freedom.press /digisec/blog/choosing-a-vpn/

An in-depth guide to choosing a VPN

14-18 minutes

Why you may need a VPN

A Virtual Private Network (VPN) is no cure-all for newsroom security or personal privacy, but it offers key security benefits to your workflow as a journalist, especially if any part of your day involves using Wi-Fi, visiting websites or sending emails.

Much like how every phone needs a unique phone number for the phone system to know where to send calls, every device that is connected to the internet has a unique internet protocol address. An IP address in your home or office is likely leased from an internet service provider, or ISP, which bills you or your boss for internet access every month. An IP address has no built-in correlation to specific geography but, over time, IP addresses can be mapped to physical locations with varying degrees of accuracy. In many cases, the mapping correspondence is accurate to a city block. Anyone who can see your IP address can use that to find out — approximately — where you are physically located. This presents a variety of risks, ranging from exposing yourself to the website you are investigating, exposing your location to people you're sending emails to or having your ISP record and sell your internet traffic.

When you visit a website that you're investigating, that website will discover and usually record the IP address from your visit. Similarly, some email systems may record the origin IP address you send an email from and include it with the email's header metadata, possibly exposing your IP address to the recipient. Additionally, embedded images in an email message can broadcast your IP address to wherever the images are being loaded from, unless you turn that off. There are other examples — and more yet to be discovered — of how your IP address can fall into the wrong hands. Rather than tweaking the settings of an infinite variety of applications and hoping to never make a mistake, you can use a VPN to protect your devices from revealing your IP address from the rest of the internet, which would instead only see a VPN's IP address and not the one for your home, office or favorite coffee shop. In addition to protecting your location, a VPN can protect your online activities from being recorded by the ISP that provides the internet connection you are using, or by anyone sitting next to you or even in a nearby boat.

There are countless VPN providers, but not all VPNs are credible. Some might be "free" but otherwise may need to make money by recording their users' unencrypted internet activity and then repackaging and selling that data. "If you're not paying for the product, you are the product" is a relevant axiom here. That's not to say that paid VPNs are invulnerable to that same risk when they are operated by companies with a history of questionable practices. And even paid VPN services can potentially raise other concerns with their privacy policies and technology implementation.

Policy considerations

On the policy side of things, you'll want to look for no-logging guarantees, which will legally restrict a VPN from keeping records of your internet activity for longer than a given period of time — the less time it's kept around, the better. Some of these logs may be anonymized in some way, keeping certain data for tracking usage metrics without tracking the users behind that usage. Although anonymizing logs can be a challenge to do well, it's still better than not attempting to anonymize the logs. Just as with any buying decision, however, reputation is established by a service's users. So, see what VPN users you know say about the VPN providers you're considering, especially if those users have concerns similar to yours.

Despite the claims in marketing copy, little or no protection might come from having a VPN located in a particular country. "Based in Switzerland" will not save you from the very long, international arm of the law. Aside from the vast complex of mutual legal assistance treaties and other agreements between countries, law enforcement has a long history of international cooperation, whether they're in the Five Eyes or any other set of eyes. And in the national jurisdiction on the other end of your connection, the VPN may seem suspicious if VPN usage is rare or heavily restricted.

Ultimately, a VPN is not a system designed for anonymity. Even VPN providers that offer semi-anonymous payment options and collect little customer data still see the IP address you are using to connect to their service and, thus, where you are in the world. In many cases, this can be enough to narrow down your identity significantly.

Technology considerations

On the tech side of things, a well-intentioned VPN provider may read the same philosophy books you like, but ultimately may not be competent in implementing reliable, secure internet infrastructure. Depending on what sort of security concerns you have, some of these features might not be too important, but for the best security a plain VPN can offer, here are some settings and features to look for.

Technical standards and standard settings

Just as there are standards for determining the design of bike tire valves or the size of toilet paper, there are also standards around VPN systems. OpenVPN is one such standard, widely used and very secure when implemented correctly. OpenVPN's protocol consists of a few moving parts, each with different possible configurations, some more secure than others. The authentication part of the protocol ensures that you are the VPN customer you say you are and not someone trying to impersonate you. The "handshake" at the beginning of your VPN connection sets the encryption keys for your session and, finally, a data encryption cipher uses those keys for the actual encryption of data as it travels through a VPN connection.

For a VPN provider's OpenVPN configuration options, these are ideal settings for secure VPN usage:

Ideal settings for OpenVPN authentication, handshake, and encryption.

Authentication	Handshake	Data Encryption
SHA-256	RSA-4096 or at least RSA-2048	AES-256-GCM, AES-256-CBC or ChaCha20-Poly1305

In addition to OpenVPN, the WireGuard protocol has matured into a reliable and secure standard for VPNs and is offered by a growing number of providers. WireGuard's codebase is small and lean, which gives it the advantage of being easily audited for security issues and less dependent on external components. By leaving far fewer components, WireGuard minimizes the number of moving parts that can fail.

Although WireGuard is a newer VPN protocol, its minimal set of components has been thoroughly tested for correctness and has endured the cauldron of security research without too many issues. Unlike OpenVPN, which could be set up to use less secure encryption settings than the ones we've recommended, WireGuard's encryption settings don't include the option of fewer secure options, so there's no need for a separate chart for its ideal settings — they're already great.

A reputable VPN provider will be transparent about which encryption algorithms and ciphers it uses. Some may have different configurations that aren't precisely the most secure option but may have a precise explanation for why their configuration is fine for them and possibly just fine for your privacy concerns as well. Sometimes, VPN software will be limited in the type or strength of encryption it can use due to your device or operating system. So you'll want to check the VPN provider's technical documentation to see if that is the case or not.

Every now and then, a VPN provider will cook up a fancy-sounding custom protocol, bucking existing standards. Although those may be fun to explore, they may not have the same level of scrutiny, peer review or history of being battle-tested with large numbers of people in real-world situations. Where possible, it’s generally best to use a VPN that at least uses a standard protocol vetted by security researchers.

Third-party certifications and audits

Although a VPN company can promise a certain privacy policy or technical specification on its website, it may turn out that what a company *says* it does is different than what it *actually* does. Having an objective third party take a look at a company’s infrastructure to ensure it meets the promises outlined in the VPN’s privacy policy makes those guarantees much stronger, and signals that the VPN company is willing to invest time and money in keeping itself accountable to its users.

A minimum effort popular among some VPN providers is a no-logging certification, in which a third-party auditor inspects a VPN’s servers just deep enough to make sure no logs of your IP address and web traffic are stored. This is better than nothing, but full security audits that check both for the privacy protection and overall security stature of a VPN’s infrastructure — servers, networks and internal rules around access — offer a more complete look into the technical competency of a VPN. Having these audits available to prospective customers *before* they subscribe also helps incentivize VPN companies to improve their security stature more broadly, since those customers, as well as industry reporting, may be weighing recommendations based on how well they score against their competitor’s audits.

iOS caveats

Some devices, namely the iPhones and iPads popular with many journalists, do not have OpenVPN support built-in, but require the use of third-party apps such as OpenVPN Connect, which can be buggy and cumbersome. Some VPN providers may provide instructions on setting up their service using OpenVPN with iOS, but not all will. Fortunately, some VPN providers offer their own iOS apps with built-in WireGuard support, and we recommend using that protocol on iPhones and iPads.

Leaky tunnels

Beyond the fundamental nuts and bolts of the VPN protocol, the way that your device’s additional protocols connect to the internet pose other challenges. Some of those protocols cannot be routed through most VPNs and have to be blocked or routed differently to keep your ISP or local network operator from seeing what you might be up to. Domain name system, or DNS, is another computer network protocol standard. DNS uses DNS servers to translate addresses like “freedom.press” into IP addresses that a computer can route a connection to. Unfortunately, the DNS servers you use are usually automatically set by your ISP or even the Wi-Fi network you connect to and will leak the fact that your device requested the IP address for freedom.press, even if they can’t determine what exactly you’re reading on freedom.press. Make sure to look for a VPN provider that is set up to prevent DNS leaks.

Yet another protocol to add to the ever-expanding alphabet soup of network standards is IPv6. IPv6 is a newer computer network protocol that promises a larger pool of IP addresses than those being used in IPv4. Unfortunately, it can also lead to similar leaking on many VPN protocols, including OpenVPN. So it’s best to look for a VPN with software settings or instructions for blocking all IPv6 traffic. If something you're doing online absolutely requires IPv6, using WireGuard can go a step further than OpenVPN, and route IPv6 traffic securely without having to block IPv6 to prevent leaks.

In addition to DNS and IPv6 leaking issues, there’s also the matter of any network activity your devices broadcast before they get a chance to connect to your VPN provider. Some VPN providers will offer software to connect to their VPN and feature the ability to block all network traffic until the VPN connection is made, sometimes called a “kill switch.” Look for this feature to block other potential leakage. The layering of a growing number of new protocols and systems may also not always have been tested to see if they play nicely with OpenVPN or WireGuard, and it's important to keep an eye out for what new protocols emerge and how they interact with your VPN usage.

National firewall circumvention

Many journalists and others use VPNs to get around national firewalls and access-blocked websites and apps. In countries that use national firewalls, VPN websites are usually also blocked, and VPN apps are unavailable to download in that country's regional app store. If you plan on using a VPN in a country with an internet censorship regime, you'll want to have that set up before you arrive there.

National firewalls also try to block the IP addresses of known VPN servers. This means that even if you're able to install a VPN on your phone or laptop, you may still be blocked from making a connection to the VPN. More sophisticated firewalls go even further, automatically blocking anything that may appear to be VPN traffic using deep packet inspection algorithms. Some VPN providers offer features that aim to disguise traffic so that it's not immediately blocked, such as TunnelBear's GhostBear and VyprVPN's Chameleon protocol. Other VPN providers may address this need with guides on using third-party tools like Shadowsocks. Since internet censorship is a cat-and-mouse game, however, the long-term efficacy of these features cannot be guaranteed.

The shortlist

These five VPN providers have options that, according to their online documentation or support staff, meet the aforementioned recommended settings and features. Those options, however, might not be available for every device or automatically activated right away. You may need to do some additional research to see if your specific device can support the aforementioned tech considerations and if there are any additional steps you'll need to take to switch features on or make changes to them:

- Mullvad
- Mozilla VPN*
- IVPN
- ProtonVPN
- Surfshark

There may be other VPNs that match our criteria and include features that make it a better choice for your situation, including options that may be faster or include a broader range of payment options or specialized protocols that circumvent national online censorship. If your newsroom has a unique situation and would like to learn more about how a VPN can fit into the equation, contact us about our training options.

---

* Mozilla VPN uses Mullvad's servers, and both Mullvad and Mozilla VPN apps have roughly similar features, leaving very little difference in choosing one or the other.