Online safety – why is a VPN important?

While we are all using our computers and digital devices more as we spend more time at home, it is essential to know how to keep your online activities safe.

A virtual private network (VPN) can link tA virtual private network (VPN) can link the user to an overseas server—in the UK for example https://surfshark.com/servers/uk. A VPN is especially important during times of quarantine and social distancing of the Covid-19 pandemic.

In fact, according to this CNET piece, the demand for commercial VPNs "is surging following work-from-home trends." VPN providers and ISPs are struggling to handle a huge increase in internet traffic around the world. Even before the pandemic "VPN use was already projected to grow exponentially."

But, says CNET, "with new growth comes new risks." Those risks are increasing targets of opportunity as telecommuters and on-line students crowd cyberspace—many in the open and unprotected from snoopers, spies, and perpetrators of man-in-the-middle (MITM) attacks.

How a VPN Keeps Stay-at-Home Users Safer

Browsers are vulnerable.

A web browser has inherent security and privacy vulnerabilities. To work efficiently, it must record everything about the user from the brand of computer to a list of every website visited and every email sent. Accordingly,

the browser is the ideal resource for outsiders to:

- monitor, gather, and sell all the user's browsing activity to marketers
- reveal the user's location to anyone wishing to track online activity
- send poisoned links, hidden bots, and destructive viruses

A VPN defends against all that by making the user's browser a hidden (and moving) target.

MITM attacks are clever and costly.

Nowadays with the proliferation of public Wi-Fi hotspots, a VPN is even more vital. Practicing social distancing in a coffee shop and logging on to an unprotected public network is the perfect setup for a MITM attack. MITM attackers employ the following tactics:

- surveillance as benign as stealing tracker cookies, or as intrusive as recording everything the user does and everywhere the user goes on the web
- malware downloads from compromised websites that invade the victim's system
- live interference between the user and a third party. Example: The MITM detects banking activity and spoofs a warning message from the bank: "You need to change your password immediately before we proceed."
- planting malware for future tracking and vulnerability detection
- fake local networks or bogus websites with an authentic-looking brand logo— Once the victim is in, the hacker owns, can use, or can sell the user's credentials and identity.

Public web users can protect their privacy with a VPN connection. Hackers and spies see only the gibberish of encryption go elsewhere for easier targets.

What a VPN Does

In addition to encryption, a VPN helps protect the user's privacy by:

- masking the user's IP address
- defeating geo-blocking—The rerouting of a VPN connection allows the user to sign on to websites that would ordinarily be restricted to local users only; for example, Netflix local programming, lower customer pricing—products, tickets, and services— for local area customers, etc.
- bypassing net censorship. A government might want to prevent its citizens from accessing controversial or politically unflattering web sites. A VPN bypasses net censorship.

(Read more on how VPN defeats geo-blocking later on in this blog.)

A Cautionary Note

VPN's do not provide protection against malware and viruses. While premium VPN services use encryption protocols and security features, they do not provide full protection against virus infection through phishing or links at unsecured web sites.

For example, a VPN will never prevent a user from downloading a cleverly concealed bot or virus program from an insecure website. A VPN also is no guarantee against compromising a password.

A VPN, then, is an invisible mobile shield. It hides the user's IP address and actual login location. In a toolkit of online safety measures, a VPN can be more insurance along with up-to-date malware protection, a solid password strategy, and other commonsense security practices.

Extra Security for Bitcoin Miners and Traders

For those who are into Bitcoin mining and trading and need an extra level of security, a VPN provides greater security. While blockchain encrypted technology provides a distributed secure ledger to safeguard bitcoin owners, access keys to individual user accounts have been stolen through phishing and bot injections. A VPN is the best insurance against Bitcoin theft. It adds another layer of anonymity and hides the owner's connection.

Free VPNs Vs. Premium Services

Free VPNs can be costly in terms of security and privacy.

Free VPN services have proliferated the marketplace. Even the best free products are but shrunken versions of premium products. There are even some free VPN products that should be avoided altogether.

The reality is that free VPN providers must cover their costs and turn a profit. They cover costs and generate income through a variety of legal, but often shady tools and tricks. Instead of charging users a monthly fee, some free VPN services employ revenue-raising tactics. Those practices can actually exploit their users. In some cases, the user could actually be less secure. For example:

- **Free VPNs track the user's online activity**—One study by VPN Mentor revealed that over 70% of free VPNs used embedded trackers to monitor the user's web activity.
- **Free VPNs sell the user data they collect to marketers**—Amazon, Google and others have made millions selling anonymous user data to marketers and advertisers. Free VPN providers have gotten in on that action. They do it by tracking their users and harvesting data logged through their VPN servers.
- **Free VPNs often slow down an internet connection**—Free

VPN providers typically allocate the majority of bandwidth to paying customers and less to nonpaying customers, whose VPN connection is squeezed through a narrower bandwidth. Less bandwidth means slower web browser performance.

- **Free VPNs load intrusive ads.** Since free VPNs are supported by advertising, their trackers generate tailored ad popups. Those popup ads also slow browser performance. Loading in the background, the ads jump on the screen frequently provide an unsatisfactory and slower user experience.
- **Free VPNs provide a tempting secondary target for hackers.** VPN Mentor has reported that free VPNs are more likely to contain malware than premium services. The ads and image files loaded into free VPN services can contain hidden malware, which hides in plain sight. When the user clicks on an ad or link, the malware or adware begins its dirty work.

Premium VPNs are a better choice.

For a low monthly subscription cost, a premium VPN service provides the following advantages over free VPNs:

- a “no-logs” policy that ensures that the user is never tracked online—With no connection nor activity logs, there is nothing to sell to marketers or provide to government officials—even when backed up by a subpoena.
- best-in-class 256-bit encryption—It is impossible to break or brute-force 256-bit encryption with any computer now available to the public.
- a “kill switch” to close a user’s connection is the VPN server disconnects—A premium VPN service prevents data leakage.
- Premium service extras to block ads, trackers, phishing, and malware attempts.
- Guaranteed effective geo-blocking—A U.S. user could log into a UK VPN server and access streaming services

denied to outsiders.

A premium VPN can thwart internet censorship.

As previously discussed, geo-blocking occurs when some country restrictions involving copyrights, or simply political censorship block out local users. **A premium VPN is especially effective in circumventing geographical restrictions**, which:

- **block entertainment streaming services to users signing in from outside servers**—For example, popular streaming services like Netflix vary program availability from region to region. So, what is available in the U.S. is not always available in the U.K., and vice versa. A VPN bypasses those restrictions.
- **practice unfair pricing**—Some vendors employ geo-blocking to charge higher prices to more affluent customers. Logging into a local VPN server provides access to local pricing and discounts.
- **employ differential ticket and traveler travelers**—Airlines and ticketing companies, auto rental agencies, and hotels will display a variety of prices for the same trip, depending on the customer's sign-in location. Smart travelers can use a VPN server at the travel destination to begin comparison shopping.

Summary and Conclusions

A reliable premium VPN is an important security and privacy tool during pandemics and user quarantines like the COVID-19. With increased web traffic, security threats have grown exponentially.

A premium VPN is encrypted and secure. It hides the user's location and by masking the ISP address and routing the encrypted connection to another location.

VPNs, are not malware or virus hunters. Using a VPN as part of an overall cybersecurity strategy in tandem with commercial-

grade anti-virus programs. A VPN can provide additional insurance against cyber threats. A VPN will, however, protect a user from a man-in-the-middle attack on an unsecured Wi-Fi network.

The best option when choosing a VPN is a premium service. Free VPNs often contain intrusive ads and other performance disadvantages. Premium VPNs, on the other hand, guarantee privacy with a “no-logs” policy, which keeps no records of the user’s online activity.

VPNs, however, are not virus hunters. Use a VPN as part of an overall cybersecurity strategy. A VPN will, however, hide a user from a man-in-the-middle attack on an unsecured Wi-Fi network. A VPN is also another security safeguard for Bitcoin miners and traders.

When choosing a VPN, the best option is a premium service. Free VPNs frequently come with intrusive, performance-crippling ads and other disadvantages. Premium VPNs, on the other hand, ensure complete privacy with a “no-logs” policy where the user can never be tracked. Finally, use a premium VPN to bypass net censorship and geo-blocking.

Sponsored post