BLINN.COMmunications

179 Caren Avenue • Worthington • Ohio 43085-2520 • 718.577.1054 (NYC) • 614.785.9359 (Ohio)

1 August 2023

Protecting Privacy with a Virtual Private Network

Virtual private networks (VPN) have become popular because they make communications more secure, but they can also impart a false sense of security.

Google started offering a free VPN service in May and some cellular providers also include VPN technology. Google-Fi, for example, enables always-on VPN that functions whether the user is connecting via the cellular data plan or a Wi-Fi hotspot.

Your computer or phone sends and receives a lot of data. Connections are more secure now that most websites support secure HTTP (addresses that start with http**s** instead of http), but a VPN encrypts the entire connection so that it can't be intercepted.

In addition to encryption, a VPN service disguises your IP address and your location. Although beneficial, this can create problems for sites that want to know your location and base their decision on the IP address. You may search for a nearby restaurant only to be given a list of locations in a city hundreds of miles away. This is easily remedied, but it can be confusing.

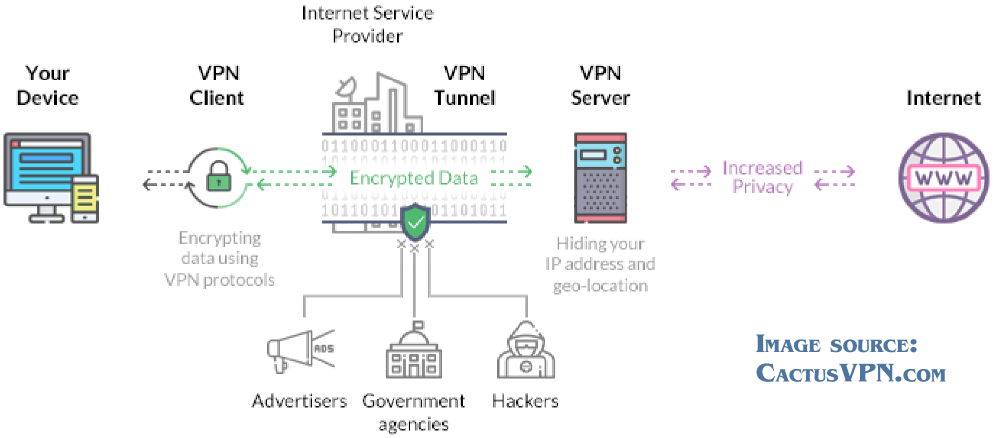
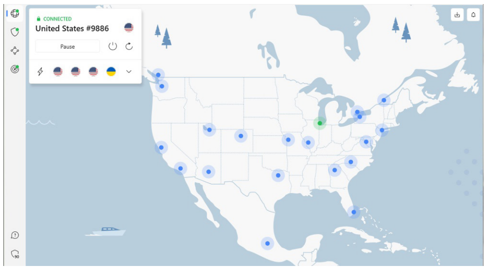


Image source: CactusVPN.com

Also, some websites may not work when a VPN is active, network performance will be at least slightly slower, and good VPN services aren't free.

Until she retired, my wife worked from home using a computer provided by her employer. The computer connected via a VPN to the company's servers. Without the VPN, the connection would be refused. I work from home and do not need to connect to enterprise servers. I enable secure FTP and secure shell when I connect to banks, medical offices, and streaming services, but I enable a VPN for added security.

Your computer and devices inside a corporate or home network have private IP addresses, but the address on the internet side of the router is visible to any site you connect to. The address reveals your general location.



My VPN (Nord) defaults to show my location as Chicago, but I can select other locations such as New York, Toronto, Montreal, Los Angeles, Seattle, or even an address in Mexico, Brazil, South Africa, England, Finland, or elsewhere.

When information is sent as plain text, it can be read by anyone who gains access to the data stream. Encrypted data can also be revealed, but the content is meaningless to anyone who lacks the proper encryption key.

```
PLAIN TEXT
In addition to encryption, a VPN service disguises your IP address and your location.
Although beneficial, this can create problems for sites that want to know your location
and base their decision on the IP address. You may search for a nearby restaurant only to
be given a list of locations in a city hundreds of miles away. This is easily remedied,
but it can be confusing.

ENCRYPTED TEXT
fr6gjkXQQ5P+tVCyIYd37/jJ/rCpr0TuXk9G/clZ0Yoqw/YDb9p+v3kI9OflRtnzAaPpTmmBTmZYIK0l6JgslEhUC2n
e56WvhfgeR7aQfyQVVBXmgsm7Oaas6+wS+7bLCBYi4w+YaTae3eJuGfuPmlssjpG9AUDiSa2Ydow9CCnN2u4zsdshSS
CWMBPX7xjcGAOUcvxC+aUTnBBYVZ6t5bQFnqVOYjfDFhwvOR2fp9KTsgi+yZK6oyiBWdvsFyZIaDsGN+PVdOKD2erNt
3176PomINVKgUKrtzdVwaEAhAafo9X76LbHLzGcsHVp5Df+b6U5cXLIrjSlBMYTkSNMsM3IXyrRH9T+yh2u0chdimdn
AwrBVOEsAEbmsL2FwrbYcuO2VZ/JUwNAYocVB+RFcIwGE1XPHXcfM2nBPsqMXZ3zG8ALDbv+0nyKvaH7Z90MOKECdiB
lMejinI4hGrlxe391nHuY7ZgaMaRUUCTe2BRPDgmTZonkY83RW17GMMaj
```

Blinn Communications News (ISSN 2639-5762) is for clients and friends of William Blinn Communications, Worthington, Ohio. Phone 614.785.9359 (Columbus) and 718.577.1054 (NYC). On the Web at www.blinn.com. All rights reserved.

Appearing to be in an alternate location may allow access to some services that are geo-restricted. However, being able to stream BBC television programs live by changing the VPN server to London isn't one of them. You would also need a government television license that requires an address in Great Britain.

So the primary advantage is privacy. Encryption keeps your data safe from your internet service provider. The ISP can see that you're connected to a VPN, but not which websites you visit. Some ISPs collect that kind of information and sell it to advertisers.

A VPN might be helpful for home or office computers, but it's essential when you're mobile. Using public Wi-Fi at an airport or cafe is risky because scammers can intercept unencrypted data.

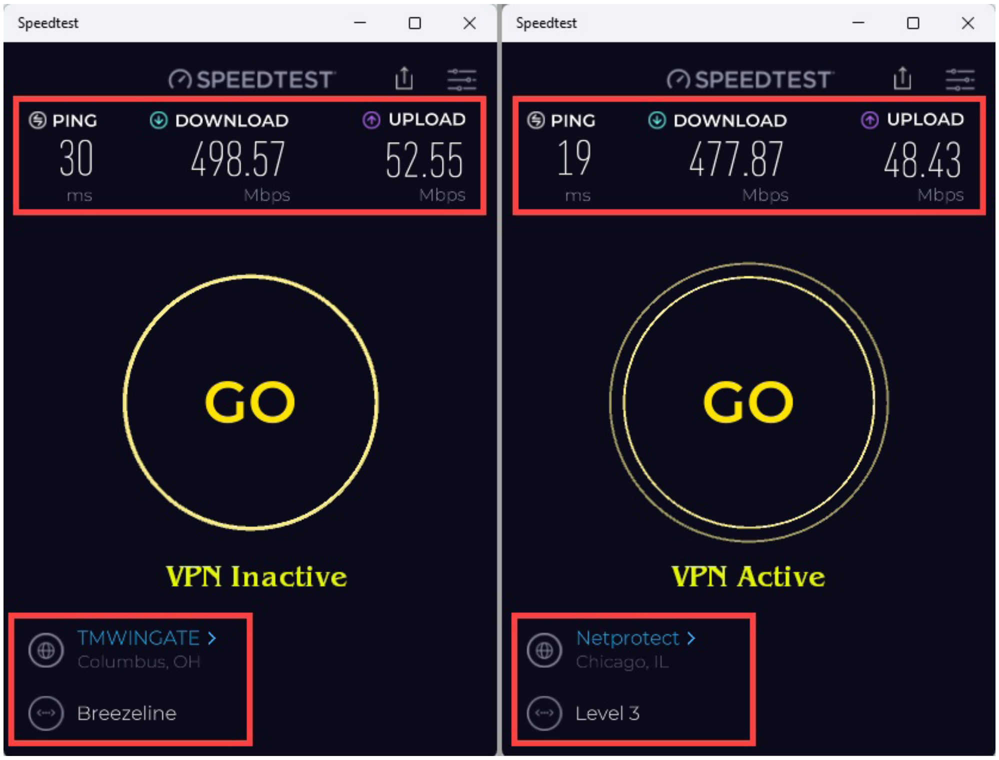
There is one threat that a VPN can't eliminate: Browser fingerprinting is a technique that can be deployed by organizations to identify a specific computer with more than 90% accuracy based on information that can be obtained from most browsers.

So consider a VPN to be optional for home use, essential for public use, and yet insufficient to *guarantee* privacy and security.

Do Downsides Exist?

Some downsides exist, but overall there are more advantages than disadvantages. Most of the problems are easily overcome or not difficult to endure.

The most common is degraded downlink and uplink speeds, but this has not been a problem recently for me. Nord's servers reduce throughput only a little. My service at home is rated for 500Mbps (downlink) and 50Mbps (uplink). Recently, SpeedTest.net showed 499Mbps downlink with the VPN off and 478Mbps with the VPN on. That's less than a 4% difference. Results were similar for the uplink, 53Mbps with the VPN off and 48Mbps with the VPN on.



PING 30 ms | DOWNLOAD 498.57 Mbps | UPLOAD 52.55 Mbps

VPN Inactive

TMWINGATE >
Columbus, OH
Breezeline

PING 19 ms | DOWNLOAD 477.87 Mbps | UPLOAD 48.43 Mbps

VPN Active

Netprotect >
Chicago, IL
Level 3

A VPN will always reduce network transmission speeds, but a well run VPN will have only minimal effect.

Oddly, the ping speeds were faster when the VPN on, 19ms versus 30ms. Ping measures the amount of time required for one system to respond to another. Ideally, these times should always be single digits, but the two values I received are common for consumer-grade internet service.

Another potential problem: Some websites don't work when a VPN is involved. Although the VPN doesn't make it impossible to connect to one of my bank's servers, it means that the bank's computer is less certain that I am who I claim to be and it generates an out-of-band challenge that adds a few seconds to the login every time I visit the site.

Overall, it's better to have a VPN than to forego it because of perceived or actual shortcomings.

How Much?

Although free VPN services exist, it's generally better to pay.

Operating a VPN has associated costs and, if the VPN provider offers the service for free, the obvious question is about how the service is being monetized.

Google's VPN is free and can be used by anyone with any type of Google account, but a full-featured VPN such as the one from Nord is generally a better choice. There is a cost, but it's modest.

It's better to pay a few dollars per month for a commercial service. Three recent VPN reviews are online and can help you choose the VPN that's right for you. The articles are from *Tom's Guide*, *PC Magazine*, and *Wired*.

The VPN I selected several years ago and recently renewed for two years is from Nord. *Tom's Guide* ranks Nord second behind ExpressVPN, *PC Magazine* places Nord second behind Proton, and *Wired* says Nord is best for circumventing geographic restrictions but Surfshark is best for most people.

Check out the reviews and think about which features are most important for you. Ω