How to Set Up and Use a VPN

There's more to setting up a virtual private network than just signing up and activating the service. Our guide can help you get the most from this critical privacy and security tool.

By Max Eddy May 9, 2018 10:40AM EST

Everyone should be using a virtual private network or VPN, whether you're connecting to the Internet on your computer or your smartphone. That may sound paranoid, but there are real threats out there, and they're only getting worse. On Wi-Fi networks, unscrupulous individuals can attempt to intercept your information. And whenever you connect to the internet, your Internet Service Provider (ISP) has access to everything you send and has been given the green light from Congress to sell your anonymized information to advertisers, too. Out on the wide open internet, advertisers and spies can track your movements between websites and discern your location by peeking at your IP address. It's scary out there.

The fact is the internet was not designed to protect your privacy. It was created for easy information exchange, not user privacy, anonymization, or encrypted communication. While HTTPS goes a long way toward protecting your information, it doesn't guard against ISP snooping or local network attacks—a major problem if you ever use a connection that isn't yours, such as one at a hotel or a coffee shop.

So until a new, more private internet comes together (probably never), using a VPN is the easiest way to make sure that you're sharing as little information as possible. Make no mistake: You need a VPN.

What a VPN Does and Does Not Do

As with any security tool, it's important to understand the limitations of a VPN. After all, you wouldn't expect a kevlar vest to save you from falling out of an airplane or a parachute to stop a bullet.

When you switch on a VPN, your traffic is routed through an encrypted tunnel to a server operated by the VPN company. That means that your ISP and anything (or anyone) connected to your router won't be able to see your web traffic. From the VPN server, your traffic exits onto the public internet. Unless you're headed to a site that uses HTTPS, your traffic is no longer encrypted.

Because your traffic appears to come from the VPN's server, your actual IP address is effectively hidden. That's important, because IP addresses are distributed geographically and can be used to infer someone's location. If someone checks your IP address, they'll see the IP address of the VPN server. This can come in handy if you want to spoof your location. By connecting to a VPN server in London, you can make it appear as if you are accessing the internet from the UK.

What a VPN won't do is completely anonymize your traffic. To do that, you'll want to use a service such as Tor. This excellent anonymization service is easily accessed through a special version of the Firefox browser. Instead of just piping your data through a single intermediary (that is, a VPN server) Tor bounces your data through several different

volunteer computers. This makes it much harder for someone trying to track your activities to see what you're up to.

Additionally, websites can track your movements through cookies, browser fingerprinting, online trackers, and other tricky tools. Using an ad-blocker such as Privacy Badger helps suppress these ever watchful nasties and can make it much harder for advertisers to follow your movements across the web.

Finally, just because you have a VPN doesn't mean you can forget about the security basics. While some VPN services claim they can block malware, we recommend standalone antivirus software for your computer, because these tools are designed specifically to protect your computer from malicious software. You should also use a password manager, because recycled passwords are a major point of failure. Another precaution is to use common sense when clicking on links or opening email attachments. Phishing attacks—when an attacker uses a bogus website that mimics a familiar one to trick you into entering your login credentials—are so common as to almost be mundane, so stay alert.

How to Choose a VPN

When we review VPNs, there are a few key metrics we look for. One is that the VPN service should allow you to connect at least five devices at a time. Another is whether or not the VPN service allows BitTorrent traffic on their servers. Some do, some do not, and you don't want to run afoul of the company you're paying a monthly fee to.

Speaking of fees, the average cost of a VPN service is $10.53 per month. A VPN service that is charging more per month isn't necessarily ripping you off, but it should offer something significant, such as a great interface or lots of server locations to sweeten the deal. You can usually get a discount if you buy longer-term contracts, but we recommend avoiding those until you're certain that you're happy with the service.

Before you sign up with a VPN, be sure to read its terms of service. This document will outline what information the VPN collects and what it does with that information. Most companies say that they don't log traffic, which is great. Others go further, saying that they do not monitor user activity at all. This is important,because a VPN has access to all the information you're trying to protect from others. The best terms of service make all these issues clear, while the worst are opaque on the details and written in legalese. If reading one of these documents feels like you're trying to translate the Dead Sea Scrolls, consider trying another service. TunnelBear, for example, clearly outlines its operation in easy-to-understand language.

It's also useful to see where the VPN company is based. Keep in mind that this isn't always the physical location of the business, but a legal distinction that outlines what jurisdiction the company operates under. NordVPN, for example, is in Panama, while ProtonVPN is in Switzerland. That means that these companies are not beholden to data retention laws, which would require them to hold on to certain information that could be obtained by law enforcement. Hide My Ass VPN, on the other hand, is based in the UK, which has more intrusive laws.

The most important thing about a VPN is trust. If the location, pricing, or terms of service don't fill you with confidence, try another service.

Free or Paid VPNs?

We at PCMag recently conducted a survey of 1,000 people, asking questions about VPN use. According to our results, 62.9 percent said they didn't want to pay more than $5, and 47.1 percent said they want to use a free VPN.

Unfortunately, most VPNs are a far cry from free. Or even from $5. But you don't need to break the bank to get protected. If after trying out a service for a month or two, you can save more by purchasing longer-term contracts. Private Internet Access is an excellent and affordable service that costs just $6.95 per month for an albeit no-frills experience.

Many VPN services offer a free trial, but usually for a limited time. Others, like TunnelBear and AnchorFree Hotspot Shield Elite, have totally free versions but may limit some features to paid users. TunnelBear, for example, has a data allowance for free users. Hotspot Shield, on the other hand, has an ad-supported free version. ProtonVPN, from the creators of the secure email service ProtonMail, has a limited free version of its VPN, too.

The browser Opera has a free VPN baked in,and charges nothing for its use. Opera separately offers excellent VPN apps for Android and iOS, also completely free, extending protection to wherever you go.

Getting Started

Once you've settled on a service, the first thing to do is to download the company's app. There's usually a downloads page for this on the VPN service's website. Go ahead and download the apps for your mobile devices as well; you'll want to protect as many of your devices as you can. Generally, you pay one subscription fee for a certain number of licenses (usually five) and then you can use the service on any device for which it provides apps.

We have found that when releasing VPNs for Mac, companies occasionally have different versions available in the Mac App Store and on the company website. This appears to be in order to comply with Apple's restrictions. Figuring out which will work for you can be tricky, but we've broken down the differences in our reviews.

Once you've installed the apps, you're prompted to enter your login information. In most cases, this is the username and password you created when you signed up for the service. Some companies, such as Private Internet Access assign you a username that's different from your billing credentials, in order to provide customers with more privacy.

Once you're logged in, your VPN app usually connects to the VPN server closest to your current location. That's done to provide better speeds with a VPN, as latency and speed reductions increase the farther the VPN server is from your actual location. That's it: Your information is now being securely tunneled to the VPN server.

Note that you do not *have* to install the VPN company's app. Instead, you can configure your device's network settings to connect directly to the VPN service. If you're concerned about the potential for surveillance within app ecosystems, this might be a good option for you. Most VPN services will have documentation on how to configure your device.

Choosing a Server

Sometimes you might not want to be connected to the server the VPN app recommends. Perhaps you want to spoof your location, use BitTorrent via VPN, or you want to take advantage of some of the custom servers your VPN company has provided.

Many VPN companies include an interactive map as part of their app. NordVPN, for example, lets you click on countries to connect to those servers. It's a useful way to understand where your information is going, but there's probably a list of servers you can select from.

Choosing a server depends entirely on what you want to accomplish. For security and speed, you should choose a server that's close by. To access region-locked content, you'll want a server that's local to content you want to watch. If you're trying to watch the BBC, you'll want to tunnel to the UK. Some VPN companies, such as KeepSolid VPN Unlimited and NordVPN, have specialized servers for streaming video.

These specialized servers are useful because streaming services such as Netflix block VPNs. At issue are the licensing deals Netflix secures with studios. For example, Netflix has the rights to provide *Star Trek: Discovery* outside the US, but within the US you need to pay for CBS's All Access service.

It's also a good idea to check and see whether your VPN service allows BitTorrent traffic on any server, or just specific ones. NordVPN clearly marks the servers cleared for torrenting, and others do the same. TorGuard, on the other hand, is all about torrenting and allows its use on all the company's servers.

Other services like NordVPN and ProtonVPN have enhanced security options, such as access to Tor or multihop VPNs. Tor, as mentioned above, is a way to better protect your privacy, and lets you access hidden websites on the so-called Dark Web. Multihop VPN is similar: Instead of just routing your traffic through a single VPN server, a multihop connection tunnels you to one server and then another. Both of these offerings trade speed for enhanced privacy.

If you've opted to ignore first-party apps and configure your network settings manually, you will probably have to enter the information for each VPN server individually.

Advanced Settings

The set of features in each VPN varies from service to service, so we can only generalize about what you may see when you open the Settings pane. But we encourage you to read through the documentation and try clicking some buttons. The best way to learn how to use a tool is to try, after all.

Most VPN services include some kind of Kill-Switch feature. Once engaged, this option prevents your computer from transmitting or receiving information over the internet unless the VPN is engaged. It's useful for when your computer disconnects from the VPN, and it can prevent little bits of data sneaking through unencrypted.

Most services offer an option to select a VPN protocol. This can be intimidating, since they have weird names and companies rarely provide information about what these are, and what changing the protocol will do. In general, this is something you can leave alone.

But if you're interested, the protocol we recommend is OpenVPN. It's open-source, so it has been picked over by many eyes for any potential vulnerabilities. IKEv2 is also a good, secure option if OpenVPN is not available. Note that on some platforms, such as macOS and iPhone, OpenVPN is not always available, because of additional restrictions placed on developers. The best VPNS for iPhone give you access to the latest and greatest protocols available on that platform.

When Should I Use a VPN?

For the best security, you should use a VPN as often as possible and, ideally, all the time. But that's an ideal, and it's not always achievable. At minimum, you should use a VPN whenever you're using a network that's not one you control, and especially if it's a public Wi-Fi network. But in general we recommend that users set the default on their VPN apps to be connected as much as possible. You can always disconnect if it's causing a problem.

VPNs for Android and other mobile devices are a little trickier, particularly if you frequently move in and out of cellphone coverage. Each time you lose and regain data connectivity, the VPN has to reconnect, which adds a frustrating wait. It's also just less likely that your cell traffic can be intercepted, but we've seen researchers prove that it can be done. And considering that law enforcement and intelligence agencies have effectively unfettered access to telecom data, it's a good idea to use a VPN even over cellular connections. Also, most mobile devices can automatically connect to any familiar looking Wi-Fi network. At minimum, you should use a VPN when connecting via Wi-Fi, especially because it's trivially simple to impersonate a Wi-Fi network.

Many VPNs have settings for how and under what circumstances they should reconnect if they become disrupted. We honestly cannot think of a reason you wouldn't want your VPN to try reconnecting and encourage everyone to make sure their settings reflect this.

If you're concerned about VPNs slowing your connections or blocking important traffic, you should take a look at split-tunneling options. Again, different companies give this feature different names, but the gist is that you can decide which apps will use the VPN for their traffic and which apps can transmit without the VPN. TunnelBear, for example, includes an option to not tunnel any Apple apps to ensure they function properly on a Mac. Frequent video streamers and gamers in need of a VPN may want to look into this as an option.

How to Use a VPN For Streaming With Chromecast or AirPlay

Chromecast and AirPlay let you share music and video from your computer or mobile device to speakers, TVs, and streaming boxes. But all of them require Wi-Fi, which can be a problem when you're using a VPN.

When a VPN is engaged, your traffic is moving through an encrypted tunnel, which prevents the devices from finding each other on the same Wi-Fi network. That's as it should be, since you don't want someone snooping around a network to see what you're

up to. Sadly, it also means that Chromecast and AirPlay won't work when you have a VPN active.

The simplest solution is to switch off your VPN, but that's not your only option. You can use split-tunneling, as mentioned above, to route only the traffic you want secured through the VPN. You can use a VPN browser plugin, which only encrypts your browser traffic and nothing else.

Alternatively, you can install a VPN on your router. Doing so means that all the devices connected to your router—from your phone to your smart juicer—will have their traffic encrypted. That's a great option for a heavily wired smart home.

VPNs Aren't Rocket Science

Too many of you aren't using a VPN, and maybe that's because they seem like arcane security tools. But many companies have worked hard to make them friendly and easy to use. Most are now set-and-forget security tools, as it should be. And though opening your wallet to guard against potential threats is always annoying, buying a VPN is one of the best and easiest ways to guard your web traffic from, well, just about everyone.