Pull the Shades Down on Your Browsing With a VPN

Did you know that your cruise around the internet every day might not be totally private?

After shopping for a product, you've probably noticed advertising for it pop up later on unrelated websites. And what about the telecom company that pumps in the internet to your household?

Each of your devices has an IP address, a string of characters that identifies where you go on the web.

In an era where online privacy is increasingly under threat, safeguarding your digital security has never been more crucial. Virtual private networks (VPNs) have emerged as a powerful tool for individuals seeking to protect their sensitive data, maintain anonymity, and fortify their cybersecurity defenses. While Metro already provides secure methods of getting to Metro managed assets and the internet, using a VPN might make reduce your personal risk. This month's newsletter explores the key reasons why using a VPN is essential in today's interconnected world.

What to know about VPNs

VPN stands for virtual private network. VPNs encrypt data from your computers and devices to the internet by rerouting it to a private computer server. This masks your location and hides your IP address from websites. VPNs also reduce the risks of using public Wi-Fi by acting as an encrypted middle-ground between your device and the internet router.

VPNs can be either software or hardware. Hardware VPNs (sometimes called VPN routers or VPN firewalls) are physical devices you connect to your computer, while software VPNs are apps or programs you install on your device. Because of their expense, size, and technical requirements, hardware VPNs are more commonly found in business settings, while you probably will opt for a software VPN for remote work or personal use.

Should you use a VPN?

Fortunately, most of the websites you use are probably encrypted – you can tell because the web address uses an HTTPS connection as its first four letters. Unencrypted web pages used to be a major reason to use a VPN, but since now most of the websites you visit, from social media networks to your bank to most top-ranked search results, use HTTPS, that isn't as much of an issue.

Still, a VPN can create a very useful barrier between your device and the internet connection. This becomes especially important if you are traveling and connect to public Wi-Fi. Nowadays, a VPN alone cannot mask your web activity from everyone – a VPN won't keep you anonymous if you log into a website via your Google or Microsoft account, for example.

A VPN prevents your internet service provider (i.e., the company that sells your internet access) from tracking your specific journey on the internet, although they can still gather some data, like the fact that you're connected to a VPN. Using a VPN is great from a privacy perspective because ISPs have a history of handing your data over to others, like selling it to marketers so they can target ads. Some people opt for VPNs because they can help them access content on streaming platforms that might be blocked in their area, or VPNs can bypass internet censorship in some countries.

Of course, a VPN can see what you do on its network. That's why you should compare options and read through the VPN's terms of service to see what sort of data they log, if any. Look up reviews and ask your tech-savvy friends for advice. Generally, a free or very cheap VPN isn't a good choice because you are trusting them with all your internet activity data.

PROTECT YOURSELF WHILE OUT AND ABOUT

To summarize, we recommend using a quality VPN as another layer of security for your digital life, especially if you ever use public or unsecured Wi-Fi networks. However, remember that a VPN is not a cybersecurity silver bullet that will replace antivirus programs, password managers, or enabling multi-factor authentication.

How to choose a VPN

When comparing VPN options, read expert reviews and the terms of service. You want to ensure that the VPN treats your data as sacrosanct. And a free or shady VPN might be worse than not using a VPN at all.

Here are some other factors to consider when in the market for a VPN:

- Security and encryption infrastructure
- Speed and performance
- Privacy and data logging policy
- Server locations and network size
- Compatibility and features
- Customer support and reviews
- Price

While we don't supply recommendations on specific VPNs, you can look up quality reviews at outlets including *Consumer Reports*, *Tom's Guide*, *CNET*, and *Wired*.

How to use a VPN

Setting up a software VPN is straightforward for most computers and smart devices. Generally, here are the steps to follow:

1. Download and install the VPN program on your device. Make sure you are downloading the program from the legitimate vendor.
2. Create an account and sign in – turn on multi-factor authentication to keep your login credentials very safe.
3. Within the VPN program, select a server location based on your needs.
4. Connect to the VPN. Enjoy secure and private browsing!

VPN tips and tricks

While you're surfing privately on your VPN, here are some extra credit tips for optimizing it:

- Flip on your VPN's "kill switch" feature to prevent data leaks if the VPN connection drops. The kill switch will disconnect your device from the internet if you lose your VPN connection.
- "Split tunneling" allows you to route some web traffic through the VPN and some through your regular network simultaneously. This is useful if a VPN is too slow for some uses (gaming, for example) or you're prevented from accessing certain websites through a VPN. This way, you can use a VPN for internet activities you want to keep protected, like banking or email.
- Use a DNS leak test to check if your DNS requests are exposed. This will show if any of your web activity isn't being correctly routed through your VPN.
- Test the performance of your VPN using a speed test. Then you can tell if it is working as advertised.

How to troubleshoot a VPN

Because most or all of your internet use moves through your VPN tunnel, you want to respond to problems ASAP. If these tips don't seem to help or you can't find a solution here, contact the VPN company directly.

My VPN connection fails or drops frequently

If your VPN is fluttery or dropping often, check your internet connection, firewall settings, and server status. It might also help to switch to another protocol or server through the VPN.

My internet is too slow when my VPN is on

Encrypting and decrypting your web activity takes time, but most current VPNs should not noticeably impact most of your browsing activities. If your internet is moving at a snail's pace with your VPN turned on, select a server that is closer geographically or less crowded. Reducing the encryption level might help, and you might want to think about setting up split tunneling. Also, disable background apps that consume bandwidth.

My VPN doesn't unblock geo-restricted content

If you have trouble accessing content using a VPN, clear the browser cache and cookies first. It might help to change your device's time zone, too.

My VPN causes errors or crashes my device

Make sure your device and your VPN are running the latest updates – it's a good idea to turn on automatic updates. If this doesn't work, try to uninstall and reinstall the VPN software. If you are still having trouble at this point, you should contact the VPN provider for support.

VPNs allow for very private netsurfing

Using a VPN increases your safety online and peace of mind, especially when traveling or using a public Wi-Fi network. Metro already provides secure methods of getting to Metro assets remotely, but you should think about using VPN for personal use.
