(Approx. 1,022 Words)

What Is a VPN, and Do I Need One?

By Joel Ewing, President, Bella Vista Computer Club

March 2021 issue, *Bits & Bytes*

www.bvcomputerclub.org

president (at) bvcomputerclub.org

VPN stands for Virtual Private Network. When your computer or mobile device uses a connection to a VPN service, your device behaves as if it were connected to the Internet at the remote VPN service location, and all your traffic on the Internet appears to others as if it originates at that remote location.

In actuality, the Internet service to which you are physically connected is used to establish a secure encrypted connection to your remote VPN service over the Internet. While the VPN service connection is active, your device is configured to reject any other direct network connections, so all inbound and outbound data flows through that encrypted VPN "tunnel" to the VPN server. The VPN server then establishes the final part of the path to the data's intended destination. Data that needs to be returned to your device flows over the Internet to the VPN server and then passes hidden over the VPN tunnel back to your device.

The logical behavior from the viewpoint of your device is as if your device were directly connected to the Internet through an Ethernet cable at the remote VPN server location. Your device is even assigned a LAN IP address on the remote site LAN. Others on the Local Area Network to which your device has physical attachment will be unable to establish connections in or out to your device while the VPN connection is active, and anyone seeing your data traffic either on your physical LAN or as it passes through any routers and the associated Internet Service Provider, will only see that you are communicating with your VPN service and be unable to read the encrypted data content. Note that if you are communicating insecurely with some website (like http vs. https), your communications will still be vulnerable on the Internet between the VPN Service and the destination website.

Reason for Using a VPN

Businesses that allow employees to work from remote locations may host their own VPN service to allow employees to access corporate network resources securely from a remote location. Suitable restrictions and conventions must be in place to ensure that devices that are not under direct corporate control that connects to the corporate network through VPN are suitably protected so they can't introduce malware into the corporate network.

People who do not use a corporate VPN service to work remotely use a VPN service, not to access resources in the remote network, but to use the remote network merely as a gateway to connect back to the Internet.

If you choose to utilize insecure public Wi-Fi connections with your devices, then by default, anyone else connected to that same Wi-Fi LAN could potentially observe your data traffic, see what Internet sites you are contacting, and observe any un-encrypted data coming from or to your device. If the Wi-Fi network is compromised or misconfigured and there are any security flaws in your device vulnerable to network attacks, your device could also become compromised by malware. The use of a VPN greatly reduces the risks. If your device immediately enters VPN mode upon connecting to a public Wi-Fi, then attacks from other devices on the same local network are blocked, and the most someone else will be able to observe locally about your activity is that you are communicating with and sending unknown data to some specific VPN server.

If you are planning on traveling to a foreign country, you will probably discover that your email services block direct access from a foreign country to reduce spam abuse and that your favorite streaming services have region-specific content restrictions. If you have a VPN Service, you can circumvent those problems by using a VPN server in this country to make it appear you are still in-country, so normal email and streaming services still work. If you have a legitimate need to access foreign-only content, or perhaps a need to verify that some service is indeed blocked in a foreign county, then you can deliberately choose to connect to one of the servers your VPN service provides that is located in a foreign country.

If you are accessing the Internet in a country under an authoritarian government that regards visiting some Internet sites as unacceptable, a VPN service could be part of a means to disguise unacceptable behavior; but under those circumstances, more than just a VPN may be required, as any obvious use of a VPN service could by itself be regarded as an intent to violate restrictions.

Available VPN Services

A search for "VPN services" will locate the most popular services. You may even locate some free services, but I would not be inclined to trust them. Remember that whoever is running the VPN service is the one who CAN observe all the Internet sites you are actually connecting to and any data you might send in un-encrypted form, and they have to fund their service somehow. That would have to be either by data mining for advertisers or restricting service in some way to encourage you to move to a paid plan.

Avast currently provides Avast SecureLine VPN service at an introductory rate of $3.99 / month or $47.88 for the first year (it looks like their regular price is $89.99/year). Their service supports Windows, Mac, Android, and iOS devices on five devices concurrently.

NordVPN is a very popular service, currently available for a 2-year introductory offer of $3.71/month, $89.00 /2- years. Their regular price appears to be $143.40 / year, making them much pricier down the road, but NordVPN also supports Linux operating systems and allows use on up to 6 devices concurrently.

Unlike an email service or an ISP service, which are a pain to change, changing a VPN service should be simple -- no identity change to communicate to others. Perhaps the best strategy is to use one VPN service provider until their introductory rate expires and then shop for the best offer available at that time.

*Caveat Utilitor*