

What a VPN Really Is

It changes who can see you, not whether someone can.

To put it plainly: a VPN stops your internet provider, or an airport Wi-Fi, from seeing where you connect. That information does not disappear; it is passed to the VPN company, which now sees it instead. What was already encrypted, like email or your bank, was encrypted beforehand as well. It serves a few specific purposes and is often sold as if it solved many more.

For years I heard about VPNs and ignored them, just like antivirus software: I don't use antivirus, or almost never. I keep real-time copies of everything in three places, and I am very careful about what I download, which links I click, and which websites I visit. It isn't one-hundred percent security, but it works for me. One day I saw a VPN offer for just over two euros a month and signed up out of curiosity. It works well, but it has served me little: for instance, testing a service that was only open in the United States back then. Do I feel safer? No. If they offer it to me at that price again, I might renew; if not, no. It is just my experience; it proves nothing. So I asked myself what a VPN actually does. Here is how I understood it.

Imagine you drop a letter into the mailbox with the recipient's address clearly visible. The mail carrier sees who you are sending it to, even if they cannot read it when it is sealed. That mail carrier is your internet provider. A VPN puts your letter inside another envelope, addressed to an intermediary who opens it and forwards it. Your usual mail carrier no longer sees the real address. They only see that you are writing to that intermediary.

Whoever controls the network you connect from, like airport Wi-Fi, stops seeing where you go. But the intermediary now sees what your provider used to see, and sometimes more, because all your traffic passes through them. The surveillance does not disappear: it changes hands. Hence the name.

Furthermore, almost everything you do today, such as opening your email or logging into your bank, already travels encrypted to the destination server thanks to the browser's padlock. That happens with or without a VPN. A VPN adds protection only on the first leg, up to its own server. From there, the path is the usual one.

That is why there are things it cannot promise you, even if it is sometimes marketed that way. If you have signed into your email or bank, that service knows it is you, with or without a VPN. Nor does it guarantee that no one is watching your traffic: it only changes who is watching. When the company claims it «keeps no logs», that is a promise, just like when a large platform says «your messages are encrypted, we don't read them». An audit may back it up at a given moment, but it remains something you trust to be honored, not something that cannot be broken by design.

And the content of a conversation remains the same. If your messaging app already encrypts end-to-end, a VPN adds nothing. If it doesn't, a VPN doesn't fix it either: it protects the path of the message, not what the app or its server do with it upon arrival.

None of this makes it useless. Hiding where you connect from public Wi-Fi, from a provider that might sell that history, or from a country blocking a service is real work, and it does it well. Marketing, however, usually promises far more than that layer can deliver.

The question worth asking, with a VPN or any service that promises to protect you, is not «is it encrypted?». Probably yes, at least along one stretch. It is this one: in whom am I placing the trust I took away from someone else? And what am I left with if it proves unwarranted?

A VPN, when it does its job well, only changes who the intermediary of your connection is. An app like Solo2, whose messages pass through no server at all, removes the intermediary from the conversation. They do not compete: they solve different problems.

Confusing them is a very common way to believe you are more protected than you actually are.

Editor's note: when these Cuadernos name companies or products, it is not to accuse. Those who build them do work that millions of people use and appreciate. What we point out is structural — the model, not the brand. Brands appear as examples because they are the ones the reader recognizes.

Sources and further reading

- The HTTPS protocol and transport encryption are open standards, publicly documented by the IETF.
- In this same collection: “When no one is in between” and “You are not anonymous” explore, from other angles, the same distinction between structure and promise.

[← Previous You Are Not Anonymous](#)

Recent readings

- [Reflection · June 29, 2026 You Are Not Anonymous](#)
- [Reflection · May 27, 2026 What a signature cannot fix](#)
- [Analysis · May 26, 2026 Real vs. apparent privacy: the questions to ask yourself](#)

Take this article wherever you need it.

[↓ Markdown](#) [↓ Plain text](#) [↓ PDF](#)

The file is downloaded to your device. From there, you can save it, import it into Solo2, or share it as you wish. Cuadernos does not decide the destination for you.

Wax seal · SHA-256 0ea3d60061bfef41f6d3bc194ac3b3ca008be11b55f3c6efd925efd485853e5b

[Features](#) [Pricing](#) [Install](#) [What's New](#) [Blog](#) [Pro](#) [Help](#) [About](#) [Contact](#)
[Transparency](#) [Verification](#) [Privacy](#) [Terms](#) [Cookies](#)

Cuadernos Lacre · A publication of [Menzuri Gestión S.L.](#) ·
written by R.Eugenio · edited by the team of [Solo2](#).

This website does not use cookies. Everything your browser loads is written or supervised by us and hosted on our European servers: the anonymous visit counter (Umami, self-hosted) and the minimum JavaScript needed for the language selector and your light/dark theme preference, which is stored on your own device. No third-party resources, no trackers, no profiling, no data sharing. If you want to follow us: [RSS](#).