VPN: Virtual Private Networking

To all;

At last night’s computer club meeting, several people asked what are Virtual Private Networks (VPN) and are they worth getting. Below is a link to a good explanatory article on the subject.

First, some background:

Intercepting Wi-Fi communications for later decryption - it's a modern day version of the WWII saga of the Enigma machine & cracking the German code, except that the bad guys are often doing the cracking today.

Using Point-to-Point Tunneling Protocol (PPTP), which is the standard VPN tech from about 10-15 years ago has holes and it’s been cracked. Someone could crack a VPN encryption with about 1 day of compute effort now. That would get them the keys to log into the VPN themselves and/or decrypt your communications. Here is some additional information for people trying to choose a VPC provider

Not all VPN's are created equal.

There are many different ways to encrypt your data, just like there are different technologies for setting up VPN and encrypted communication. Some are better than others. Some methods are obsolete, but still in use.

One of these is PPTP. The first line of the Wikipedia article on PPTP (https://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol) reads, as of April 2017:

The Point-to-Point Tunneling Protocol (PPTP) is an obsolete method for implementing Virtual Private Networks, with many known security issues."

Would you want this protocol protecting your data? If not, then you shouldn't use PPTP. Some people still do. The advantage of PPTP is that it's widely available and uses little CPU power, so it works easily on smart phones. It's also built into Windows 10 (how convenient).

However, this ease of use comes with a false sense of security. If you connect to public Wi-Fi and use a PPTP VPN for security, a bad actor could intercept and record your encrypted communications, and within a couple of days decrypt them, along with the password used to access the VPN. The bad actor could then access your VPN account or snoop your transmissions. The bad actor could be a smart high school student with too much time and a laptop.

I recommend a more modern implementation, such as OpenVPN or L2TP/IPSec. These are more difficult to set up, but provide more robust and verifiable protection. The protection isn't perfect – note, there are rumors that the NSA tried to mess with IPSec and insert backdoors. However, now the bad actor needs the resources of the NSA or similar, rather than the easily hackable PPTP versions mentioned above.

Please note you still have to decide which VPN service to use and to also decide how much you are willing to pay for this service (monthly, yearly, or lifetime).

An ISP is your Internet Service Provider, like Cox.

Link to website with the article discussed above is as follows:

https://newsletter.askleo.com/ask-leo-648-vpn-protect/

Bob