Willow Valley Computer Club

September 2024 | Newsletter | Volume 25, Issue 4

Programs are at 2:00 pm the first Thursday of the month (except July-August) in the Cultural Center unless otherwise noted.

Computer Club Leadership

- President: Al Williams
- Vice President: Dick Beidleman
- Secretary: Paula Sandridge
- Treasurer: Lee Wermuth
- Previous President: Sid Paskowitz

Committee Chairpersons

- Club Website: Paula Sandridge
- Computer Room: Lee Wermuth
- Information Central: Sid Paskowitz
- Newsletter: Mike Pancione
- Program: Dick Beidleman
- Publicity: Bill Adams
- SmartLife: Al Fulvio
- Training: Bill Skelly

Director

- CCTC: John Santora

Advisors

- Bruce Mawson
- Tony Poulos
- Bob Scala
- Cathy Thorn

President's Pen *by Al Williams*

Welcome to the Computer Club's September Newsletter!

It's becoming even more evident from the news that scammers deliberately target those over 60 years old. That's because seniors have accumulated more money. Be careful! Don't respond to or click on links in unexpected emails. If you see an alert on your computer that your computer has malicious malware, don't call that phone number! If you receive a receipt in an email supposedly from PayPal, don't google PayPal Customer Service – scammers have websites that appear in Google searches! Go to PayPal.com for help instead. Be skeptical – scammers are constantly finding new ways to scam!

If you would like assistance, go to our website, *wvcomputerclub.org*, click Get Help, and contact one of our volunteers who helps with scams.

We've received requests for VPN information! In this newsletter, we've reprinted the recent VPN article. Elsewhere in this issue, you'll find our VPN recommendations.

Monthly Programs
1st Thursdays at 2:00 pm
Cultural Center Theater

What Is a VPN? Why Would I Need One?

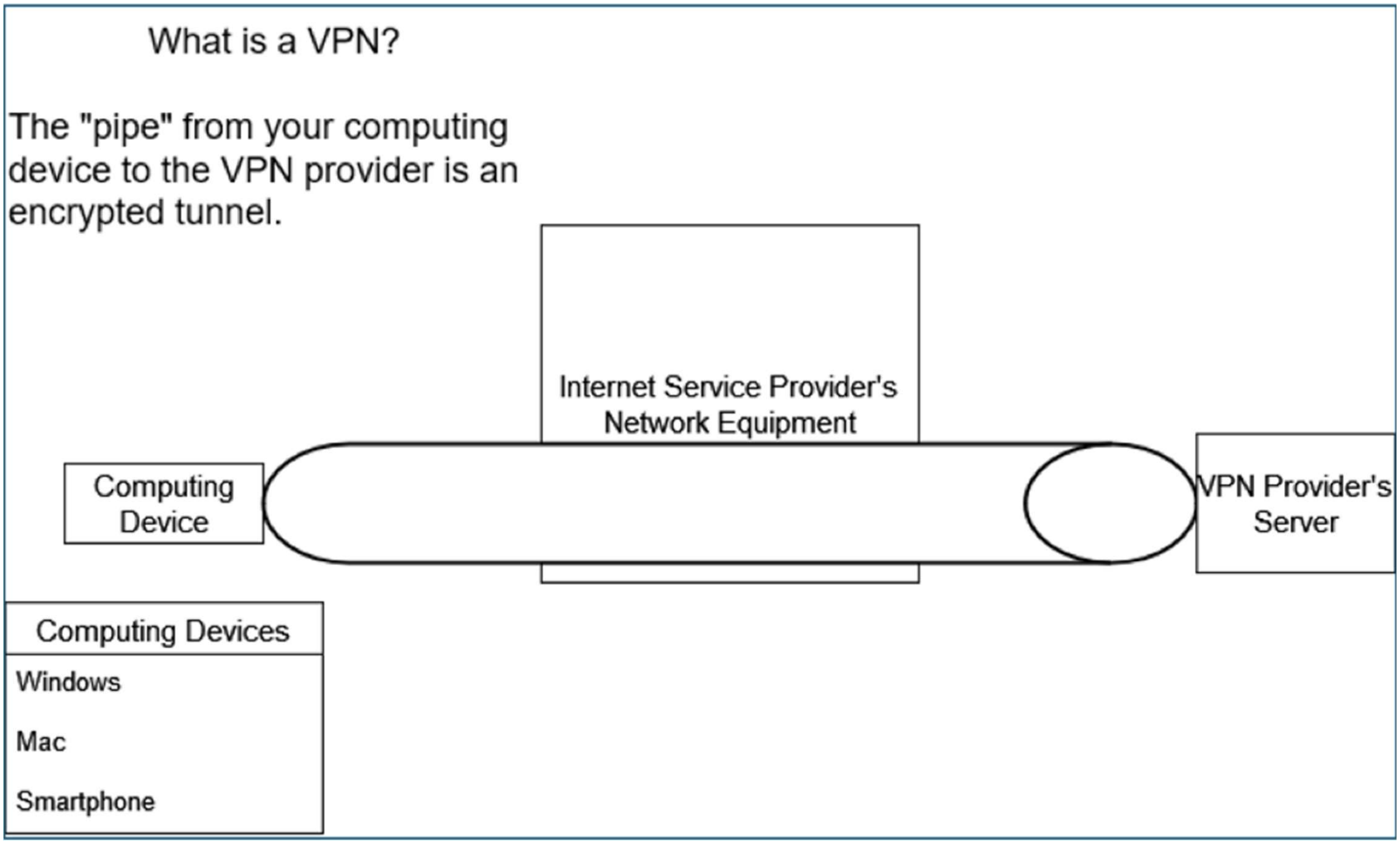
by Al Williams

You may have seen an ad on TV claiming that you need a Virtual Private Network (VPN) right now! But why would you need one? What does it do for you?

Some of the advertisements claim that a VPN gives you anonymity. As the claim is stated in most ads, it isn't true because it is misleading. I'll explain why.

A VPN can be beneficial. Individuals may use a VPN at home or while traveling. Unfortunately, different names are used for the various types of VPNs. As a user at home, you'll be interested in a Personal VPN. When using a VPN away from home, it is called a Remote Access VPN.

Personal VPN
A Personal VPN provides an encrypted tunnel between your computing device and one of the VPN provider's servers. The tunnel is created by software on your computing device. The tunnel starts at your device and goes through all network equipment, including your Internet Service Provider's, to a VPN provider's server. Typically, all your browser, email, and other Internet communications go through the encrypted tunnel and come out onto the Internet. Still, you can choose which will go through the tunnel. See the tunnel in the figure below.


What is a VPN?
The "pipe" from your computing device to the VPN provider is an encrypted tunnel.
Internet Service Provider's Network Equipment
Computing Device
VPN Provider's Server
Computing Devices
Windows
Mac
Smartphone

Personal VPN and ISP Data Collection
Why would you want to use a VPN at home? A VPN prevents Internet Service Providers (ISPs) from monitoring your communications, which ISPs may legally do in the U.S.A. Some ISPs collect information about you and sell it to data brokers. Why would you care? According to the Federal Trade Commission's *A Look at What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers* (https://www.ftc.gov/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers). The report identifies data collection by many ISPs including:

- Home security and automation
- Video streaming
- Content creation
- Advertising
- Email
- Search activity
- Wearables, and
- Connected cars

Several ISPs gather and use data in ways consumers do not expect that could cause harm, including:

- Browsing information
- TV viewing history (through the TV's collection of information)
- Contents of email and search (not if the email is encrypted, which is normal)
- Data from connected devices (Refrigerators, thermostats, etc.)
- Location
- Race and ethnicity

This information, plus information from data brokers, allows ISPs to draw particular insights and inferences about subscribers, families, and households.

Personal VPN and Anonymity
Because a VPN tunnel is encrypted, the ISP cannot read communications through the tunnel or monitor which websites you use. However, the ISP can see that your computing device is connected to that VPN provider's server because of how the Internet works.

Because the ISP knows that you are connected to a VPN provider's server, you are not anonymous to the ISP. Because the VPN provider knows that you are using their server, you are not anonymous to them. However, you are anonymous to anyone observing your communications from or into the VPN provider's server.

Please note that no network that supports anonymity can protect you from *browser fingerprinting*. All browsers must provide information about themselves, the operating system you use, the screen size (monitor) you use, and the rendering engine the browser supports so the website's information can be displayed correctly on your screen. The more unique this information is, the easier it is to identify you. Therefore, when you access a website without logging in, the website may be able to identify you. Of course, when you log into a website, they know who you are.

Personal VPN Considerations
A primary consideration when using a VPN at home is that you could have problems accessing your email. If you access your email using a browser such as Firefox or Chrome, you will not have a problem. However, if you use an app such as Mail, Outlook, or Thunderbird to access your email, you may encounter a problem.

Email providers know your computer's IP address, which is also the IP address associated with your email app. That IP address is tied to a geographical location, such as Lancaster, PA. For example, if you connect to Gmail while using your VPN, your computing device and email app will appear far from home. Gmail will then flag your email activity as highly suspicious. You would then have to work with Gmail to restore email access.

Any ISP can read any email's *To*, *From*, and *Subject* fields. However, an ISP cannot read the contents of an encrypted email. Therefore, if the VPN provider supports *split tunneling*, you could configure the VPN to send all communications through the encrypted tunnel except email, which avoids the apparent geolocation change.

Another consideration is the degree of anonymity usually provided by a VPN. An organization with significant capabilities (a nation-state actor) could correlate traffic from your home IP address with the provider's server traffic to identify your traffic while using the VPN. If you want to reduce the likelihood of that correlation, you could use a feature such as Secure Core, which is available through Proton VPN, to route the output of the provided server to another provided server in a different physical location. Because it is improbable that an observer can see what other server is being used, communications through the second server would likely be anonymous. To restate, that anonymity would be because observers monitoring the output of the second server would not know your "home" IP address.

Remote Access VPN
A user using a remote access VPN may use their home computer while traveling. Two types of VPNs support remote access: hub-and-spoke and mesh.

Although the typical mesh VPN is challenging to set up, providers such as *Tailscale* and *ZeroTier* offer mesh VPNs that are easily configured—more easily configured than a hub-and-spoke VPN.

I use and am familiar with *Tailscale*. When *Tailscale* is installed on your computing devices, you may access them, including your computers at home, from your traveling computer using a *Remote Desktop Protocol (RDP)* application. This gives you complete access to your computers. Although *RDP* is not encrypted, *Tailscale* protects RDP communications because it encrypts all traffic in the mesh VPN.

A consideration when using a VPN while traveling is VPN blockage. Some organizations block any VPN traffic on their networks. For example, according to Heidi Mitchell's *How Secure Is an Airplane's Wi-Fi?* article in the March 18, 2024, issue of the *Wall Street Journal*, the Wi-Fi service on a plane may not work smoothly or allow a VPN to function.

Final VPN Considerations
The final VPN consideration is choosing personal and remote access VPN providers. First, is it essential that the VPN provider will not reveal your identity? Many VPN providers claim that they will not, but the laws of their country will override any such claims. Second, does the VPN provider provide consistent and reliable service? If you want guidance, I recommend Proton VPN for a personal VPN. They are reliable, and they offer free and paid plans. Also, Swiss law guarantees that Proton VPN cannot be forced to reveal your identity.

I recommend *Tailscale* for the remote access VPN. They offer a free plan that should meet your needs.

Conclusion
In conclusion, while VPNs may provide some level of anonymity, they are most effective and are recommended for protecting personal information from ISPs.

WVCC mission: "to provide the means to educate beginners or interested non-users on how to use a computer"

WVCC mission: "to provide a forum for interchange of computer information among members"

WVCC mission: "to arrange for speakers to talk about subjects of interest to those with some background and experience in computer use"

Computer Club Technology Center

NOTE: The Computer Club Technology Center (CCTC) is open on Mondays only, from 10 am to 4 pm. The CCTC is located on the 5th floor of Manor North ‘J ’building. The door may be closed, but with a sign indicating *Please Knock.*

Apple Items Available: See Bruce Thompson in the CCTC. ♻

VPN Recommendations

Do you want to use a VPN after reading the article in this newsletter? Here are features I recommend:

- It should have a kill switch
- It should block tracking
- It should provide in-tunnel DNS
- It should support simultaneous connections
- It should use open-source protocols and encryption algorithms

Proton VPN is a great choice!

For explanations of the above terms, see https://www.howtogeek.com/i-wont-use-a-vpn-without-these-features/

Club Officers 2024-2026

Our officers for 2024-2026!

Al Williams ~ President
Dick Beidleman and Bob Schaffer ~ Co-Vice-Presidents
Lee Wermuth ~ Treasurer
Paula Sandridge ~ Secretary

We thank you for your willingness to serve the club membership!

Willow Valley Computer Club
Volunteer Opportunity

Volunteer Position Title: Deputy CCTC Director

Description of Role: The Deputy CCTC Director assists the CCTC Director as needed to accomplish the objectives set forth by the Willow Valley Computer Club’s Executive Committee.

Training: The CCTC Director will provide training as needed for the Deputy CCTC Director to successfully accomplish their assignments.

Reporting: The Deputy CCTC Director will report to the CCTC Director.

Time Commitment: A minimum of four hours per week is needed. The candidate must be able to work during hours acceptable to the CCTC Director

Qualifications: Prior operations experience is desirable. A willingness to learn is imperative.

Contact Information

For more information about the Computer Club, please contact Al Williams via email at wvcomputerclub@gmail.com.

Please keep your email address on Club records current so we can send you important emails. Send email corrections or updates to Lee Wermuth at lwermuth582@gmail.com.

Bill Skelly is the Willow Valley Computer Club Training Coordinator. We are always looking for residents qualified to teach computer-related topics. We want our classes to support your needs. Contact Bill (whskelly@aol.com) to volunteer or to offer ideas on topics needed.