

4.4 Virtual Private Networks (VPNs)

Core Concepts: Protect Yourself, Protect Your Data

VPNs are one of the most misunderstood security tools. They're marketed as making you "invisible online" which isn't true, but they do have legitimate, specific uses that can protect your privacy and security.

This section cuts through the marketing hype to explain what VPNs actually do, when you need one, when you don't, and how to choose and use one effectively.

4.4.1. Understanding VPNs

What is a VPN?

A Virtual Private Network creates an encrypted tunnel between your device and a VPN server. All your internet traffic goes through this tunnel before reaching its destination. A VPN protects your network traffic from local snooping on public WiFi, but it does not make you anonymous or protect you from phishing or malware.

Think of regular internet traffic like sending a postcard. Anyone handling it can read the message and see where it's going. A VPN puts your postcards in sealed envelopes and sends them to a trusted friend (the VPN server) who opens them and sends them to their final destination. The recipient sees the message as coming from your friend, not you.

What VPNs DO:

- **Encrypts your traffic:** Prevents people between you and the VPN server from seeing what you're doing
- **Hides your IP address:** Websites see the VPN server's IP, not yours
- **Hides activity from your ISP:** Your internet provider sees you're using a VPN but not what you're doing
- **Bypasses geographic restrictions:** Access content blocked in your location
- **Protection on public WiFi:** Secure your connection on untrusted networks

What VPNs DON'T DO:

- **Make you anonymous:** Websites can still identify you through logins, cookies, and device fingerprinting
- **Protect against malware:** You can still download viruses or visit phishing sites
- **Prevent tracking:** Facebook, Google, etc. still track you when you're logged in

The trade-off: VPNs add an extra step to your internet connection, which usually means slower speeds. You're trading some speed for privacy and security in specific situations.

When You Should Use a VPN

On Public or Untrusted WiFi

This is the real reason for using a VPN. Use a VPN when connected to any open (unencrypted) WiFi network. An open WiFi network is any network you do not have to enter a network key to connect to.

Note that captive portal sign-in is not the same thing. If you have ever connected to a network, then had to open a browser and sign in to get internet access, you were probably on an open network with a captive portal. A captive portal is a web page that appears when you connect to some WiFi networks (like at hotels or airports) requiring you to agree to terms or enter a password before accessing the internet. These do not offer any protection!

When you connect to an open WiFi network, all other people on the network can potentially see what you are doing. This means a malicious person could also tamper with the data coming from or going to your device. A VPN encrypts all your traffic so they cannot.

For Privacy from Your ISP

Your internet service provider can see all the websites you visit. A VPN hides this.

Why you might want this:

- ISPs can sell your browsing history to advertisers (legal in the US)
- ISPs may throttle certain types of traffic (streaming, gaming)
- You don't trust your ISP with your browsing data

Keep in mind: You're shifting trust from your ISP to your VPN provider. Choose your VPN provider carefully.

When You DON'T Need a VPN

To "Stay Anonymous Online"

VPNs don't make you anonymous, this is marketing hype. You are still tracked based on the accounts you log into, browser and device fingerprinting, tracking cookies, and payment information.

If you want more anonymity (for journalism, activism, etc.), you need specialized tools like Tor, not just a VPN.

4.4.2. The Basics

Choose a Reputable VPN Provider

This is the most important decision. A bad VPN provider is worse than no VPN as they can see and log everything you do. Avoid free tiers, as they make money by selling ads to you or your data to someone else. In fact, avoid any VPN that offers a free tier.

What to look for:

- **No-logs policy:** Provider doesn't keep records of your activity
- **Independent audit:** Third-party verification of no-logs claims
- **Strong encryption:** AES-256 or equivalent
- **Kill switch:** Blocks internet if VPN disconnects so you don't accidentally disclose unencrypted internet traffic
- **Based in privacy-friendly jurisdiction:** Not subject to invasive data retention laws
- **Good reputation:** Positive reviews from independent tech sites

My recommendation is Mullvad <https://mullvad.net/en>.

4.4.3. Better Protection

Install On Your Phone Too

(Tested with Mullvad, should be a similar process for others)

Android Setup:

- Install & Log In
 - Download from the Play Store
 - Log in or activate using your subscription code
- Enable Always-on VPN + Kill Switch

- Go to: Settings > Network & internet > VPN > [Your VPN] > Gear Icon
- Toggle: Always-on VPN
- Block connections without VPN (kill switch)
 - This ensures traffic only flows through the VPN when it's meant to.
- Configure Auto-Connect
 - In your VPN app: Settings > Auto-connect > On WiFi
 - Choose "Untrusted networks only".
 - Add your home/work SSIDs to the Trusted Network List.
- Use WireGuard
 - If offered, select WireGuard protocol for faster performance and quicker reconnections on unstable public WiFi.

iOS Setup:

- Install & Log In
 - Download from the App Store
 - Sign in or activate your account
- Enable Kill Switch
 - In the VPN app, toggle "Kill switch" or "Permanent VPN" (name varies)
 - This is critical on iOS because background app behavior can otherwise leak traffic
- Set Auto-Connect for Untrusted Networks
 - In the VPN app: Settings → Auto-connect → On WiFi
 - Choose "When joining unsecured networks" or "Untrusted networks only"
 - Add your safe networks (home/work) to the Trusted list
- Allow VPN Configurations
 - First time you enable Auto-connect, iOS will prompt to install a VPN profile; approve it

4.4.4. Extra Credit

Run Your Own VPN Server

Advanced users can set up their own VPN server.

Options:

- Cloud VPS (DigitalOcean, Linode, Vultr) - ~\$5/month
- Home server (Raspberry Pi, old computer)
- Use WireGuard or OpenVPN software

Benefits:

- Complete control; you're the VPN provider

- No third party to trust
- Access your home network from anywhere (if you host on your network)

Drawbacks:

- Doesn't hide activity from ISP (traffic still goes through your connection)
- Single server location (wherever you host it)
- Requires technical knowledge
- You're responsible for security and maintenance

Best for encrypting your traffic on a public WiFi or accessing your home network remotely, not for privacy from ISP or geographical restrictions.

Revision #1

Created 2026-07-12 21:54:33 UTC by Chris Landis

Updated 2026-07-12 21:56:34 UTC by Chris Landis