BLINN.COMmunications
1 April 2022
179 Caren Avenue • Worthington • Ohio 43085-2520 • 718.577.1054 (NYC) • 614.785.9359 (Ohio)

Reasons to Use a VPN or Not to Use a VPN

Security experts stress the importance of using a virtual private network (VPN) all the time. Yes, but ...

A VPN is essential in some cases, helpful in others, and sometimes unimportant or even detrimental.

Anyone whose employer allows working from home should have a VPN that's provided by the employer, and employers who are serious about security will both require a VPN and install one on the company-owned computer that the employee will use at home.

Additionally, the company will not allow the employee to use the work computer for non-business tasks or to install software on it. That's not the point of this article, though. Instead, let's consider your personal devices such as home computers, tablets, and your mobile phone.

A virtual private network will obscure the information flowing to and from your computer, but it's not a perfect security solution.

When VPNs are Essential

Any device used outside the home should have a VPN.

Without a VPN, important information such as user names and passwords can be captured by someone nearby when you're using a public hot-spot in a restaurant, library, coffee shop, or airport. Fortunately, some mobile service providers include an always-on VPN. If yours does, make sure it's enabled.

But is a VPN important when you're using your computer from home?

Maybe. Without a VPN, your internet service provider can see which websites you visit, when, what you search for, who you send email to, and more. Some ISPs collect this data and sell it to advertisers.

The ISP can see this information even when you use a browser's *private* mode. A VPN encrypts all traffic so the ISP can't see it, and it obscures your IP address that could otherwise be used to build a profile that's useful to advertisers.

My wife and I have dissimilar use cases. She works from home using a company-provided computer that's encrypted and that connects to the corporate network via a VPN. The VPN is essential, and her work computer will not connect to the corporate network without it. I also work from home, but no longer connect to a corporate system.

Our cellular service provider offers a built-in always-on VPN. Previously I had used Nord VPN on the phone, but it interfered with my primary banking application because the virtual private network made it impossible for the bank's system to confirm that the connection was coming from the United States.

Protecting bank and other financial connections is exactly the reason many people use a VPN. Fortunately, the cellular services's VPN doesn't interfere with the bank's app and I've uninstalled Nord VPN from the phone. I retain it on the desktop computer.

Hide Your IP Address

The VPN hides the user's IP address, which makes it more difficult for someone to identify and track you.

With the VPN off, those who know how to examine the computer's external IP address will know that I'm somewhere in or around Columbus. Columbus covers a big area though, and more than 1.6 million people live in the metro area.

The VPN can make it appear that I'm near Chicago, New York City, San Francisco, or Dallas. It could also use an IP address from Spain, Ireland, France, or Australia. This can be helpful for someone who is attempting to view

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.

a website that's not available in the United States, but some sites refuse connections from computers that use a VPN.

Although web browsers have improved their ability to protect users from being tracked across the internet, a VPN will do a better job. By disguising your IP address, it limits (but doesn't remove) the ability of websites to associate your activities to a specific computer.

Encryption provided by a VPN protects data that could be viewed if you use public Wi-Fi access points, but this isn't a consideration for those who use their computers at home with a wired connection to the router or their own private Wi-Fi system. Ideally, a VPN would be added to the router, not to individual devices; but few consumer-grade routers have that capability.

No Free Lunch Today

VPNs offer increased security, but at a cost. Convenience and speed may both suffer.

A VPN will reduce the speed of your internet connection — maybe just a little, but VPN providers differ. If there's one immutable life rule, it's this: *There is no such thing as a free lunch*.

The speed reduction may be nearly undetectable, cutting a 500Mb/s connection to 435Mb/s, but some VPNs can reduce throughput by half. Fortunately, most VPN speed reductions are in the 10-20% range — noticeable, but not a show stopper.

Depending on how your computer is used, even a large speed reduction may be an acceptable trade-off for the increased security.

Better Security, But ...

Keep in mind that a VPN won't protect your login credentials, eliminate malware threats, or defeat social engineering.

Presumably your computer's operating system has a built-in firewall or you've added one, you use a password manager, and you're careful to avoid social engineering ploys.

Having a VPN can lead to a false sense of complacency. While the VPN will offer some protections against being tracked or identified, there are lots of holes in the net.

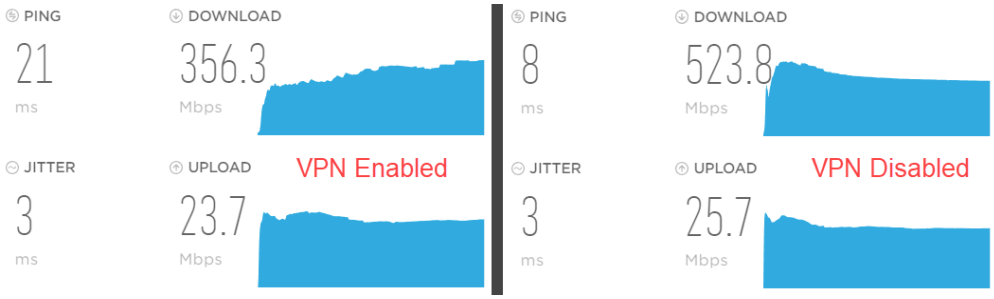
Browser fingerprinting, a technique that captures information from your browser as you wander around the internet, can definitively identify a particular computer nearly 100% of the time with a surprisingly small amount of information.

Not all VPNs are created equal. Nearly all VPN operators say that they log nothing, but some are not being entirely truthful. Free VPNs are the most suspect in this regard. If the VPN you're considering doesn't have a paid subscription option, beware. Some operators of free VPN services collect data about users and sell it.

VPNs increase the amount of data for each connection. This is unimportant for home users unless they have a metered connection, but the increased data usage could hike the cost of your mobile data plan. This increase is usually modest, but can approach 20% depending on the protocol the VPN uses.

Good VPNs are not free. Expect to pay $3 to $4 per month. In many cases, that fee is distributed across all (or some specific number) of your desktop, notebook, and tablet computers as well as any mobile devices you own. It's not a large expense, but it is an expense.

PC Magazine has a well-researched *review of VPNs*. The article examines 19 services and identifies the ones the authors consider to be best.



All VPNs have some detrimental effect on network speed. The effect is usually in the ten to twenty percent range, but can be much more significant.

The *best choices* include Private Internet Access and Nord VPN. I have used Private Internet Access, but switched to Nord about two years ago. One new entry that might be worth looking at is the Mozilla VPN. *PC Magazine* rates it as excellent, but the cost is $10 per month, which is far higher than any competing service. Ω

A New Face

You may notice that this issue of the monthly newsletter looks a bit different. That's because it has a new face.

The typeface selected for any publication affects readability. The face used for this newsletter has been Alegreya 10 on 14 for many years. Starting with this issue, body text is set in Benguiat Pro Book 10 on 14. That's pronounced "ben-GAT", and it was created by graphic designer *Ed Benguiat*, who died in October 2020.

The new face has a taller x-height, which makes it easier to read. This advantage comes at the cost of somewhat fewer letters per line. Although both the old typeface and the new typeface are set at 10 points on 14-point lines, Benguiat Pro Book appears to be larger.

Designers such as Jan White say that the best typography is invisible and never calls attention to itself. I hope that's the case here. Ω