

VPN

Contents

- 1** What Is a VPN? The Basics Explained
- 2** How a VPN Works Behind the Scenes
- 3** Why You Need a VPN: Privacy in a Connected World
- 4** Myths Debunked
- 5** Types of VPNs: Personal, Business, Remote Access and Site-to-Site
- 6** VPN Protocols Explained: OpenVPN, WireGuard, IKEv2 and More
- 7** Choosing the Right VPN Provider
- 8** No-Logs Policies, Jurisdictions and Trust
- 9** Setting Up a VPN on Your Computer, Phone and Tablet
- 10** Using a VPN in Real Life: Streaming, Gaming, Travel, Wi-Fi, Troubleshooting and the Future

What Is a VPN?

The Basics Explained



A VPN, short for Virtual Private Network, is a tool that creates a secure, private connection between your device and a device on the internet. Think of it as a protected tunnel. Instead of your data travelling openly across the web, where others can potentially observe it, everything passes through this tunnel first.

Here is what normally happens when you go online. Your device connects through your internet provider, and every website you visit can see your real IP address, which works like a home address for your connection. It reveals roughly where you are and who your provider is. Your internet provider can also see which sites you visit, and on public networks, others may be able to snoop on your activity.

A VPN changes this in two important ways. First, it encrypts your data, scrambling it so that anyone intercepting it sees only meaningless code. Second, it routes your traffic through a VPN server run by the VPN provider. To the websites you visit, your connection appears to come from that server, not from your own device. Your real IP address stays hidden.

This means a VPN can help protect your privacy, keep you safer on public Wi-Fi in cafés, hotels and airports, and let you appear to be in a different country, which is useful for travel and accessing content.

Without a VPN, big companies use your IP address to work out where you come from. From that, they build a picture of who you are and show you ads aimed at you. A VPN breaks that link, because all they see is the VPN server, not you. This matters a great deal, and later in this book I will show you how to wiggle out of their grip and take a real step against big tech.

This also gives you a way to take back control of the ads you see. Because ads are matched to where you appear to be, you can choose a VPN server in a country where advertisers spend very little, such as the Democratic Republic of the Congo or Ethiopia. You will often see far fewer ads there, and on some services almost none. I tried it on Spotify and on YouTube, and it worked on both. It should work on other apps that show location-based ads too. If you only pay for something like YouTube Premium to get rid of ads, you may find you no longer need it. Results vary from one service to another, and some services have rules against changing your location, so check the terms before you rely on it.

There is a catch. As YouTube and other companies start showing general ads in these countries too, this trick may be short-lived. So do it while you can.

You 1, Big Tech 0.

Here is something even more useful, and a little surprising. A VPN setup can get you around your own router. Normally, if you want to reach a computer in your home network from the outside, you have to open doors on the router, known as ports, and every open door is also a way in for anyone else who wants to try. With a VPN, you do not need to open any of them. From wherever you are in the world, you connect through the VPN and reach the computer you want inside your local network, as if you were sitting at home. Without it, you would not be able to see

that computer at all. I will walk you through exactly how to do this later in the book.

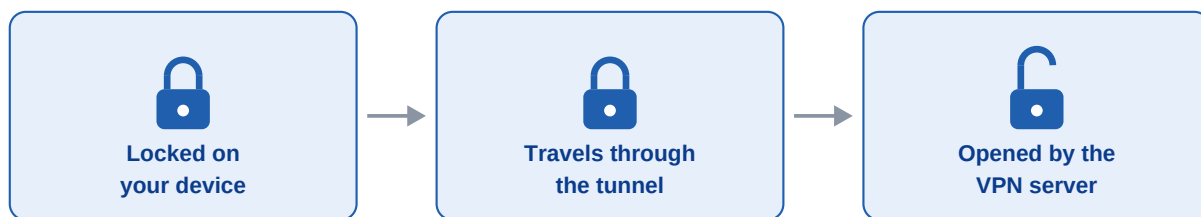
It is worth being clear about what a VPN does not do. It is not a magic shield. It will not stop viruses, and it does not make you completely anonymous. It is one valuable layer of protection among several.

Yes, the VPN server can see the traffic that passes through it, which is why trust matters. A good VPN provider handles this responsibly. The best ones keep no activity logs at all, and others delete their access logs on a daily basis, so there is no lasting record of where you have been or what you did online. This also protects you when outside parties, such as the police or other authorities, ask a provider for a user's browsing history. A provider that stores nothing has nothing to hand over. This is why a clear, independently audited no-logs policy is one of the most important things to look for.

In the chapters ahead, you will learn how VPNs work, how to choose one, and how to use it with confidence.

How a VPN Works

Behind the Scenes



In Chapter 1, you learned that a VPN is a protected tunnel. Now let's look at what actually happens inside it, step by step, in plain language.

It starts with an app on your device, often called the VPN client. When you switch it on, it contacts a VPN server run by your VPN provider, the company you subscribe to for the VPN service. This is not the same as your internet provider, which only connects you to the internet. The two devices introduce themselves and agree on a secret set of digital keys. This handshake is what makes the connection private, because only your device and the VPN server hold those keys.

From then on, everything you send is encrypted before it leaves your device. Imagine locking each message in a box that only the VPN server can open. Your internet provider, the café Wi-Fi, or anyone else along the way sees a stream of locked boxes going to one place, but they cannot see what is inside or which websites the boxes are really meant for. There is one important catch. Today's encryption is extremely strong against normal computers, but once powerful quantum computers are built, they will be able to break the methods used to set up many of today's connections. Data recorded now could even be unlocked years later. This is why, when you choose a VPN, you should look for one that states it is quantum-safe, meaning its encryption is designed so that quantum computers cannot break it either.

When your data arrives at the VPN server, the server unlocks it and passes your request on to the website or device you wanted to reach. That website sees the request coming from the VPN server's IP address, not yours. This is how your real location and identity stay hidden.

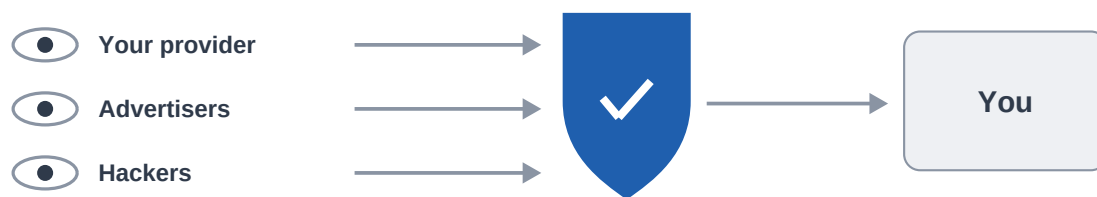
The journey then runs in reverse. The website answers the VPN server, the server locks the reply in a new box, and sends it back through the tunnel to your device, where your VPN app unlocks it. All of this happens in a fraction of a second, so you barely notice it.

The rules for how the tunnel is built and how the locking works are called VPN protocols. Some are faster, some are more secure, and we will compare them in Chapter 6.

The key idea to remember is simple: your device talks to the VPN server in secret, and the VPN server talks to the rest of the internet for you.

Why You Need a VPN

Privacy in a Connected World



Almost everything we do now happens online: banking, shopping, messaging, working, even talking to our doctors. Each of those actions leaves a trail, and many different parties are quietly collecting it.

Start with your internet provider. It carries all your traffic, so it can see which websites you visit and when. In some countries, providers are allowed to use that information for their own purposes, including selling insights about their customers. Then come the websites and apps themselves. Big tech companies track your IP address, your location, and your habits across the web, and they use that profile to decide which ads to show you and sometimes even which prices.

Public networks add another risk. Wi-Fi in cafés, airports and hotels is often shared with strangers and poorly protected. On a weak network, someone nearby may be able to watch your connection or set up a fake hotspot to capture what you send. A VPN encrypts your traffic, so even on a bad network, what an attacker sees is unreadable.

A VPN also helps when you travel. Some services and websites change what they show you, or block you completely, depending on the country you are in. A VPN lets you connect through a server back home, so you can use your usual services as normal.

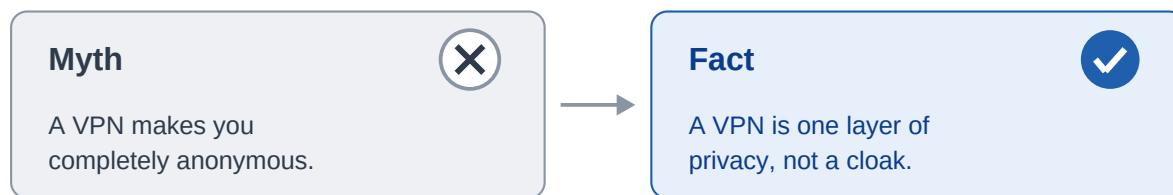
Be aware that some hotels, and some workplaces and schools, block VPNs on their networks, so the VPN simply will not connect over their Wi-Fi. When that happens, do not give up. Switch your phone or device to a different kind of network, such as mobile data over 4G or 5G, or use your phone as a hotspot, and then connect your VPN. Because you are no longer going through the hotel's network, the block does not apply. Many VPN apps also have a stealth or obfuscation mode that disguises VPN traffic as ordinary web traffic, which can get past these blocks too.

There is also a simple matter of principle. Privacy is not about having something to hide. You close the curtains at home and put letters in envelopes, and a VPN is the digital version of that habit.

A VPN will not solve every problem, but it is one of the easiest and most effective steps you can take to get control of your information. In the next chapter, we will clear up the most common myths about what VPNs can and cannot do.

Myths Debunked

10 VPN myths and the facts behind them



VPNs are surrounded by confusion. Some people think they are magic, others think they are only for criminals. Let's clear up the ten most common myths.

- **Myth 1: A VPN makes you completely anonymous.** It does not. A VPN hides your real IP address from websites and encrypts your traffic, but if you log in to your accounts, those sites still know who you are. Cookies and browser fingerprinting can also still identify you. A VPN is one layer of privacy, not an invisibility cloak. For this, we will create a new ebook.
- **Myth 2: A VPN protects you from viruses.** It does not. A VPN protects your connection, not your device. If you download a malicious file, the VPN will not stop it. You still need up-to-date software and sensible habits.
- **Myth 3: VPNs are illegal.** In most countries, using a VPN is perfectly legal, and businesses rely on them every day. A small number of countries restrict or ban them, so check the rules wherever you live or travel. What you do while connected must also stay within the law, just as it would without a VPN.
- **Myth 4: VPNs are only for tech experts.** Today's VPN apps are simple. You install one, tap a button, and you are connected.
- **Myth 5: All VPNs are the same.** They are not. Providers differ widely in speed, security, and honesty. Some keep logs of your activity, and some free ones even make money by selling your data. This is why choosing the right provider matters, as we will see in Chapter 7.
- **Myth 6: A VPN will slow your internet to a crawl.** Encryption does add a small delay, but a good VPN on a modern connection is barely noticeable. In some cases, speeds even improve.
- **Myth 7: Free VPNs are just as good as paid ones.** Running servers around the world costs real money, so a free VPN has to earn it somewhere else. Many do so by showing you ads, limiting your speed and data, or collecting and selling information about what you do online, which is the very thing you were trying to avoid. A few free plans from trusted providers are fine for light use, but as a rule, if you are not paying for the product, your data may be the price.
- **Myth 8: You only need a VPN if you have something to hide.** Privacy is not the same as secrecy. You close your curtains at home and seal your letters in envelopes, not because you are doing anything wrong, but because some things are nobody else's business. A VPN also protects ordinary people on public Wi-Fi, while travelling, and from companies that track them for profit.
- **Myth 9: A VPN is only for computers.** Your phone and tablet are just as exposed, and often more so, because they hop between networks all day. Most VPN providers offer apps for phones and tablets, and many let you protect several devices, and even your router, with a single subscription.
- **Myth 10: The VPN with the most servers or the loudest advertising is the best.** Big numbers and big promises are marketing, not proof. What matters is a clear, independently audited no-logs policy, strong

encryption, good speeds, and a company you can trust. We will go through exactly what to look for in Chapter 7.

The truth is simple. A VPN is a useful, legal tool that does a specific job well, as long as you understand what that job is. In the next chapter, we will look at the different types of VPNs.

Myths at a glance

Myth	The fact
A VPN makes you anonymous	It is one layer of privacy, not an invisibility cloak
A VPN stops viruses	It protects your connection, not your device
VPNs are illegal	Legal in most countries, but check local rules
VPNs are for experts only	Today's apps connect with one tap
All VPNs are the same	Speed, security and honesty vary widely
A VPN slows you to a crawl	A good one is barely noticeable
Free VPNs are just as good	Free often means your data is the price
Only needed if you have something to hide	Privacy is not the same as secrecy
VPNs are only for computers	Phones and tablets need one too
The most servers is the best	Audits, encryption and trust matter more

Types of VPNs

Personal, Business, Remote Access and Site-to-Site



Not every VPN does the same job. The tunnel idea is always the same, but what sits at each end of it changes. Here are the four main types.

- **Personal VPN.** This is the kind most people know. You subscribe to a VPN provider, install an app on your device, and connect to one of the provider's servers. Your traffic is encrypted, your real IP address is hidden, and you can appear to be in another country. It is the right choice for privacy, public Wi-Fi, and travel.
- **Business VPN.** Companies use VPNs to protect their staff and their data. Instead of connecting to a public provider's servers, employees connect to servers the company controls, or to a business service built for teams. This keeps company information private, and it lets the company decide who gets access to what.
- **Remote access VPN.** This type connects you to a private network from somewhere else. Imagine you are away from home and need a file from your computer, or you are working from a café and need to reach the office network. The VPN lets you reach those computers as if you were sitting right next to them, and, as I mentioned in Chapter 1, without opening any ports on the router. We will build one together later in this book.
- **Site-to-site VPN.** This one connects two whole networks to each other, not just one person to a network. A company with offices in two cities can join their networks so that computers in both places can talk to each other securely, as if they were in the same building. Once set up, it runs quietly in the background, and nobody has to switch anything on.

Which one is right for you? If your goal is privacy online, choose a personal VPN. If you want to reach your own computers from outside, you need a remote access setup. Businesses often use the last two. In the next chapter, we will look at the technical rules that make all of these work, called VPN protocols.

VPN Protocols Explained

OpenVPN, WireGuard, IKEv2 and More



A VPN protocol is the set of rules your device and the VPN server follow to build the tunnel and lock your data inside it. Different protocols make different trade-offs between speed, security, and compatibility. Here are the ones you will meet most often.

- **WireGuard.** The newest of the popular protocols, and the one many providers now recommend. It is very fast, uses modern encryption, and its code is small, which makes it easier to check for flaws. It is a great default choice.
- **OpenVPN.** The long-time favourite. It has been tested by experts for many years and works on almost every device. It is also flexible: it can run in a way that looks like ordinary secure web traffic, which helps it get past networks that block VPNs, like the hotels from Chapter 3. It is usually a little slower than WireGuard.
- **IKEv2/IPsec.** A strong choice for phones and tablets. It reconnects very quickly when you switch between Wi-Fi and mobile data, so your protection does not drop as you move around.
- **L2TP/IPsec.** An older protocol that is still found in some places. It is secure enough, but slower and less capable than the newer options, so use it only if nothing better is available.
- **PPTP.** The oldest of all, and now considered broken. Avoid it entirely.

Many providers also offer their own custom protocols, often built on top of WireGuard, along with stealth modes that disguise your VPN traffic.

Remember the quantum computing warning from Chapter 2. Protocols are exactly where this protection is added. Some providers now add quantum-safe key exchange to their protocols, so look for that when you choose.

As a simple rule, pick WireGuard first, OpenVPN when you need to get past a block, and IKEv2 on a phone that moves around a lot. In the next chapter, we will look at how to choose the right VPN provider.

Choosing the Right VPN Provider

- ✓ No-logs policy
- ✓ Strong encryption
- ✓ Independent audit
- ✓ Good speed

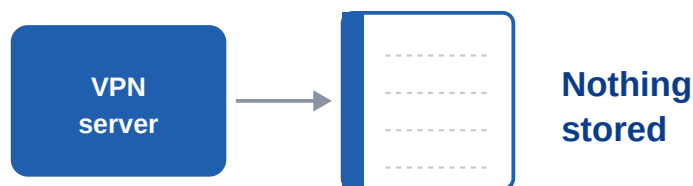
Choosing a VPN provider is really a question of trust. As you learned in Chapter 1, the VPN server can see the traffic that passes through it, so the company behind it matters as much as the technology. Here is what to look for.

- **A clear no-logs policy, independently audited.** The provider should state plainly that it does not keep records of your activity, and it should have had that claim checked by an outside auditor. Anyone can write "no logs" on a website, so proof matters. We cover this in depth in Chapter 8.
- **Strong, modern encryption.** Look for up-to-date protocols such as WireGuard and OpenVPN, as explained in Chapter 6. Ideally, the provider also says its encryption is quantum-safe, so your data stays protected in the years ahead.
- **The right features for you.** A kill switch cuts your internet if the VPN drops, so nothing leaks. A stealth mode helps you connect from hotels and other places that block VPNs. Apps for all your devices, and the ability to protect several at once, are also worth having.
- **Good speed and a wide choice of servers.** More servers does not automatically mean better, as we saw in Chapter 4, but you do want servers in the countries you need, and fast, stable connections.
- **An honest business model.** If the VPN is free, ask how it makes money. A reputable provider earns its income from subscriptions, not from selling your data.
- **Transparency and support.** Good providers explain who owns them, where they are based, and how they handle legal requests. They should also offer helpful support and a money-back guarantee, so you can try the service without risk.

Before you commit, take advantage of that guarantee. Test the speed, try the apps on your devices, and check that the features work. In the next chapter, we will look more closely at no-logs policies and why the country a provider is based in matters.

No-Logs Policies

Jurisdictions and Trust



Every VPN asks you to trust it with your traffic. This chapter explains the two things that decide whether that trust is deserved: what the provider records, and which country's laws it has to obey.

- **What "no logs" really means.** There are two kinds of records. Activity logs show what you did, such as the sites you visited. Connection logs show that you connected, such as when and from where. The best providers keep neither. Others keep minimal connection data and delete it quickly, for example on a daily basis, as mentioned in Chapter 1. What matters is that nothing is kept that could be tied back to you.
- **Proof, not promises.** Anyone can claim "no logs". Look for an independent audit, where an outside firm inspects the provider's systems and publishes its findings. Another strong sign is servers that run only on RAM, meaning the memory is wiped every time a server restarts, so data cannot be stored for long even if someone wanted to. Real-world cases also count: some providers have had servers seized by authorities and had nothing useful to hand over.
- **Why jurisdiction matters.** A VPN company must follow the laws of the country where it is based. Some countries force companies to keep records or hand over data when asked. Others have strong privacy laws and no such requirements. You may hear about the Five Eyes, an intelligence-sharing alliance between the United States, United Kingdom, Canada, Australia and New Zealand. Many people prefer providers based outside these countries, in places with strong privacy protections.
- **Be realistic.** Jurisdiction is not everything. A provider in a privacy-friendly country can still be dishonest, and one in a strict country can still be audited and trustworthy. Weigh the policy, the proof, and the location together.

If a provider keeps nothing, it has nothing to hand over, which is the protection we want. In the next chapter, we will get practical and set up a VPN on your computer, phone and tablet.

Setting Up a VPN

on Your Computer, Phone and Tablet



Setting up a VPN is easier than most people expect. The steps are almost the same on every device, and it usually takes only a few minutes.

- **Step 1: Sign up with your chosen provider.** Use the checklist from Chapter 7, create an account, and pick a plan. Take advantage of the money-back guarantee so you can test it risk-free.
- **Step 2: Download the official app.** Get it from the provider's own website or your device's app store, whether that is the Google Play Store, the Apple App Store, or the Microsoft or Mac store. Apps exist for Windows, Mac, Android, iPhone, iPad and more. Be careful to install the real one, because fake VPN apps do exist.
- **Step 3: Log in and allow the connection.** The first time you connect, your phone or tablet will ask permission to set up a VPN connection. This is normal. Approve it, and the app can build the tunnel.
- **Step 4: Choose your settings.** Most apps work well out of the box, but it is worth checking a few things. Pick a protocol, with WireGuard as a good default from Chapter 6. Turn on the kill switch so your internet cuts off if the VPN drops. Enable the option to connect automatically, so you are protected without having to think about it.
- **Step 5: Connect and check.** Tap the connect button, and choose a nearby server for the best speed, or a server in another country if you need one. To confirm it works, search "what is my IP" in your browser. The address and location should now be the VPN server's, not yours.
- **Tips for success.** Install the VPN on every device you use, and keep the app updated. If it will not connect on a hotel network, try the fixes from Chapter 3, such as stealth mode or mobile data.

In the next chapter, we will look at how to use a VPN in real life.

VPN	Where to sign up
Proton VPN *	<i>(your Proton link here)</i>
NordVPN *	<i>(your NordVPN link here)</i>
Surfshark *	<i>(your Surfshark link here)</i>
Others	ExpressVPN, Mullvad, IVPN, CyberGhost, Private Internet Access, Windscribe, TunnelBear, PureVPN, IPVanish, Hotspot Shield. For self-hosting: WireGuard, OpenVPN, Tailscale.

* If you sign up through these links, I earn a commission. If you would rather not, you can search for the VPN's name on Google and sign up directly, and I will not earn anything. The choice is yours.

Using a VPN in Real Life

Streaming, Gaming, Travel, Wi-Fi, Troubleshooting and the Future



You now know what a VPN is and how to choose and set one up. This final chapter covers how to use it well in everyday life.

- **Streaming.** Services show different libraries in different countries. Connect to a server in another country, or back home when you travel, to see that library. Streaming companies try to block VPN servers, so if one fails, switch servers or ask your provider's support which ones work. Check the service's terms of use, since some do not allow VPNs.
- **Gaming.** A VPN rarely makes games faster, but it hides your IP address from other players, protecting you from attacks that knock you offline. Extra steps add delay, so choose a nearby server, use WireGuard, and turn the VPN off when speed matters most.
- **Travel.** Connect to a home server to use your banking, streaming and work accounts as normal. Install and test the VPN before you leave, because some countries block VPN downloads. If a hotel blocks it, use stealth mode or mobile data. Check local laws, since a few countries restrict VPNs.
- **Public Wi-Fi.** Cafés, airports and hotels are shared with strangers, and attackers can set up fake hotspots with believable names. Turn the VPN on before opening any apps, confirm the network name with staff, prefer https sites, turn off automatic Wi-Fi joining, and forget the network when you leave. For banking, mobile data is safer still.
- **Troubleshooting.** If it is slow, test your speed without the VPN, connect to a closer server, switch to WireGuard, and restart the app. If it will not connect, try another server or protocol, update the app, use stealth mode, and check your device's clock. If a site will not work, switch servers or use split tunneling. If it keeps dropping, try IKEv2. If nothing works, contact support.
- **Advanced features.** The kill switch cuts your internet if the VPN drops, so your real IP never leaks, and you should always turn it on. Split tunneling lets you choose which apps use the VPN, but anything outside the tunnel is unprotected. Multi-hop sends traffic through two servers for extra privacy, at the cost of speed.
- **Free, paid and self-hosted.** Free VPNs often rely on ads, limits or sold data, so never trust an unknown free app. Paid providers are funded by subscriptions and are more accountable, but still check the policy and audits. A self-hosted VPN lets you hold the keys and reach your home network from anywhere without opening ports, though it takes setup and does not hide your identity like shared servers. Many people use both.
- **The future.** Expect quantum-safe encryption to become standard, along with faster protocols, smarter blocking and changing laws. Big tech tracking is also growing beyond IP addresses, and a VPN alone does not make you anonymous. Real privacy comes from a trustworthy VPN plus good habits and awareness.

Take back control, one smart choice at a time, and keep pushing back against big tech.