någon annan? Och vad har jag kvar om det visar sig obefogat?

En VPN, när den gör sitt jobb väl, ändrar bara vem som är mellanhand för din anslutning. En app som Solo2, vars meddelanden inte passerar genom någon server alls, tar bort mellanhanden från samtalet helt. De konkurrerar inte: De löser olika problem.

Att förväxla dem är ett mycket vanligt sätt att tro sig mer skyddad än man i själva verket är.

Redaktionell not: när dessa Cuadernos nämner företag eller produkter är det inte för att anklaga. De som bygger dem gör ett jobb som miljontals människor använder och uppskattar. Det vi pekar på är strukturellt — modellen, inte varumärket. Varumärken visas som exempel eftersom det är dessa läsaren känner igen.

Källor och vidare läsning

- HTTPS-protokollet och transportkryptering är öppna standarder, offentligt dokumenterade av IETF.
- I samma serie: «När ingen är emellan» och «Du är inte anonym» utvecklar ur andra vinklar samma skillnad mellan struktur och löfte.

[← Föregående](#)[Du är inte anonym](#)

Senaste läsning

- [Reflektion · 29 juni 2026 Du är inte anonym](#)
- [Reflektion · 27 maj 2026 Det en signatur inte kan fixa](#)
- [Analys · 26 maj 2026 Verklig vs skenbar integritet: Frågorna man bör ställa sig](#)

Ta med dig den här artikeln dit du behöver den.

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

Filen laddas ner till din enhet. Därifrån kan du spara den, importera den till Solo2 eller dela den var du vill. Cuadernos bestämmer inte destinationen åt dig.

Lacksigill · SHA-256 5ced23d7f12e86711ab03de0c47087ce0fe53dea18b769739b937fd4f286a19f

[Funktioner](#) [Priser](#) [Installera](#) [Nyheter](#) [Blog](#) [Pro](#) [Hjälp](#) [Om oss](#) [Kontakt](#)
[Transparens](#) [Verifiering](#) [Integritet](#) [Villkor](#) [Cookies](#)

Cuadernos Lacre · En utgåva från [Menzuri Gestión S.L.](#) ·
skriven av R.Eugenio · redigerad av teamet bakom [Solo2](#).

Denna webbplats använder inte cookies. Allt som din webbläsare laddar är skrivet eller övervakat av oss och placerat på våra europeiska servrar: den anonyma besöksräknaren (Umami, självhostad) och det minimala JavaScript som krävs för språkväljaren och din inställning för ljus eller mörkt tema, som sparas på din egen enhet. Inga resurser från externa företag, inga trackers, ingen profilering, ingen datadelning. Om du vill följa oss: [RSS](#).