DDF VPN Guide: What is a VPN? How Do I Choose a VPN?

Contents

What's a VPN?

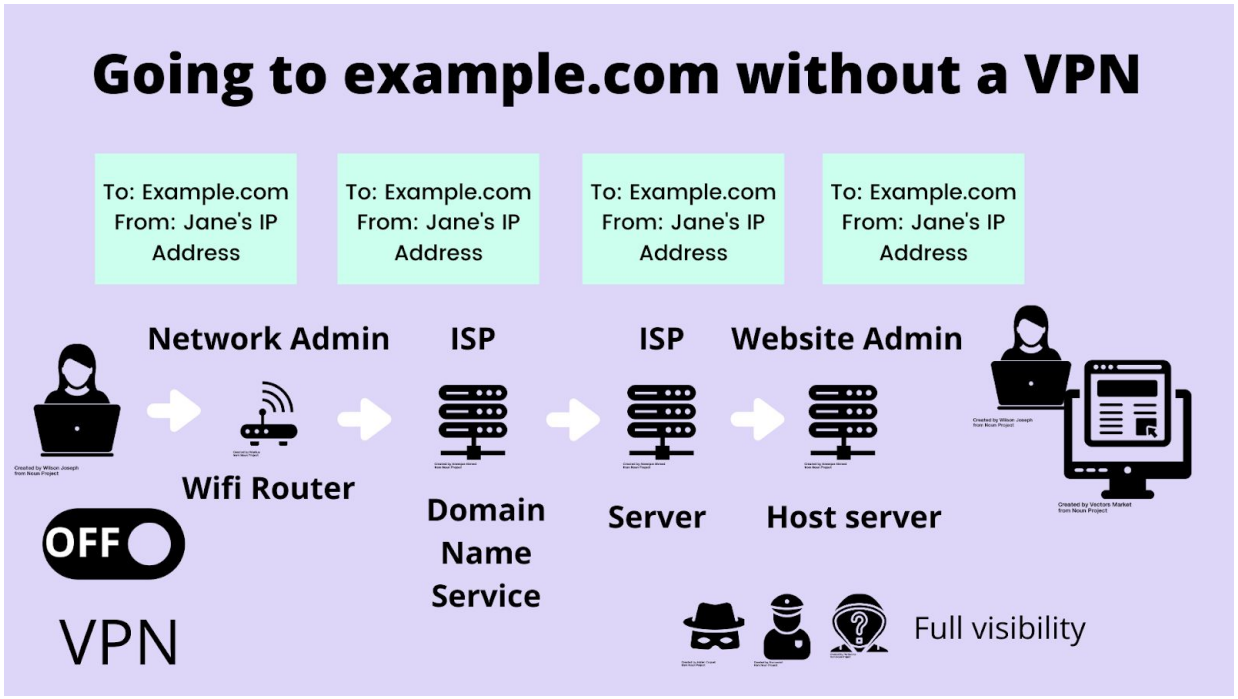
A Virtual Private Network (VPN) is a way of connecting to the internet that helps protect your privacy and security. VPNs encrypt all your communications with the internet, and hide your IP address from the websites you are visiting. Using a high-quality VPN is a user-friendly way to protect your privacy online. First we'll explain how they work, and then we'll talk about troubleshooting.

How Does a VPN Protect Your Privacy?

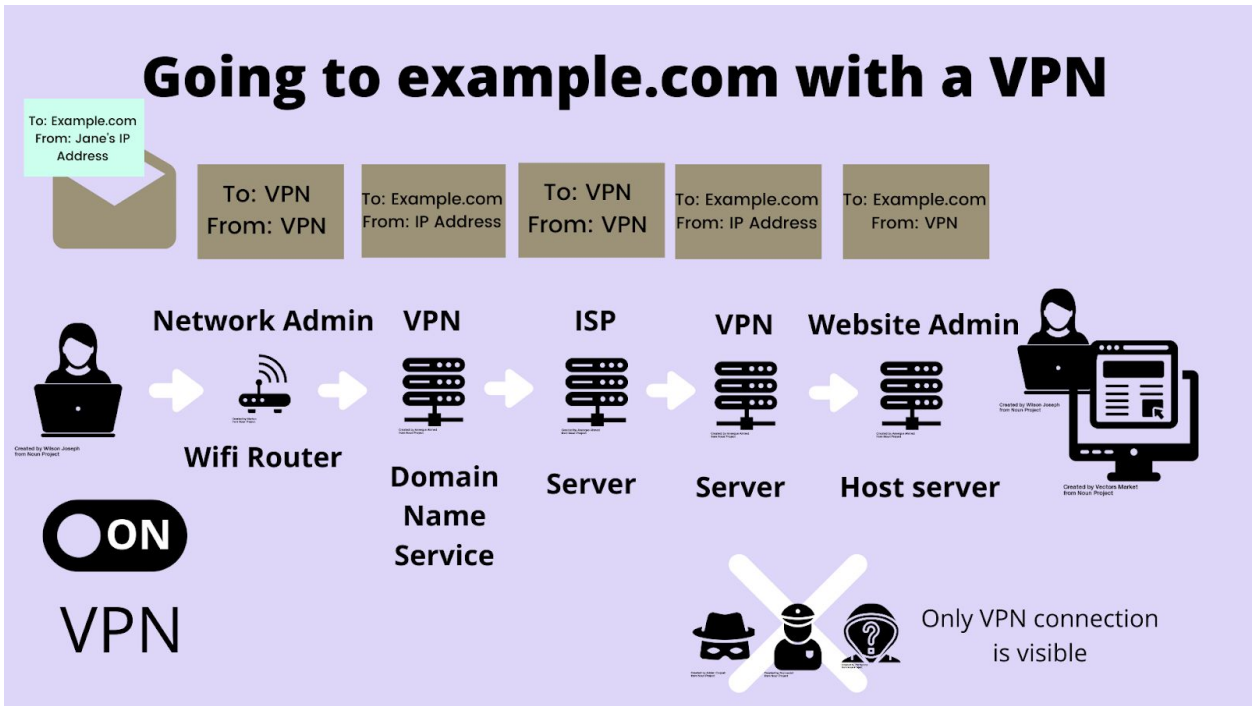
Using a VPN changes how you connect to the internet in a couple of ways. Your user experience hardly changes, making VPNs a very user-friendly way to protect your security.

Anytime you log onto the internet, your device is identified with an Internet Protocol (IP) address. You can see your IP address here (tool provided by Tunnelbear) or here (tool provided by Private Internet Access).

When you type a website's URL into your browser, a request is sent to a domain name system (DNS) that translates the words, like www.example.com, into a numerical IP address. The router for the WiFi network you're connected to processes this request and stores a copy. Without a VPN, the website's URL is translated by a DNS server owned by your internet service provider (ISP). While some browsers and DNS hosts encrypt your requests, many DNS requests are in plaintext, which means someone snooping on your connection could see which websites you're visiting. Your ISP stores a record of your requests as well, and it's suspected that some ISPs sell these records for advertising purposes. ISPs will also provide these records to law enforcement if they receive a valid legal request.



When you use a VPN, your traffic takes a different route through the internet.



digital defense fund

When you use a VPN, the VPN will replace your IP address with theirs, and the WiFi router will just see that you're connecting to a VPN. You have the option to route your request through the VPN's DNS servers instead. Your internet service provider just sees your connection to the VPN, not what website you are going to. Then, your request goes to the VPN's servers, which then sends it on to the destination. Instead of seeing your IP address, the website just sees the VPN's IP address. Your information is also encrypted throughout the process.

A VPN is like a tunnel that lets your traffic go from your computer to the website without anyone else being able to tell what's inside. The only entity that can see the full picture of what you're doing online is the VPN.

Some VPNs, especially free ones, keep records of your traffic just like your ISP does. These VPNs respond to law enforcement with those records, and many also sell your data so they can make money. (If the service is free, then you're generally the product the company is selling!)

Other VPNs are privacy advocates, who don't keep records (or logs) of your traffic. Known as no-logs VPNs, these companies do have to respond to legal requests for data, but they have no data to give.

This makes choosing a VPN that guarantees your privacy key. "VPNs are essentially a way of moving your trust," says Jacob Hoffman-Andrews, senior staff technologist at the Electronic Frontier Foundation (EFF), in this article on Verge.com. Instead of trusting your internet service provider, your public or private wifi, and the websites you visit to keep your data private, you trust the VPN instead. Transferring trust to a VPN is a decision more and more people are making, especially with the de-regulation of internet service providers. You can scroll down for our advice on choosing a VPN!

It's very important to note that a VPN does not make you anonymous or prevent all tracking. Depending on what browser (Chrome, Safari, Firefox, etc.) you are using, you'll still be creating a browser history that you'll have to clear yourself. Websites can still use cookies to track you. And you can still enter identifying information into a webform! A VPN is a great privacy tool, and is even better when used in harmony with general privacy and security hygiene.

Why use a VPN?

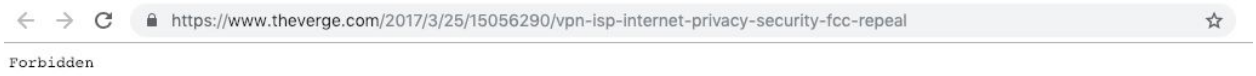
While you use the internet for work, fun, research, and whatever else you use it for, your internet service provider, wifi networks, and websites that you visit are all tracking you. That means they are collecting your data, and most likely, they are going to sell it. A VPN keeps your online activity private while you're browsing, and a good VPN doesn't keep any records of where you went online or what you did.

How a VPN Changes Your User Experience

When you first start using a VPN, you may notice a few differences in your experience online. First, you can check that the VPN is working by going back to here (tool provided by Tunnelbear) or here (tool provided by Private Internet Access).

Then: Get used to seeing CAPTCHAs. A lot of CAPTCHAs. Most forms online determine whether or not you're a bot based on your IP address, and because there are many other people out there using your same VPN's IP address, websites that use anti-spam technology like CAPTCHA will flag you as suspicious.

Usually, solving the CAPTCHA will solve the problem and you'll be able to browse the site as normal. Other times, you'll run into some barriers. For example, while looking up the TheVerge.com article about VPNs that I linked to earlier in this post, ironically TheVerge.com blocked me when I was using my VPN. When that happens, you'll get a message like this:



Because I wasn't too concerned with the privacy of any of my other tabs at that moment, I just toggled off my VPN to load the site, and turned it back on after. If there was activity in other tabs that I didn't want to make vulnerable or to be tracked by my ISP, I could have tried using a different server by opening my VPN settings, or I could have closed everything, cleared my history, and started a new browser session before turning off my VPN.

Other times, your Internet experience may be unimpeded, but you might run into problems later. Some Sales Audit departments will flag purchases made while you were using a VPN. This has only happened once or twice in my personal experience, but it's something to consider. Before turning off your VPN when you're on an online store, make sure that the vendor website has its own encryption (look for the https & the lock symbol in the URL - and for good measure, install HTTPS Everywhere!).

If you're an abortion access organization and you have questions about whether a VPN is right for you, your staff, or your volunteers, head on over to the contact page and send us a note!

How Should I Choose a VPN?

When you use a virtual private network (VPN), you are transferring your trust to keep your online activity private from your internet service provider to the VPN vendor. Because you're trusting this service with your privacy, choosing a trustworthy provider is very important.

If you're not sure what a VPN does, scroll back up to the "What's a VPN?" section of this guide first.

Our first tip in choosing a VPN is to **use a paid VPN**. If someone is offering a free product, the real product for that company is your data!

Beyond that, check the VPN's privacy policy to make sure they keep no logs of your internet activity. Most of the serious VPN providers will promise not to log. When I was choosing my VPN, reading through their privacy policies and checking the validity of their no logging promises was my top criteria for making my decision.

How can I know a VPN doesn't keep logs?

How do you know that they really aren't logging your activity, though? Because VPNs aren't strictly regulated and don't have oversight from anyone else, there are very few ways to ensure that a VPN is actually honoring their no logs promise. As discussed in this article, though, you can do some due diligence to investigate a VPN's no-logging promise by checking if the VPN has:

- An **independent audit**: a cybersecurity or accounting company examines the VPN's servers, interviews employees, and inspects relevant aspects of the VPN company to verify the no logging policy.
- **Past responses to legal requests**: companies are required to respond to subpoenas to the fullest extent, so when VPNs are unable to provide data logs in response to a court subpoena, it's considered evidence that they do not keep logs.
- **Past server seizures**: sometimes authorities seize a VPN's server as part of an investigation and search it for any relevant data; if they find nothing, it's considered evidence that the VPN company does not keep logs.

Looking at an audit and past legal experience can help you understand how a VPN might respond in a given legal situation.

Even with a no logging policy, though, it's important to note that using a VPN does not make you anonymous. All VPNs have to keep track of certain data, like your account information and connection start and stop time, for at least a limited amount of time. They have to have a way to make sure only paying customers connect to their servers! In addition, your browsing leaves traces in other places: your browser history, accounts you're logged into, and information you submit while online. You can still be vulnerable to tracking; your device still has a unique

fingerprint, made up of data like what browser you are using. You can learn more about your device's fingerprint with EFF's Panopticlick tool.

What else should I consider?

VPN providers differ in other metrics besides their no-logging policies, which you may want to take into consideration.

You'll want to make sure that the VPN is compatible with your devices - all major VPNs will have web apps for Mac & Windows, as well as apps for iOS and Android.

VPNs route your internet activity through their own servers, but not all VPNs own the servers they use. If a VPN is renting servers, they have less control over the security of those servers - and the human errors of the employees who work there. For this reason, some people look for a VPN that owns all of its servers. Ultimately, I chose not to include it in my chart and I did not choose a VPN that owns all their servers, because I felt that as long as they had enough control over their rented servers to make sure they weren't logging, that was good enough for me.

I did, however, take into consideration the number and location of servers. Using a VPN can slow down your connection, because of the extra steps your data is taking, and I knew that I wouldn't turn it on as much if I actually noticed that lag. (This is why I don't just use Tor all the time!) When a VPN has more servers, its traffic can be spread out, so you're less likely to be slowed down by overcrowding. Another benefit of having more servers in more locations is that you can choose a server that is physically closer to you, which also improves your connection speed. Some people also use different server locations to spoof their location; in fact, I first downloaded a VPN when I was trying to watch Netflix while studying abroad, before I was concerned about privacy. However, Netflix and other sites with country-specific content have gotten savvy and now blacklist known VPN IP addresses, so if you're hoping to use a VPN for streaming Netflix, you'll have to search a little harder.

VPNs also differ in the protocols that they run. The protocol is like the map that tells your data where and how to go through the VPN. Some protocols emphasize privacy, whereas others emphasize speed, for example. This article offers a good summary of the major VPN protocols, copied here:

- **Wireguard:** The newest VPN protocol, Wireguard is open source, offers a range of encryption options, and is optimized for mobile devices
- **OpenVPN:** Open source, offers strongest encryption, suitable for all activities
- **IPSec:** Widely used protocol, good speeds, but more easily blocked
- **IKEv2**: Often paired with IPSec; optimized for mobile
- **SSTP**: Good security, difficult to block and detect
- **PPTP**: Fast, widely supported, but full of security holes, only use for streaming and *basic* web browsing

I really value open source code like Wireguard and OpenVPN - this allows anyone to audit the code and see for themselves if it works the way that the creators say it does, giving you as the user some external confirmation and transparency. I can't audit it myself, but I know there is a huge community of security-obsessed software engineers and other coders who do check it. As our world becomes increasingly privatized and monetized, I also value the ethics of open source since I see the internet as a public good.

Different protocols have different encryption standards as well, which means how thoroughly your data is scrambled and what kind of key unlocks it. The most common kind of encryption is Advanced Encryption Standard (AES), an encryption standard developed by two Belgian cryptographers in response to a contest by the US government to find a new, more secure encryption process in 2000. For AES, the key to unscramble your data is most commonly 128 or 256 pieces of information long (128- or 256-"bit").

The larger the key, the harder it is to crack. As Wired.com explains, "Let's say a hacker has a computer that can test a billion keys per second, trying to brute force all combinations. That means they can break a 30-bit key in just one second. At that speed, though, it will take you a billion seconds (or 34 years) to break a 60-bit key because every 30 bits added makes it a billion times more difficult. A spy agency like the NSA can crack 60-bit keys using supercomputers, but a 90-bit key is a billion times more difficult to crack, and a 120-bit key would be a further billion times more difficult to crack than that." As far as we know, AES 256 has never been cracked. Some VPNs like Private Internet Access allow you to choose different levels of encryption based on your speed requirements and risk model.

I also paid attention to whether the VPN offers their own DNS servers. If a VPN doesn't automatically route your data through their DNS servers, your requests may go to your ISP's DNS servers first - which undermines the security you're seeking by using the VPN instead of your ISP in the first place. By using their own dedicated domain name servers, the VPN makes sure your data is protected from the moment you type a URL and hit "enter". You can check if your VPN is providing DNS protection by going to http://dnsleaktest.com/.

Some privacy advocates choose a VPN based on what country they are headquartered in. These privacy advocates usually look for a company that is based outside of the "five eyes" countries, a nickname for the first five countries - US, UK, Canada, Australia, and New Zealand - who signed the UKUSA intelligence sharing agreement in the 1940s. The intelligence sharing agreement has now expanded to include 14 countries, including most large European countries, so you'll sometimes see privacy people avoiding "14 eyes" countries as well. Personally, I figured that if a VPN isn't logging, it doesn't really matter where it is based. My take on this might change if more five eyes countries begin to pass laws like Australia's 2018 anti-encryption law, which affect the ability of companies to offer unbreakable encryption.

VPN Matrix

I encourage you to use this information to choose and develop your own criteria for evaluating a VPN. When I was choosing a VPN, this is the matrix I put together [updated 11/2020]:

	ProtonVPN	**Private Internet Access**	**Mullvad**	**Tunnelbear**
Pricing	Limited free tier $48/yearly for 2 devices $96/yearly for 5 devices	$40/year for 5 devices	$66/year for 5 devices	Limited free tier $40/year for 5 devices (on sale) $120/year for 5 devices (full price)
Servers	325 in 29 countries	3160 in 33 countries	779 servers in 36 countries	23 countries
Protocols	OpenVPN and IKEV2/IPSec	Wireguard, PPTP, OpenVPN, and L2TP/IPSec	Wireguard, OpenVPN	OpenVPN, IKEv2
Encryption	AES-256	AES 128 or AES 256	AES-256	AES-256
DNS Protection	Enabled by default	Default on MacOS, toggle on Windows	Enabled by default	Enabled by default
Logs Policy	No logs	No logs	No logs	No logs
Any evidence?	Very strong reputation	Court cases in 2016 & 2018	Open source, independent audit	Full independent audit
Based In	Switzerland	United States	Sweden	Canada
Other Factors	Created by the same company as ProtonMail encrypted email	Accept gift cards for anonymous payment	Sign up with random number; partnered w Mozilla	Adorable interface

Please note these prices are current only as of the date of this post. We hope you find this background helpful when choosing whether a VPN is right for you, and which one you will pick for your own use. Good luck!