



WHAT IS A

VPN?

A plain-English guide to staying safer online
and getting a little more out of the internet

What a VPN actually is



A private tunnel for your internet traffic

VPN stands for “Virtual Private Network.” Normally, when you go online, your information travels out in the open — like sending a postcard anyone along the way could read. A VPN puts that information in a locked, scrambled envelope instead, so only you and the VPN can read it.



Hides your data

from anyone snooping on the same network



Hides your location

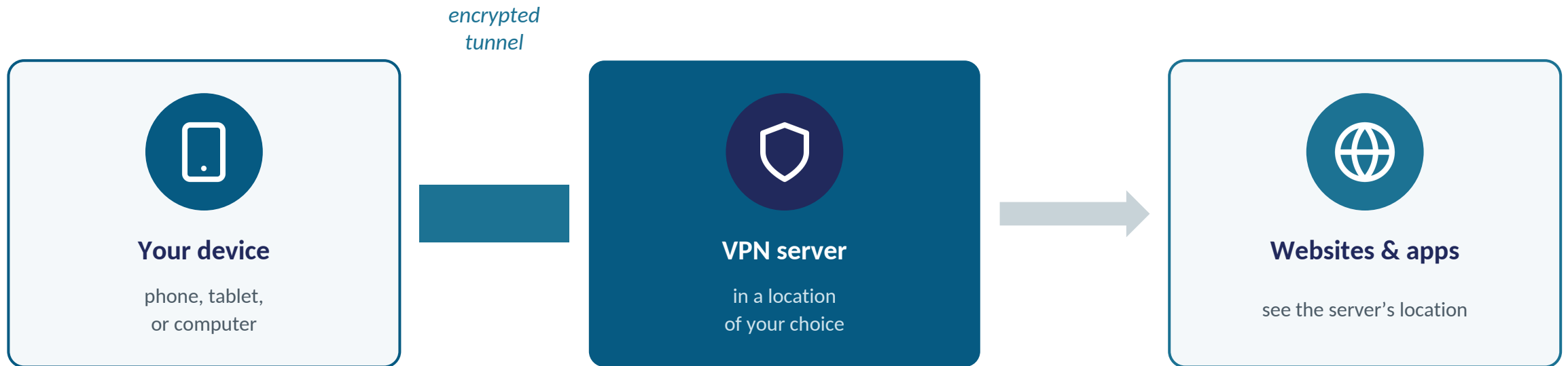
websites see the VPN’s location, not yours



Runs quietly

in the background as an app on your device

How a VPN works, step by step



In short: your data leaves your device already locked up, travels through the VPN's server, then heads out to the internet — appearing to come from that server's location instead of your own.

The main reason: privacy & security



Safer on public Wi-Fi

Coffee shops, airports, hotels, and libraries often have unsecured Wi-Fi. A VPN keeps your passwords and personal details private on those networks.



Keeps your browsing more private

Your internet provider can normally see every site you visit. A VPN keeps that list of sites private from your provider.



Adds a layer of protection

Online banking, shopping, and email already use their own security — a VPN adds an extra layer on top, especially away from home.

Fewer ads on YouTube? The Albania trick



Why some people connect to Albania

YouTube sells ads by country. Albania's ad market is very small, so YouTube often has no ad ready to show viewers there — meaning videos can play with little or no ads at all. Some people connect their VPN to an Albanian server just to take advantage of this gap.



Good to know before you try it

- It's an unofficial side effect, not a real feature — Google could close this gap at any time.
- It generally needs a reliable, paid VPN with Albanian servers; free VPNs rarely work well for it.
- Your account location and billing are unaffected — this only changes what the video player sees.

Can a VPN unlock Netflix from other countries?



What a VPN CAN do

- Make it look like you're browsing from another country.
- Sometimes reveal a different show or movie in that country's library.
- Work well for many other streaming or shopping sites with lighter blocking.



Where it usually falls short

- Netflix actively detects and blocks many VPN servers.
- If detected, you may only see titles licensed worldwide, or get an error message.
- It never changes your account's billing country or payment details.
- It goes against Netflix's terms of service, even though it isn't illegal.

When you probably don't need a VPN



At home, on your own trusted Wi-Fi

Everyday browsing, email, and video calls at home don't need a VPN for basic privacy — your own network is already reasonably safe.



When a site already shows a lock icon

Most banking, shopping, and email sites already encrypt the connection themselves (look for the padlock in the address bar). A VPN adds extra privacy, but it isn't the only thing keeping you safe there.



If it's slowing things down for no clear benefit

A VPN can make your connection a little slower. It's fine to turn it off for everyday tasks and turn it on when you actually want its benefits.

Setting up a VPN in five steps



1. Choose a reputable, paid VPN

Pick a well-reviewed provider (see next slide for what to look for).



2. Install its app

Download the official app on your phone, tablet, or computer.



3. Sign in

Use the account you created when you subscribed.



4. Tap “Connect”

Choose a country if you want a specific one, or use the nearest option.



5. Browse as usual

The VPN quietly protects your connection in the background.

Picking a VPN you can trust



Look for

- A paid subscription with a clear, well-known company behind it.
- A plain-language privacy policy that says it doesn't log your activity.
- Positive reviews from trusted tech publications.
- Simple apps for the devices you actually use.



Be cautious of

- Free VPNs — many make money by selling your browsing data instead.
- Pushy pop-ups urging you to install a VPN immediately.
- Apps with no clear company name, address, or support contact.
- Anyone asking for excessive personal or financial details up front.

A few reputable VPNs to consider



NordVPN

Widely rated as fast and reliable overall.

~\$3-4/mo (2-yr plan)
~\$13/mo month-to-month



Proton VPN

Known for strong privacy and a limited free plan.

~\$3/mo (2-yr plan)
~\$10/mo month-to-month



Private Internet Access (PIA)

Popular for affordability and deep customization.

~\$2-3/mo (long plan)
~\$12/mo month-to-month



ExpressVPN

Praised for simple, beginner-friendly apps.

~\$5-7/mo (annual plan)
~\$13-15/mo month-to-month



Surfshark

Budget-friendly with unlimited devices per plan.

~\$2-3/mo (2-yr plan)
~\$16/mo month-to-month

This isn't an endorsement of any single one — introductory prices are usually much lower than renewal rates, and current deals change often, so compare before subscribing.

QUICK RECAP

The short version



A VPN locks up your data in a private tunnel.



It's most useful on public Wi-Fi and for general privacy.



It can sometimes unlock other-country content — never guaranteed.



Choose a reputable, paid provider — skip free VPNs.



Questions?

Thank you for learning about VPNs with us.