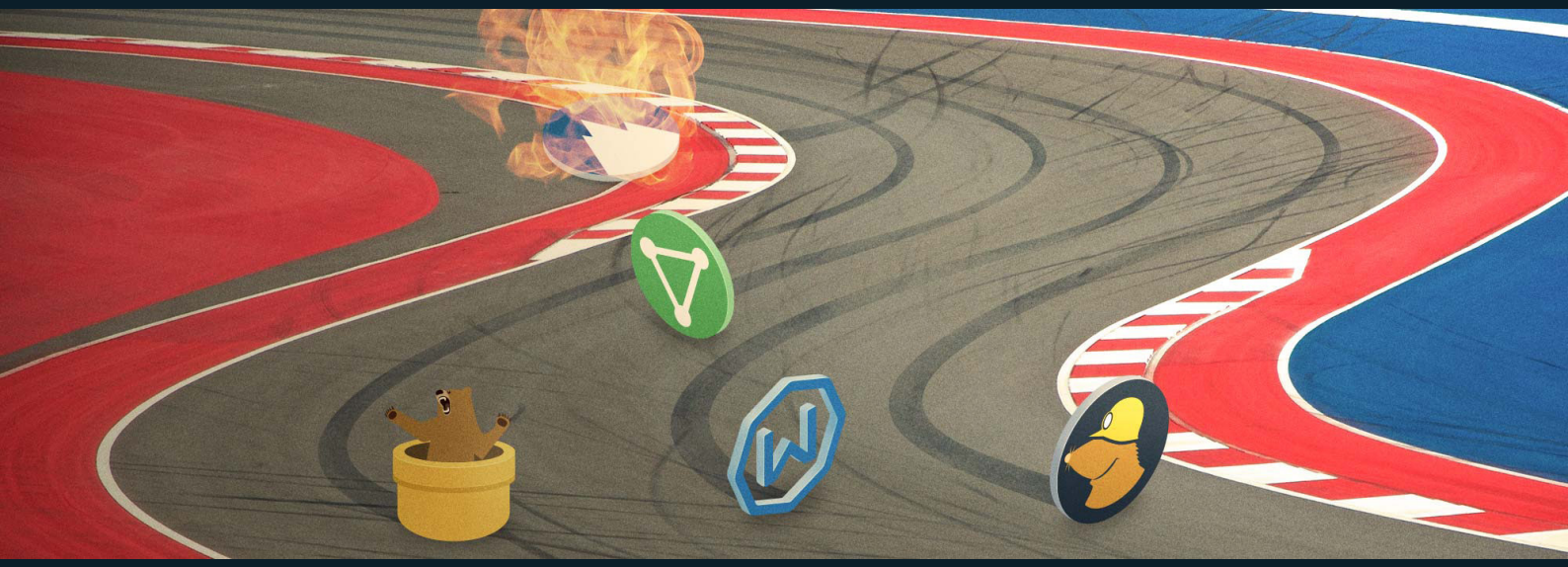


What's the "best" VPN

Virtual Private Networks works like a protective tunnel, shielding your data from the outside world while also hiding your true IP-address.

VPN services are a handy way to stay safe and get access to restricted streaming content, but they are also a good tool for hackers, advertisers and governments to steal and snoop on your data.

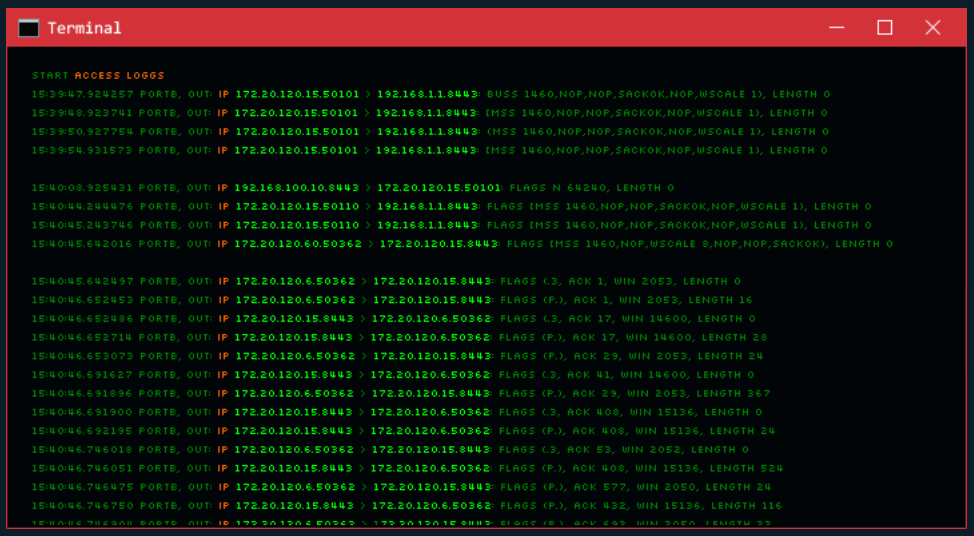
Why do I need a VPN

A VPN shields your browsing, hiding your real IP address and what sites you visit with a layer of encryption. This is useful to avoid being tracked by advertisers, or the government if you don't have access to free speech.

It can be especially useful if you're traveling and is forced to use public Wi-Fi hotspots. Public hotspots are a juicy target for hackers, and they usually snoop these unencrypted networks, catching your login details and all other information sent trough them. With a VPN, all the traffic sent from your computer (or phone) is

encrypted and impossible to access, even on public hotspots.
But privacy is not the only reason to use a VPN-service, many use it to get access to content that's restricted in their country of origin. For example, if you are in Sweden and want to access Netflix American content, you simply connect to an American VPN server and Netflix thinks your surfing from the USA.

No logs?



While the do protect your privacy, that protection comes at a cost and if you're not paying attention, your information could be leaked. When using a VPN, the VPN provider will know everything about your browsing habits since all information from your computer goes through their servers.

The information about your browsing habits is saved in logs, these logs can be subpoenaed and made available by law enforcement. Some VPN providers clearly states they do not keep logs at all, or just the required time by law, but they are not all truthful.

Connection logs

These logs help the VPN provider to monitor the workload of each server, manage traffic and prevent abuse. Any VPN provider that limits the number of connections per user has to keep these logs in order to enforce this limit.

In best cases they are limited and anonymized, but they could include:

* When you connected to the VPN server and for how long.
* The IP address you originally connected from.
* Witch VPN server you are connecting to.
* Diagnostic data you send following a crash.

Connection logs can be used to identify your computer and because of this some companies, like ExpressVPN, promise to never keep them.

Why “Free” VPN is dangerous

Intercepted traffic
There are many free VPN services out there, but running a VPN service with tens or hundreds of servers cost money, so how do they pay their bills?

They pay their bills by selling the data they collect about you and your browsing habits to advertisers and governments. You might be surfing with a free VPN service that originates in China, then your data is shared with Chinese authorities.

In a review in 2019 of Google and Apple’s app stores, 60% of popular free VPN apps were secretly Chinese-owned and 90% had serious privacy flaws. By supplying the majority of free VPN services and intercepting the data, China has created a vast industrial espionage network with minimum effort and willing participants.

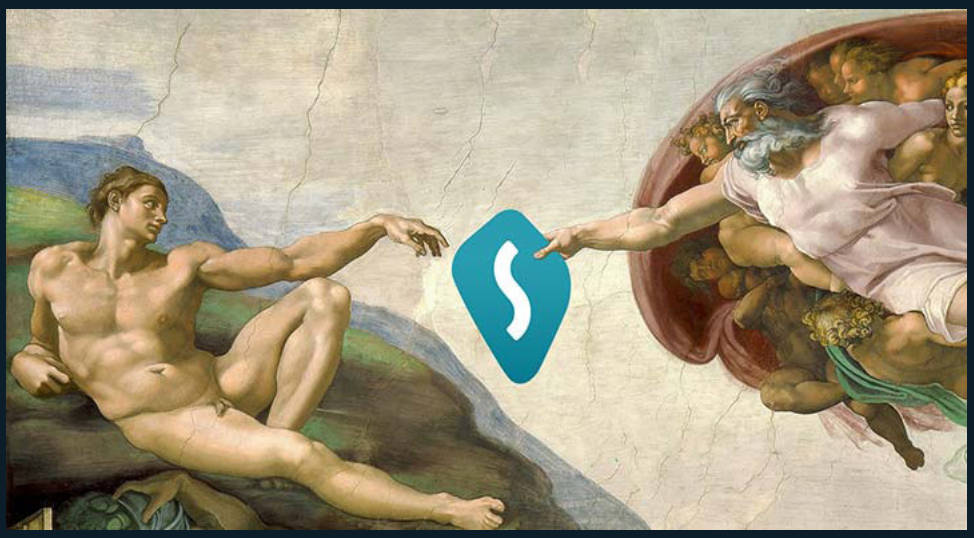
Malware
In a study on free Android VPN services, CSIRO found that a whopping 38% of these highly-rated apps, with millions of downloads, contained malware. This malware could steal personal information like passwords, social security number or even contain ransomware that locks your device.

Forced ads
By sneaking an ad-serving tracker into your browser, some free VPN providers force you to watch their ads on every page you visit. It’s an easy way to make money and is often accompanied by backdoors that secretly collect and sell your data to advertisers.

Selling your bandwidth
Getting access to their favorite subscription services when abroad is one of the main reasons people use VPN services, but what’s the point if it’s too slow to watch?

Some VPN providers pick up the slack by limiting your bandwidth, and then selling the rest. Sometimes they don't care who they sell your bandwidth to, and that can get you into legal problems. Famously, Hola was caught selling their users' bandwidth to whatever group paid, resulting in spammers using their customer's data to spread spam and malware.

Our recommendations



Here is a list of some of the Internets most recommended VPN services, all of them offer either a free trial or a free version.

If you don't want to spend money but still need a VPN, you should consider trying the trial versions of the big names. And if you like the application you should definitely consider buying it since free VPN's are just a can of worms.

Surfshark - "Best overall"

1-month: €10.85/m, 6-months: €5.44/m 1-year: €2.09/m (deal)
Homepage: www.surfshark.com

Surfshark is one of the internet's most recommend VPN services, although smaller than competitors, they make up for it in speed, features, and price. Surfshark offers unlimited device support, so you can connect all of your devices to a single account. They also have no limit on the number of connections from that account and even filters out malware and blocks ads and tracking.

For all its features and the low price, Surfshark is the clear winner.

With all subscriptions, Surfshark offers a 30-day money-back guarantee, so you can try it for a full month before claiming a refund.

Proton VPN

Free, Basic: €4/m, Plus: €8/m, Visionary: €24/m
Homepage: www.protonvpn.com

ProtonVPN takes privacy and security seriously, routing your traffic through a secure bunker of private servers, while also including a built-in route to VPN into Tor servers. The company has good transparent policies and is completely open-source with routinely published audits.

ProtonVPN is one of the few VPN providers that offers a free version, thought not as fast as their paid version it still offers unlimited bandwidth and data. The free version only supports one device and access to servers in the Netherlands, Japan and the US, for all 55 countries you need their paid version.

Tunnelbear

Free, Unlimited: $3.33/m, Teams: $5.75/user per month
Homepage: www.tunnelbear.com

TunnelBear is also a Canadian-based VPN service and is instantly recognized by its friendly bear mascot, which helps make the technology more approachable to new users. Like other privacy-minded VPN providers, TunnelBear has an anti-logging policy and a clear privacy policy, it's also been independently audited.

TunnelBear has a free trial option, so you can test and see what speeds you'll get before committing.

Mullvad

Free, Basic: €4/m, Plus: €8/m, Visionary: €24/m
Homepage: www.mullvad.net

Just like ProtonVPN, Mullvad VPN is completely open-source and the service has been independently audited. They offer apps for every major platform and routers, advanced users can even download OpenVPN configuration files.

Mullvad VPN is based in Sweden, and although they are not the biggest names in the industry, they take privacy very seriously. With Mullvad you can pay for the service completely anonymous by including a randomly generated account number with cash, and mail it.

As with other paid options, Mullvad has a 30-day money-back guarantee, so you can safely try it before you decide.

Express VPN - "Good for streaming"

1-month: €12.95/m, 6-months: €9.99/m, 1-year: €8.32
Homepage: www.expressvpn.com

ExpressVPN, a British Virgin Islands-based company, stands out from the competition by being independently verified to not keep logs of customer activity. They have been independently audited and have also failed to produce logs in court and even gotten their servers seized by the Turkish government, who found nothing.

They have apps for nearly every device including routers, Android, and iOS. ExpressVPN offers fast and reliable connections and can reliably circumvent Netflix's country restrictions.

ExpressVPN does not offer a trial period but offers a 30-day money-back guarantee just as long as you remember to request a refund.

Windscribe

Monthly: $9/m, Yearly: $4.08/m, Custom: $1/location/m
Homepage: www.windscribe.com

Windscribe is cheap, offers good speeds, and takes privacy and security seriously, it's one of the most recommended VPN providers.

Windscribe is a Canada-based VPN service, offers a custom payment plan outside the normal monthly or yearly subscriptions. For every dollar you pay, you get access to 1 country and 10 GB monthly traffic. This is perfect for when you're on vacation and only want to watch some shows in your home country, you can pay only for 1 country.

Just like ProtonVPN, Windscribe offers a free VPN service with a generous 10 GB monthly data limit.

Original post can be found at our homepage:

https://bitidentify.com/blog/whats-the-best-vpn/