What is a VPN and how does it work? Your guide to internet privacy and security

Whether you're in an office or on the road, a VPN is still one of the best ways to protect yourself on the big, bad internet.

By David Gewirtz | February 3, 2021 -- ZDNet

Whether you're in corporate office or home office, on the road or in your home, a VPN is one of the best ways to protect yourself on the internet. How effective are VPNs? What's the best one for you? What are the downsides? Our executive guide will answer all your VPN-related questions -- including a few you probably haven't thought to ask.

Also: Best VPN services for 2021: Safe and fast don't come for free

WHAT IS A VPN?

VPN is an acronym for Virtual Private Network. The purpose of a VPN is to provide you with security and privacy as you communicate over the internet.

Here's the problem with the internet: It's inherently insecure. When the internet was first designed, the priority was to be able to send packets (chunks of data) as reliably as possible. Networking across the country and the world was relatively new, and nodes often went down. Most of the internet's core protocols (methods of communicating) were designed to route around failure, rather than secure data.

The applications you're accustomed to using, whether email, web, messaging, Facebook, etc., are all built on top of that Internet Protocol (IP) core. While some standards have developed, not all internet apps are secure. Many still send their information without any security or privacy protection whatsoever.

This leaves any internet user vulnerable to criminals who might steal your banking or credit card information, governments who might want to eavesdrop on their citizens, and other internet users who might want to spy on you for a whole range of nefarious reasons.

A VPN creates a private tunnel over the open internet. The idea is that everything you send is encapsulated in this private communications channel and encrypted so -- even if your packets are intercepted -- they can't be deciphered. VPNs are very powerful and important tools to protect yourself and your data, but they do have limitations.

HOW DOES A VPN WORK?

Let's start with the basic idea of internet communication. Suppose you're at your desk and you want to access a website like ZDNet. To do this, your computer initiates a request by sending some packets. If you're in an office, those packets often travel through switches and routers on your LAN before they are transferred to the public internet through a router.

Once on the public internet, those packets travel through a bunch of computers. A separate request is made to a series of name servers to translate the DNS name ZDNet.com to an IP address. That information is sent back to your browser, which then sends the request, again, through a bunch of computers on the public internet. Eventually, it reaches the ZDNet infrastructure, which also routes those packets, grabs a web page (which is a bunch of separate elements), and sends all that back to you.

Each internet request usually results in a whole series of communication events between multiple points. The way a VPN works is by encrypting those packets at the originating point, often hiding not only the data but also the information about your originating IP address. The VPN software on your end then sends those packets to the VPN server at some destination point, decrypting that information.

One of the most important issues in understanding the limits of VPNs is understanding where the endpoint of the VPN server resides. We'll talk about that next.

WHAT ARE THE TWO MAIN TYPES OF VPNS?

Most of us are familiar with the concept of a LAN, a local area network. That's the private network inside of one physical location -- be it a home, a corporate building, or a campus. But many businesses don't run out of one location. They have branch offices, departments, and divisions that are geographically dispersed.

In many cases, each of these offices also has LANs. But how do the LANs connect? For some very specialized solutions, companies lease private lines to connect the offices. That can be very expensive. Instead, most companies opt to geographically connect separated private LANs over the public internet. To protect their data, they set up VPNs between offices, encrypting the data as it traverses the public internet.

This is corporate or enterprise VPN, and it's characterized by the same organization controlling both endpoints of the VPN. If your company controls the originating point (say a sales office) and the endpoint (like a VPN server at your corporate HQ), you can be quite well assured (unless there's a bug) that your data is securely transmitted.
The second type of VPN is a consumer VPN. This is for those of you who compute in hotels or at coffee shops and connect to web applications like social networks, email, banks, or shopping sites. Consumer VPN services help ensure that those communications are protected.

WHAT DOES A CONSUMER VPN SERVICE DO?

A consumer VPN service is, fundamentally, a software-as-a-service (SaaS) offering. The VPN service provides a secure tunnel between your computing device (whether laptop, phone, or tablet) and the provider's data center. This is important to understand. Consumer VPN services protect your transmission from your location to their location, not from your location to the destination application you're using. If you think about it, this makes sense: A consumer VPN service is operated by a completely different company than, for example, Facebook or your bank.

The VPN service gives you an app that you run on your local device, which encrypts your data, and it travels in its encrypted form through a tunnel to the VPN service provider's infrastructure. At that point, the data is decrypted and sent on its way.

Two things happen here: First, if you're using an https connection, your data is encrypted by your browser and then by your VPN app. At the VPN data center, your data is decrypted only once, leaving the original encryption provided by the browser intact. That encrypted data then goes on to the destination application, like your bank.
The second thing that happens is that the web application you're talking to does not get to see your IP address. Instead, it sees an IP address owned by the VPN service. This allows you some level of anonymous networking. This IP spoofing is also used to trick applications into thinking you're located in a different region or even a different country than you are located in. There are reasons (both illegal and legal) to do this. We'll discuss that in a bit.

WHEN SHOULD I USE A VPN?

We've already discussed the use of a VPN when connecting offices. Any time you have two LANs that need to link over the public internet, you should consider using VPN technology or an equivalent method of enterprise protection. In this case, the VPN software will probably run in a router, a server, or a dedicated VPN server hardware appliance.

We talked about two use cases above for consumer VPN services: Protecting your data and spoofing your location. We'll talk more about location spoofing later, so let's just focus on data protection for now.

When you're away from home or the office and you connect to the internet, you'll most often be doing so via Wi-Fi provided by your hotel or the restaurant, library, or coffee shop you're working out of at that moment. Sometimes, Wi-Fi has a password. Other times, it will be completely open. In either case, you have no idea who else is accessing that network, and therefore, you have no idea who might be snooping on your traffic.

I recommend always using a VPN when using someone else's Wi-Fi network. Here's a good rule of thumb: If you're away from the office or home, and you're using someone else's Wi-Fi (even that of a family member or a friend, because you never know if they've been compromised), use a VPN. It's particularly important if you're accessing a service that has personally-identifying information. Remember, a lot goes on behind the scenes, and you never really know if one or more of your apps are authenticating in the background and putting your information at risk.

Another reason you might choose to use a VPN is if you have something to hide. This isn't just about folks doing things they shouldn't do. Sometimes people really need to hide information. Take, for example, the person who is worried he or she might be discriminated against by an employer because of their sexual orientation or medical condition. Another example is a person who needs to go online but is concerned about revealing location information to a person in their life who might be a threat. And then, of course, there are those people in restrictive countries who need to hide their activity merely to gain access to the internet without potentially grave penalties.

ARE THE FREE VPN SERVICES ANY GOOD?

There are some good free VPN services, but I avoid all free VPNs.

Why? It costs quite a lot to provide the infrastructure to operate a VPN service, from the network pipes to the servers. That infrastructure has to be paid for somehow. If it's not paid for by user fees, it's likely to be paid for by advertising, data gathering, or some nastier reason. Here's another reason not to use a free service, and this one is a lot scarier: Malware providers and criminal organizations have set up free VPN services that not only don't protect you but actively harvest personal information and either use it or sell it to the highest bidder. Instead of being protected, you're being plundered.

WHAT'S THE BEST WAY TO CHOOSE A VPN SERVICE?

To be fair, not all pay VPN services are legitimate, either. It's important to be careful about which you choose. I've put together an always up-to-date directory of quality VPN providers. Some are better than others (and that's reflected in their ratings). But all are legitimate companies that provide quality service.

Beyond my directory, it's always good practice to Google a company or product name and read the user reviews. If you see a huge number of old complaints or new complaints suddenly start showing up, it might be that there's been a change of management or policies. When I'm looking for a service, I always base my decision partially on professional reviews and partially based on the tone of user reviews.

Finally, be sure to choose a service with the capabilities that meet your needs. You may need one or more features only provided by certain services. So, think through your needs as you make a decision.

CAN A VPN GUARANTEE MY PRIVACY?

Oh, heck no. A VPN can help make sure you're not snooped on when connecting between your computer and a website. But the website itself is quite capable of some serious privacy violations. For example, a VPN can't protect you against a website setting a tracking cookie that will tell other websites about you. A VPN can't protect you against a website recording information about products you're interested in. A VPN can't protect you against a website that sells your email address to list brokers. Yada, yada, yada.

A VPN does help protect you in the situations we've discussed in previous sections. But don't expect a VPN to be a magical privacy shield that will keep everything you do private and confidential. There are many, many ways your privacy can be compromised, and a VPN will be of only partial help.
Also: A VPN will not save you from government surveillance

WILL VPN SOFTWARE SLOW DOWN MY COMPUTER?

That would be a definite maybe. Here's the thing: Back in the day, the process of encrypting and decrypting packets would take a toll on CPU performance. Most current CPUs are now fast enough that most crypto algorithms can run without much of an impact on processor performance. However, network performance is another thing entirely. First, keep in mind that if you're using a VPN, you're probably using it at a public location. That public Wi-Fi service is likely to range in performance somewhere between "meh" and unusable. So, just the fact that you're remotely working on a mediocre network will reduce performance. But then, if you connect to a VPN in a different country, the connection between countries is also likely to degrade network performance. Server locations matter.

My rule of thumb is to use a domestic VPN and connect to servers as close to my location as possible. That said, I have had good nights and bad nights getting online. In my recent trip, I found most hotels' networks to become unusable after about 9pm. My theory is that many of the guests were watching Netflix at that time, completely clogging the hotels' pipes.
Also: How to use a VPN to protect your internet privacy

DO VPN SERVICE PROVIDERS LIMIT USAGE AND HOW?

Some do. Some don't. Look at that directory I mentioned earlier because that's one of the factors where a service might lose some points.

Some VPN services will limit the total amount of data you can send and receive, either in one connection session or over a month. Other VPN services will limit the speed of the data, effectively sharing less of their pipe with you than might be optimal. That could slow your browsing experience to a crawl or completely prevent you from watching streaming video.

Usually, it's the free services that throttle your usage in these ways. Some paid services will offer a trial, where you can transmit up to a certain data cap before being asked to sign up as a paying customer. That's actually pretty cool because it gives you a chance to try out the performance of their service before paying, but it also gives the vendor a chance to make the money necessary to operate the service.

Many VPN services claim that if you pay their fee, they'll provide you unlimited data transmission and won't throttle your speeds. Generally, this is true, but I'll give you my standard "unlimited bandwidth" warning: It's been my experience that when a vendor says something is "unlimited," it's almost always limited. Somewhere, there will be a note in the fine print or terms of service that allows the vendor to limit you in some way. It pays to read those agreements.
Also: **Why free VPNs are not a risk worth taking**

HOW PRIVATE ARE VPNS? DO THEY LOG EVERYTHING I DO?

In my VPN directory, I tracked two types of logging. The first is whether they log traffic, DNS requests, and IP addresses. This is pretty nasty stuff. If a VPN service logs this, they would have the information you might choose to hide, like sites you visit, locations where you are, and possibly even information you might be sending.

Although the use of these services will still protect you from Wi-Fi spies in your hotel or restaurant, I can't recommend signing up for any service that does DNS, traffic, or IP logging. There are better, more private options.

The second type of logging is more benign. VPN services that log bandwidth usage and connection timestamp data usually do so either to tune their own systems or manage any abuse of their services.

I have less of a concern with services that just monitor bandwidth usage, as long as they don't store any specifics. That said, we gave top marks to those services that don't do any logging. When I choose a VPN service, those are the services I pick for my use.

WHAT DO NET NEUTRALITY CHANGES MEAN FOR MY VPN USAGE?

Net neutrality has been severely under fire in the US. The Federal Communications Commission (FCC) has eliminated many of the consumer protections against internet service providers (ISPs) harvesting traffic data and selling that data to advertisers, or worse.

This could be bad. I'm not terribly concerned if Comcast discovers my secret passion for muscle cars and I get more ads for car customizing kits. It might be annoying, but I'm not doing anything I want to hide. Where the problem could occur is if ISPs start inserting their own ads in place of ads by, say, ZDNet. That could cut off the revenue that keeps websites alive, and that could have very serious repercussions.

As for personal use and whether you should use a VPN at home because of net neutrality, I don't think we're there... yet. Certainly, if you're working on confidential information and connecting to work, you should use a VPN. But we haven't yet seen any evidence of ISPs being so intrusive that always-on VPNs are required at home.
Stay tuned to this guide, because if that changes, we'll let you know.

IS IT LEGAL TO USE A VPN?

That depends. VPN use is legal in most countries, but, according to VPN provider CyberGhost, VPN use is illegal in the United Arab Emirates, Turkey, China, Iran, North Korea, Saudi Arabia, and Russia. Vladimir Putin has recently banned VPN use in Russia. Also, be aware that the so-called proxy server alternative to VPNs is also illegal in many countries, which consider any form of IP spoofing to be illegal, not just those services labeled as VPN.

Restrictions vary, as do penalties. China allows certain approved VPNs. In the UAE, if you use a VPN, you could go to jail or be fined a minimum of more than the equivalent of $100,000.

Definitely research this before you visit a country. Many travelers mistakenly believe that just because they're not citizens, and all they're doing is linking back to a corporate system, they should be able to have unrestricted use of VPN software. This is a mistake.

The bottom line: Check the laws of the country you're in before connecting. It's also a good idea to check with your VPN provider, both for insight as to whether it knows if there are issues and whether it'll support connectivity from the country you're visiting.

DO I NEED TO USE A VPN IF MY HOTEL HAS A WIRED INTERNET CONNECTION?

Yes. It is almost totally unlikely that each room is on a dedicated subnet, so that means packets are traveling across a network shared by other guests. In addition, you never know whether someone in the front office has set up a packet sniffer for the express purpose of mining guest information.

So, yes, use a VPN, even if there's a hard-wired connection to the wall.

WILL A VPN SERVICE HELP ME CONNECT SECURELY TO MY OFFICE NETWORK?

If you're trying to connect to your on-premises corporate network, you'll most likely be assigned a VPN application by your IT department. This will allow you to establish a point-to-point connection between your local device and a server owned and operated by your company.

But, if your company is cloud-based, and you're connecting to SaaS applications like Salesforce or Google, you should probably use a VPN service, since you're not actually connecting to your company but instead to a public cloud application.

If your IT department does not specifically identify a VPN service you should use for accessing their public cloud applications, definitely look at our VPN directory and choose one of the higher-rated service providers.

CAN I GET AWAY WITH A VPN APP, OR DO I NEED TO BRING MY OWN ROUTER/BRIDGE/DONGLE?

Let's talk about what happens when you use a VPN app on your computer or mobile device. Any VPN app will require an existing network connection to be able to connect to the VPN service provider. This means that even if you set your VPN app to automatically launch when your device boots, there will be a period when your computer is connected to the internet directly, not through your VPN. Some background services can send information across that initial, unsecured connection before the VPN loads. To be fair, the risk is relatively minor for most usage profiles. If you're establishing a connection automatically to your corporate server, you will want to check with your IT team about how they want you to set things up.

If you are interested in an added level of protection, there are intriguing gadgets called Tiny Hardware Firewalls. These devices range from about $30 to $70 and connect via a network port or a USB slot to your laptop. They make the initial network connection, and so your computer's communication is always blocked before it calls out to the internet.

SHOULD I USE A VPN ON MY PHONE OR TABLET?

Both Android and iOS come with basic VPN capabilities to allow you to securely connect to your corporate networks. Your IT organization will generally advise you when you should use this feature, but as we've discussed, when away from your home or office, and especially if you're using an open, public Wi-Fi connection, you should.

If you're connecting to web applications like email or Facebook, you should consider using a VPN service -- particularly if you're connecting via an open Wi-Fi network. Most good VPN services offer both iOS and Android clients.

- The best mobile VPNs can ensure your privacy anywhere
-

DO I NEED A VPN IF I'M CONNECTING MY PHONE VIA LTE?

That depends. Once again, your corporate IT department will let you know their policy for connection directly to their corporate network. Usually, you'll use the VPN client built into your device's operating system for that.

But here's the thing: It's up to how much you trust your carrier, where you're located in the world, and how secure you want to be. In the US, the carriers (net neutrality notwithstanding) can generally be relied upon to provide a secure connection from your phone to their network.

That said, it is possible to compromise wireless phone service with a man-in-the-middle attack. This situation occurs when a malevolent actor places a device designed to confuse your phone and cause your phone to connect to what it thinks is the phone network, but, in fact, it's a device designed for spying.

Outside the US, it depends on what country you're in. If you are really concerned about security, simply avoid bringing any devices into a foreign nation that you intend to use after your trip. Those devices can be compromised in the country or during customs inspections.

Likewise, if you're connecting via a nation's local carrier, that carrier may be intercepting your traffic, particularly if you're a non-native of that nation. In that situation, if you must connect back to applications and services at home, using a VPN is quite literally the least you can do. Also, keep in mind that if you use your phone's hotspot to connect your computer to the internet, you'll want to use a VPN on your computer as well.

Finally, it's worth reminding you, as we covered earlier in this guide, that some countries consider VPN use illegal. If you're planning on traveling, be sure to research local laws exhaustively.

WHAT HAPPENS IF A VPN CONNECTION FAILS WHILE I'M ON A REMOTE CONNECTION?

A lot depends on what VPN you're using, how it's set up, and where you're connecting. That said, let's look at the most likely scenario.

Recall that when you're online and connected to an internet application through a VPN, a few things are happening: Your data from your computer to the VPN service is encrypted by the VPN. Your data from the VPN service to the internet application may or may not be encrypted via https, but it's not encrypted by the VPN service. And your IP address is spoofed. The online application sees the IP address of the VPN service, not of your laptop.

When a VPN connection drops, you might just lose your connection. But because the internet is very good at routing around failures, what is more likely to happen is your computer will reconnect to the internet application, simply bypassing the VPN service. That means that -- on failure -- your local IP address may "leak out" and be logged by the internet application, and your data may be open to local Wi-Fi hackers at your hotel or wherever you're doing your computing.

There is a reasonably robust solution to that problem, and that's next.

WHAT DOES A VPN KILL SWITCH DO?

Put simply, a VPN kill switch kills your internet connection if it detects that your VPN's connection has failed. There are generally two types of VPN kill switches.

The first runs in the VPN client app on your computer, so if the VPN connection fails while the VPN client app is running, that VPN client app can turn off the computer or mobile device's internet connection. However, if your VPN connection has failed because the VPN client app itself crashed, then the kill switch may not work, and your IP and data may leak onto the internet.

The second type of VPN kill switch is at the operating system level. These are usually driver-level systems that run whether or not the VPN application is running. As such, they provide a bit more protection for your surfing activities.

Given that so many VPN products we reviewed in our directory support a kill switch, we recommend choosing a client with a kill switch feature. There may be a slight annoyance if you lose your connection, but that's more than made up for in the added security.

WHAT DO ALL THOSE PROTOCOL NAMES MEAN AND WHICH ONE SHOULD I CHOOSE?

If you've been shopping for a VPN service, you've undoubtedly come across a bunch of names like SSL, OpenVPN, SSTP, L2TP/IPSec, PPP, PPTP, IKEv2/IPSec, SOCKS5, and more. These are all communication protocols. They are, essentially, the name of the method by which your communication is encrypted and packaged for tunneling to the VPN provider.

There is a lot of debate among security purists about which protocol is better. Some of the protocols (like PPP and its tunneling variant, PPTP) are old and have been compromised. Others, like SSTP, are proprietary to one company or another.

My recommendation -- and the protocol I most often choose to use -- is OpenVPN. OpenVPN is a non-proprietary, open-source implementation of a VPN communication layer protocol. It's well-understood, wellregarded, generally quite secure, and robust. Also, it has the benefit of being able to communicate over port 443, which is the standard port for https communication, which means almost all firewalls will allow OpenVPN traffic -- and most won't even be able to detect that a VPN is being used.

Yes, there are certainly other protocol choices, even some that might be more appropriate than OpenVPN in certain situations. But if that's the case, either you've already made that decision, or your IT organization has specified a specific protocol you should use. As a default, however, if you're not sure what to look for, look for OpenVPN.

WHAT DOES IT MEAN WHEN A VPN SERVICE TALKS ABOUT SIMULTANEOUS CONNECTIONS?

The term "simultaneous connections" generally refers to the number of devices that can be connected to the VPN service and talk to the internet at once. For example, when I was driving across the country and working in my hotel room at night, I often had both my MacBook Pro and iPad connected to the internet.

I used the MacBook Pro for writing, keeping the iPad open to do searches and find supporting information. Both of these were connected to the internet at one time. This was possible because the VPN service I was using allowed up to three connections open at once.

This is also a good way to provide support for more than one family member on a single subscription. Generally, there's no good reason for a VPN provider to allow less than two or three connections. If your provider only allows one, find another vendor. We gave extra points in our VPN directory to those vendors who allowed three or more connections.

WHEN SHOULD I CHOOSE EITHER DYNAMIC OR STATIC IP?

Every device connected to the public internet is assigned an IP address. It's like a phone number for each device. To be able to connect to the internet, each device needs such an address.

The term "dynamic IP address" means that when a device connects to the internet, it's given an IP address taken from a pool of available addresses. While it's possible to get the same IP address on multiple connections, generally each time you connect, you'll get a different address.

If you want to hide your address from the web applications you're connecting to, you'll want a VPN service that provides dynamic IP addresses. In our directory, we list the number of IP addresses each service offers. By using a service with more available IP addresses, the chances of you getting a repeated IP are quite small.

There are some minor disadvantages to using a dynamic IP. If someone who previously had the IP address you've been assigned did something nefarious on a service you use, the IP address might be banned. Usually, VPN providers are very careful about checking their IP addresses against blacklists, so the chances of this being a problem for you are slim.

By contrast, a static IP address is an address that's assigned to you and only you. Most often, this is needed if you're running a server. Usually, static IP addresses are used in corporate situations and are generally not practical for general remote access, like from a hotel or coffee shop.

Unless you have a specific application that you know needs a static IP, you'll want to be assigned a new dynamic IP address for each VPN session you initiate.

WHAT DOES IT MEAN WHEN A VPN SERVICE TALKS ABOUT SERVER SWITCHING?

As we mentioned in the previous section, when you connect into a VPN service, you're usually assigned a dynamic IP address from a pool of addresses. But where are those addresses located? They're attached to servers located, usually, throughout the world.

Most VPN services allow you to connect to server locations in many different countries. In our VPN directory, we list both the number of servers the service maintains, as well as the number of countries. By default, you'll usually be assigned a server located in your home country, but if you want to obfuscate your location, you may want to connect to a server location in a different country.

Server switching is a feature -- offered by most VPN service providers -- that allows you to change what region or country you're going to connect to. Most providers allow you to switch as often as you'd like (although you usually have to disconnect, then change your configuration, and reconnect). This may be useful if you're trying to hide your location, or if you're running into some communications glitches on the server you're currently using.

CAN I USE A VPN TO SPOOF MY LOCATION OR COUNTRY OF ORIGIN?

Because the VPN server you're connected to presents its IP address to whatever web application you're using, by choosing a server located in a different country, you can represent your connection as if you're in a different country. This may be illegal in certain regions, so use caution when doing this.

In my testing, some VPN providers were able to successfully hide their originating country or the fact that they were VPNs, but others were not. You'll probably want to do some testing. Of the services where I did in-depth testing, NordVPN and Hotspot Shield were able to successfully hide their VPN origins, while StrongVPN and CyberGhost were not.

CAN I USE A VPN TO WATCH A BLACKED-OUT PROGRAM OR VIDEO?

Sometimes it is possible to watch a blacked-out sporting event or other show, although we certainly can't advise you to do so. Spoofing your location to bypass broadcast restrictions may get you in hot water.

Also, do be aware that some broadcasters have developed increasingly sophisticated methods to determine whether the IP address you represent is the IP address where you're located. The VPN may be able to protect your original IP address from being seen, but there are characteristics of proxy communications (like a slightly longer time to transfer packets) that can be used to identify users who are trying to bypass watching restrictions.

Also: Why a proxy server can't protect you like a VPN can

IS IT TRUE THAT A VPN IS COMPLETELY UNHACKABLE?

No. No. Did I mention... no. Nothing is unhackable. As evidence…

In January 2018, Cisco Systems (a very highly respected maker of internet communications hardware) revealed that a critical bug was found in its ASA (Adaptive Security Appliance) software that could allow hackers to remotely execute code.

This is a bug in enterprise-level VPN systems used by corporations, so it's very serious, indeed. Fortunately, responsible IT administrators can patch their systems to fix the bug. However, it goes to show how no system can be truly deemed absolutely secure.

Another example was a bug in Hotspot Shield, a popular VPN service. This bug allowed a hacker to expose private information, including originating IP. Hotspot Shield issued an update, which gives us an excuse to remind you that you should always install updates, especially on your VPN client software.

WHO ARE THE KEY PLAYERS?

We've done in-depth reviews of the following VPN services. If you're considering a VPN, you might want to read these articles first:

- **NordVPN review:** Sincere about security and privacy
- **StrongVPN review:** A clear and easy-to-use VPN ideal for coffee shop use
- **Hotspot Shield review:** Here's a VPN that actually lives up to its hype

- **CyberGhost VPN review:** More than just VPN, an all-in-one security kit
- **IPVanish review:** VPN delivers a wealth of options and browsing controls

While there are a tremendous number of VPN vendors out there, we think the following are some of the best:

- **NordVPN:** 30-day refund, lots of simultaneous connections
- **ExpressVPN:** Detailed FAQ, good refund policy, Bitcoin
- **IPVanish VPN:** Keeps no log files and has support for Kodi
- **PureVPN:** Large network, strong technically, good performance
- **Surfshark:** Unlimited device support, whitelisting feature
- **Norton Secure VPN:** Company is trustworthy and accountable
- **StrongVPN:** Excellent infrastructure, decent price performance
- **Hotspot Shield:** Best money-back guarantee
- **Private Internet Access:** Lowest yearly price, most servers
- **CyberGhost:** Supports Kodi, good Linux and router support

For a more detailed review of each, visit our VPN directory.

original article:

https://www.zdnet.com/article/what-is-a-vpn-and-how-does-it-work/?ftag=TRE-03-10aaa6b&bhid=23405847687286447375579737817622&mid=13257984&cid=716947763