$3.00 (membership includes monthly subscription)

The Digital Viking

Twin Cities PC USER GROUP NEWSLETTER

Minneapolis & St. Paul, Minnesota USA • Vol. 40 No.7• Feb. 2020

*TC/PC Exists to Facilitate and Encourage the Cooperative Exchange of PC Knowledge and Information Across All Levels of Experience*

**February 2020**



# General Meeting
## Tuesday, Feb. 11, 2020
## 7:00 PM

### Installation, Care, and Feeding of a Mesh Router

**Summit Place**
**8505 Flying Cloud Drive**
**Eden Prairie, MN**

Greg Skalka, President of the Under the Computer Hood User Group in California and an active member of APCUG, gave this presentation at last fall's Virtual Tech Conference. He walks through the history of WiFi and its current specs and his decision to purchase and install a mesh router to solve dead spots and poor WiFi signals in his home. He is very knowledgeable and does a great job of explaining the technical information. You have probably read some of his articles that have been published in the TC/PC Digital Viking.

**Tech Topics with Jack Ungerleider at 6:00 PM.**
Always lots to learn from our tech guru.

# The Digital Viking

The Digital Viking is the *official monthly publication of the Twin Cities PC User Group, a 501(c)(3)organization and an all-volunteer organization dedicated to users of IBM-compatible computers. Subscriptions are included in membership. We welcome articles and reviews from members.* The Digital Viking is a *copyrighted publication and reproduction of any material is expressly prohibited without permission. Exception: other User Groups may use material if unaltered and credited.*



# Advertising

| | |
|---|---|
| **Full page (7½ x 9½)** | **$100.00** |
| **Two-thirds page (7½ x 6)** | **80.00** |
| **Half page (7½ x 4¾)** | **65.00** |
| **One-third page (7½ x 3)** | **50.00** |
| **Quarter page (3½ x 4¾)** | **40.00** |
| **Member Bus. Card (2 x 3½)** | **10.00** |

***Multiple insertion discounts available.***

Contact Sharon Walbran at:: SQWalbran@yahoo.com

Deadline for ad placement is the 1st of the month prior to publication. All rates are per issue and for digital or camera-ready ads. Typesetting and other services are extra and must be requested in advance of submission deadlines.

Payment must accompany order unless other arrangements are made in advance. Place make checks payable to: **Twin Cities PC User Group**

## TC/PC Member Benefits

**Product previews and demonstrations**

**Special Interest Groups**
**Monthly Newsletter**

**Discounts on products and services**

**Contests and prizes**

## Business Member Benefits

**All of the above PLUS:**

**FREE ½ page ad on payment of each renewal**

**20% discount on all ads Placed in the *Digital Viking* Newsletter**

**Up to 5 newsletters mailed to your site (only a nominal cost for each additional 5 mailed)**

# TC/PC 2019-2020 Board of Directors

Meets once or twice per year. All members welcome to attend.
Visit www.tcpc.com for meeting details.

| | |
|---|---|
| **President** —William Ryder | br@rydereng.com |
| **Vice President** —Curtiss Trout | ctrout@troutreach.com |
| **Secretary** - Sharon Walbran | sharon.walbran@gmail.com |
| **Treasurer** - Sharon Trout | strout@troutreach.com |
| **Newsletter Publisher** Sharon Walbran | 952-925-2726 sharon.walbran@gmail.com |
| **Web Master** Curt Trout | ctrout@troutreach.com |
| Board Members: | |
| Steve Kuhlmey | skuhlmey@hotmail.com |
| Lon Ortner | 612-824-4946 lon@csacomp.com |
| William Ryder | br@rydereng.com |
| Jeannine Sloan | Ambassador for Friendship Village |
| Curtiss Trout | ctrout@troutreach.com |
| Sharon Trout | strout@troutreach.com |
| Jack Ungerleider | jack@jacku.com |
| Sharon Walbran | sharon.walbran@gmail.com |

## Newsletter Staff

**Editor Sharon Walbran**

# My Experience with a subscriber VPN

**Advantages, costs, pitfalls, workarounds**
**Part 1 of a 2-part article series**
**Author: John Krout, Member, Potomac Area Technology and Computer Society (PATACS), www.patacs.org, jkrout75 (at) yahoo.com**

This article is based on a lot of research, several years of use of a corporate VPN at work, and a few months of using a subscriber VPN at home.

VPN is an acronym for Virtual Private Network. The idea is that your use of a VPN provides a secure method of data communication, through strong encryption. The encryption hides the info in your communication, such as content of emails and URLs of web sites, from your Internet Service Provider (ISP) and any other **Man in the Middle**.

**WHY VPNS EXIST**
That phrase Man in the Middle is important. Your communication with your email server or any Web site may pass through half a dozen or more servers in between. For any one of those in-between servers, any bored or underpaid system administrator, and any hacker breaking in, might install message trapping software to capture info passing through, such as your IDs and passwords for your stockbroker or bank. Those snooping activities are called Man in the Middle attacks. Encryption makes it almost impossible for them to make use of that info.

Originally, when local area networks (LANs) first became available, the only networks were inside a single building where all the computers were connected on the local network, with no connection to anything outside the building.
Later, secure direct circuits, and modems, allowed communication between computers on the inside and the outside.

A very entertaining book, **The Cuckoo's Egg**, written by Clifford Stoll, describes the Bad Old Days before VPNs, when networks were insecure. It is a fascinating read. The author, an astronomer, was given the task of tracking down a 75-cent discrepancy in billing for use of a university local area network. His investigation led him to identify peoples who broke into the network. He found the same people also broke into military computers. He tracked the people to Europe, where they were tried and convicted based on his testimony and a huge pile of printed computer logs as physical documentary evidence. Stoll was a good guy in the middle.

Because of experiences like that, corporations and the federal government have used their own VPNs for many years. VPNs have enabled greater automated data movement, ensuring privacy of the data due to the use of strong encryption.
And, now, VPNs are available to the rest of us.

While using a VPN, the encryption is based on two *digital certificates*. The VPN server provides one to your computer, tablet, and smart phone. Additionally, the VPN server itself has another one. The encryption using those two certificates is based on some very creative research done in the early 1980s by three MIT professors, Rivest, Shamir and Adelman, who founded RSA and Verisign, two companies now at the heart of modern digital security efforts.

A second result of the two-certificate approach is that your account is known to be valid by the VPN server, and the VPN server is known to you to be valid as well.
Without using a VPN, web sites and other internet services get access to the internet protocol address (IP address) of your home router, computer, phone or tablet. This is important because

those IP addresses let web sites figure out where you are located. When you use a VPN, the web sites see only the IP address of the VPN server. In this way, a VPN server acts as your proxy, and are sometimes called **Proxy servers**.
Take a look at **Illustration 1**. This shows how a VPN server fits in the overall path of servers between your computer, phone or tablet and the world of the internet. Inevitably, your VPN-

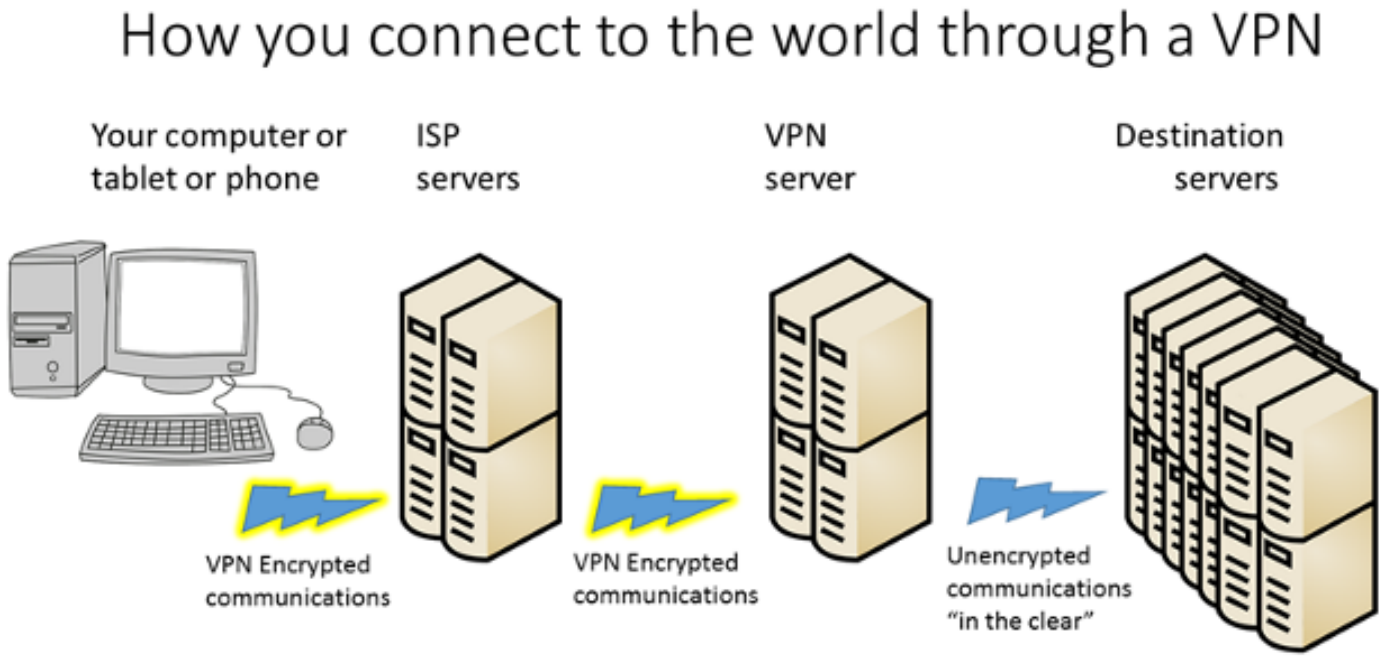



***Illustration 1.***

encrypted communications pass through your ISP servers, and then possibly through other intermediary servers until it reaches the VPN server. Using a VPN server severely limits any snooping not only by your ISP but also by any servers between the ISP servers and your VPN server. So the Man in the Middle is stymied in that part of the path.

Beyond the VPN server, the communication is unencrypted by the VPN, or *in the clear*, and at that point reaches the destination, which might be for instance a video streaming server, or a credit card company's web server. Of course, that leg of the path also involves intermediate servers.

Because that leg of the overall communications path is not depicted as encrypted, you might think that a Man in the Middle attack would succeed there.

However, these days most of those destination servers use HTTP-Secure protocol (https), which also employs encryption done in a different way, by your Web browser and by the destination server. That's right, a second encryption. As a result, the communication remains secure all the way through the entire path.

But I want to digress for a moment and suggest that your ISP might also behave as a Man in the Middle.

When you use a VPN, the fact that the servers of your ISP see only encrypted data is very significant. Your ISP is always in the best position to snoop, effectively a Man in the Middle for all the web sites you browse, the streaming services you use, and so forth. All of your browsing and other use of the Internet goes through those ISP servers.

Your ISP has a strong economic incentive to take advantage of that best position: data on the web sites you visit and the downloads you select can be quite valuable to third parties. And don't think ISPs will ignore that incentive simply because you are a customer of the ISP; the big ISPs convinced the FCC to eliminate Net Neutrality rules so that the ISPs could solicit money from the likes of Netflix and CNN to accelerate delivery of those sites to your computer.
So use of a VPN consistently protects you from snooping by your ISP.

**MORE ADVANTAGES OF A VPN**
I have been using a VPN and HTTPS from my work site for more than a decade. I have seen no significant impact on communications speed. Computers do the encryption and decryption quite quickly these days.

An advantage of subscriber VPN services is that you have access to hundreds or thousands of VPN servers, in many cases spread around the world. If one is busy or down, you can easily use another. Redundancy is a very valuable advantage.
Another advantage is that you can choose a VPN server located in a country where a local web site or video streaming service is of interest to you. For instance, the BBC streaming service is open only to users located in the UK. When the BBC servers detect a request from a US IP address, the servers ignore it. if you use a VPN Proxy server in the UK, the UK IP address of the VPN Proxy server tells the BBC that you are local, and you then get to use that streaming service.

A third advantage is far less clear. According to PC Magazine, many VPN users in the US subscribe specifically because the federal government has eliminated the Net Neutrality rules. The idea is the ISP cannot throttle back what it cannot decrypt, meaning what it cannot recognize. NordVPN, for one example, actively promotes that idea on their company's web site.

I am not convinced that idea is correct.

**COUNT YOUR VPN-READY DEVICES**
Another advantage is that subscriber VPN services let you connect more than one of your devices (computer, phone, tablet) to the VPN *at the same time*. This is important if you use two or more internet-connected devices, like I do. And it is a major convenience factor, allowing you to leave all your devices connected all the time, not just when you actively use each one.

Snoopers can monitor the web browser on your phone or tablet just as readily as they can on your computer. A VPN can and should protect all of those devices.
Several VPN services that I reviewed set a ceiling on the number of concurrent uses by a single account, and that limit varies from 3 to 10.

Because of that, before you select a VPN service, you need to make a realistic assessment of the number of concurrent connections you may need.
For example, in my case: I have two Windows computers, two Android tablets, and one Android smart phone, a total of five devices. My son has a Windows computer, a Linux computer, one android tablet, and one Android smart phone, a total of four devices.
So our grand total is nine.

**COMPARISON SHOPPING FOR VPNS**
When I was shopping for a VPN service, I came across a review of public subscriber VPNs on **TechRadar.com**, published in March 2019. **Illustration 2** is a table comparing the top three VPN services according to TechRadar's ratings system, and some details about them. The number of servers and countries will likely continue to grow for each of the public subscriber VPNs.

| VPN service | # proxy servers | # countries | Ceiling on devices per account |
|---|---|---|---|
| ExpressVPN www.expressvpn.com | 3,000 | 94 | 3 |
| IPvanish www.ipvanish.com | 1,200 | 60 | 10 |
| NordVPN www.nordvpn.com | 5,300 | 60 | 6 |

*Illustration 2.*

The column labeled ceiling of devices per account indicates the ceiling on the number of computers, tablets, and smart phones on which you run the VPN client software simultaneously.

The column labeled # proxy servers is especially valuable for redundancy purposes. If one VPN proxy server happens to be down, or malfunctioning, then you can try many others. Generally, more is better.

Concerning the number of countries, although the overall situation worldwide is improving all the time, to some extent I think there are diminishing returns beyond about 50 countries. This is because smaller countries have fewer localized streaming services, and often do not have high bandwidth connections to the internet, so VPN servers in many smaller cannot work as rapidly as VPN servers in say the US or Canada or western Europe or Japan or South Korea.

I chose to subscribe to the **IPvanish VPN service**. Its ceiling on the number of concurrent connections is 10.That was the most important factor for me.

Later on, I found that VPN services are now so popular that PC Magazine reviews the services and provides Editor's Choice awards, their long-coveted recommendation. In 2019, the Editor's Choice awards went to three VPN services:

TunnelBear (www.tunnelbear.com),
Private Internet Access (www.privateinternetaccess.com),
NordVPN (www.nordvpn.com).

NordVPN was the one service that was top rated by both TechRadar and PC Magazine.

**PRICING**
The VPN services have a monthly rate, usually less than $10, and offer discounts if you pay in advance for say 3 months or for a year. Some even offer further discounts if you pay in advance for three years.

Some VPN services have their business offices outside of the US and may charge your credit card to a bank outside of the US. You may wish to let your credit card company know in advance, so that the charges are not automatically blocked by your card company.

This ends Part 1. In Part 2, you will learn about some difficulties encountered on VPNs, and some workarounds.

ABOUT THE AUTHOR: John Krout is a former president of the Washington Area Computer User Group (WAC), one of two groups that merged to become the Potomac Area Technology and Computer Society (PATACS). He has been writing about personal computer uses since he joined WAC in the early 1980s. He is a frequent contributor to PATACS Posts, and occasionally provides presentations on tech issues at PATACS meetings. He lives in Arlington VA and is a writer for the Thales Group, a major maker of automated fingerprint identification hardware, supporting the use of that hardware in the computer system of a major federal government agency.


---

# My Experience with a subscriber VPN

**Advantages, costs, pitfalls, workarounds**
**Part 2 of a 2-part article series**
**Author: John Krout, Member, Potomac Area Technology and Computer Society (PATACS), www.patacs.org, jkrout75 (at) yahoo.com**

In part 1, you learned about the need for VPNs and how a VPN secures your internet communications. Also Part 1 identified several VPN services that are highly rated, including the one to which I subscribe, IPvanish.

This part explores some of the complications and workarounds that I have encountered.

**REAL LIFE VPN IMPACT**
As of late September 2019, I have a VPN installed on my laptop computer, two tablets, and my smart phone. As was the case at work, the VPN at home does not seem to impose any noticeable slowdown on those devices.

I use my second tablet primarily for its Roku app, which is a remote control for my Roku Premiere video streaming box. When I installed and used the IPvanish VPN app on that backup tablet, the Roku app was no longer able to communicate with the Roku box on my home network.

Why did that happen? The tablet could not search the LAN for the IP address of the Roku box. This may be because the tablet communications were encrypted and our home LAN router was not.

This led me to learn about another aspect of subscriber VPNs.

**SPLIT TUNNELING**
In operation, a VPN connection is sometimes referred to as a *tunnel*. That simply means the communication is hidden by encryption, as if concealed inside a tunnel, and cannot be read or understood by a Man in the Middle.

Split tunneling is a feature of the IPvanish app for Android. Many other VPN services offer split tunneling in their apps.

The idea of split tunneling is that you can configure the VPN client app so that, for example,

communications by a particular app on my tablet or phone should *not* be encrypted, not sent through the "tunnel" to the VPN server. Apps exempted in that way are *split* away from the encryption tunnel.

Split tunneling is configured on an app by app basis. Lucky me, the Android VPN app for iPvanish enables split tunneling, so I told the VPN app to exempt the Roku app. That way, I can use the app to control the Roku box even while the tablet is otherwise connected to the iPvanish VPN.

Later on, I set up split tunneling for the Roku app on my smart phone. At that moment, when I applied the config change to implement the split tunneling, my smart phone VPN app was already connected to the VPN. I learned that for the IPvanish VPN client, it is best to set up split tunneling while the VPN app is *not* yet connected to the VPN. I tried when the VPN client app is connected to the VPN; the VPN client app then told me it had to disconnect and reconnect the VPN in order to implement the config change for split tunneling.

I started thinking about other types of in-home communications on a home Local Area Network. The Internet **of Things (IoT)**, meaning lights and appliances connected to your router, is one example. For a control app to communicate with those devices from a phone or tablet running a VPN client app, the control app would have to be split tunneled.

**LAN PRINTERS AND VPNS**

There is one very widespread present-day LAN use that will require split tunneling: I have my printer connected to my home router, so that computers around the house can print.

The initial issue I have is that the Windows VPN client application from IPvanish does *not* permit split tunneling as of September 2019. The IPvanish help desk says the company is working on adding that feature. So I have to wait for IPvanish to update their Windows VPN client app.

If you choose a different VPN service, and you have a printer connected to the LAN at home, make absolutely sure that their VPN client app for your personal computer supports split tunneling, whether it is a Windows box, a Mac box, a Linux box, or a ChromeOS box.

The second issue is that there are a *huge* number of personal computer applications that can print. Examples include all Microsoft Office applications, all LibreOffice applications, all web browsers, Adobe Acrobat Reader, Notepad, Wordpad, graphics image editors like Adobe Photoshop, general printing applications like PrintMaster (invitations, birthday cards, banners, et cetera), desktop publishing applications, and so forth. It is fairly difficult to identify valuable desktop applications that do *not* include the ability to print.

Because split tunneling is so useful, I am researching other subscriber VPN services and their VPN clients' abilities to support split tunneling. I will report on that in a later article.

**DO NOT SPLIT TUNNEL THAT WEB BROWSER!**

Now, of all the myriad of applications that can print, the one that is most often the target of snooping and therefore most in need of a VPN is a Web browser. Don't set the VPN app to split tunnel that browser.

If you habitually print one or more web pages using your Web browser, there are a couple of ways to work around that problem while connected to a VPN.
The easy case is to connect the computer to the printer using a different method. Most, but not all, printers can be connected to computers by a USB cable.

The two following suggestions are provided in case you cannot do that.

For the special case of downloading and printing PDF files, you can download each PDF using your Web browser. In the VPN client application, apply split tunneling to **Adobe Acrobat Reader**, which is far less risky than applying it to your web browser. Then use Acrobat Reader to load and print the PDFs.

For the more general case, when you need to print Web pages, you can print each Web page through a PDF print driver such as Microsoft Print to PDF or PDFCreator or PDF995. Those drivers create a PDF file instead of sending output to a printer. Then you use the same technique: apply split tunneling to Adobe Acrobat Reader, then use Acrobat Reader to load and print the PDFs to your LAN printer.

Sounds too complicated. But wait, all is not lost.

**A MORE COMPREHENSIVE SOLUTION**

Some VPN services also allow you to install a VPN client on a *home router*. What are the advantages of that approach? First, the router connects all of your devices to the internet via a VPN server, so long as those devices are at home and connected to the home LAN, either by ethernet or by Wi-Fi. Second, the router VPN client will do the work of VPN client encryption and decryption for all of your devices.

Using this approach, your devices at home need not run a VPN client. Effectively, your device count at home, from the viewpoint of your VPN service, is ***one***: the router itself, which handles all VPN encryption and decryption for all your devices. Therefore, the home router must contain a fast CPU and a good amount of RAM and will be expensive.

When all devices use a home router VPN client, your devices at home can communicate with a LAN printer.

When all devices use a home router VPN client, your devices at home can act as the remote control for a Roku box and run an app to control home lights and appliances.

I must say that the installation process for a VPN client on a router is complex and not for newbies. It often involves installing a third-party app called DD-WRT on the router as a prerequisite. I watched a YouTube video of how to do the installation for the NordVPN router client, and the process looked daunting to me.

This strikes me as an opportunity for a **user group lab**: work on the installations together during a user group meeting. It would require you to bring your home router to the lab meeting.

Some VPN services even sell routers with the VPN client pre-installed. I think this is probably the best alternative for most folks who want to use a VPN client on a home router.

IPvanish publishes a list of router makes and models on which their router VPN client is known to be installable and is known to work. The list as of September 2019 includes high-end, expensive Linksys routers, Asus routers, and Netgear routers. I checked out the prices of those routers: the lowest I saw was about $150. With the VPN client pre-installed, the price would increase.

When you are away from your home router, yes, you will still run the VPN client on your phone, tablet or computer. But typically you won't bring your Roku box or printer or your lights and appliances along with you.

**ARE THERE WEB SITES THAT ARE NOT ACCESSIBLE WHEN YOU USE A VPN?**
At some point in 2019, I read an article published in a user group newsletter which briefly described VPNs. The author made a broad claim, without details, that VPNs *prevent use of video streaming services and financial web sites*. The VPN service was not specified, the streaming service was not specified, the financial sites were not specified, and the browser and operating system used by the author were not specified. Perhaps the author was using a home router running a VPN client. Again, no details were provided.

As I was wrapping up this article series, I went looking for that article. I could not find it.
That claim was *questionable*, in my opinion. The traveling public use those sites on the Web all the time while on the go, even overseas. Netflix in particular encourages use by travelers.

More generally, subscriber VPN services address *how* users access the Web, and do not act as content censors. Well, I admit VPNs of some corporations and government agencies block certain types of web content that they deem unrelated to work. And I suspect in some small countries the local banks lobby the government to prohibit access to foreign banks through the Web, a simple protectionism for the local banks.
But that is another big reason why VPNs exist: to enable connections to foreign web sites with powerful security so that government snooping does not know what you are accessing on the Web. The only IP addresses the snoops can see are those of your device and the VPN server.

So, as soon as I got my IPvanish account set up and I got the VPN client app installed on my laptop computer, I started testing access to financial web sites for the accounts I use, my stock brokerage, my credit card banks, and my checking account bank. I also tested watching a video on the Netflix web site.

Here's how I did that test.

First, I connected to an IPvanish VPN server in the Boston Massachusetts area. I accessed all those sites and kept track of what happened.

Second, I connected to an IPvanish VPN server in the London England area. Again, I accessed all those sites and kept track of what happened.

My tests used a Toshiba Satellite laptop running Windows 10, and the Firefox web browser.

The results appear in **Illustration 3 (page 11)**.

In short. I found that Netflix worked, my three-credit card bank web sites worked, my stock brokerage web site worked, and my checking account bank web site worked. That was true even when accessing those through the London England VPN server.
I did learn also that Netflix and my stock brokerage site both require that I enable cookies. I did that. I also have my Firefox browser set so that, when I shut down Firefox, it deletes all cookies that were created by web sites during its current use.

Cookies are one way that snooping is implemented. But there are also good cookies. Cookies are used to "remember" your login ID on various web sites such as email,

Amazon.com, and geocaching.com, so that you need not log in again when you revisit the sites.

Cookies are also central to the way retail shopping and bank transactions are handled in your Web browser.

So the lesson is: set up your browser to allow sites to install cookies, so you can shop and use the bank and stock brokerage sites.

To avoid keeping bad cookies, I set the browser to delete *all* cookies installed during the current Web browser use, when I shut down the browser, after shopping or banking is done. That way I throw out the bad cookies, but I am forced to discard the good cookies too.

And shut down your browser promptly. Don't let it run for days at a time.

The regrettable side effect is that I must log into Yahoo! email, Verizon email, geocaching.com and Amazon.com every time I use the browser to access those sites. I can even checkmark the web site login box saying remember me. The remembrance works until I shut down the web browser and the cookies get purged.
I am willing to live with that side effect.

Is my test a *comprehensive* test? No. I do not have an account for every bank and every stock brokerage in the US. Nor do I have an account with every VPN service. So a comprehensive test is just about impossible.

But I think my test results provide good news. Not every VPN service causes such problems. Not every browser causes such problems. Not every web site experiences such problems.

ABOUT THE AUTHOR: John Krout is a former president of the Washington Area Computer User Group (WAC), one of two groups that merged to become the Potomac Area Technology and Computer Society (PATACS). He has been writing about personal computer uses since he joined WAC in the early 1980s. He is a frequent contributor to PATACS Posts, and occasionally provides presentations on tech issues at PATACS meetings. He lives in Arlington VA and is a writer for the Thales Group, a major maker of automated fingerprint identification hardware, supporting the use of that hardware in the computer system of a major federal government agency.


Go to Page 1

# Thoughts from a Clicker - September

**Author: Tiny Ruisch, Member, Cajun Clickers Computer Club, LA**
**September 2019 issue, CCCC Computer News**
**www.clickers.org, tsa70785 (at) gmail.com**

This month I'd like to tell you about one of my favorite utility programs. I have it installed on all my computers and have been using it for more than ten years. I first reviewed this program in July 2009. The program has gotten even better since then. Like many other free programs, the programmer has a donate button on his website. I like the program so much that I hit the PayPal button a long time ago. Maybe it is about time I gave him a few more dollars.

FileMenu Tools lets you customize the right click menu of Windows Explorer. It also works with all the alternate explorer programs that I've tried. The program adds utilities to perform operations on files and folders and adds customized commands that let you run external applications, copy or move to a specific folder or delete specific file types.

With the built-in commands you can:

- Run With Parameters – Runs a program with parameters you input in a dialog box.
- Command Line From Here – Opens a command line window.
- Copy/Move – No need to cut and paste. You can also use filters in file selection.
- Duplicate Files – Makes a copy in the same folder.
- Pack to Folder - Moves all the selected elements to new sub-folder in the current folder.
- Copy Path/Name/Content - Copies the selected item(s) to the clipboard.
- Attributes – You can view and change them without having to open a properties dialog box.
- Find and Replace – Lets you find or replace a text for all the files in a selected folder.
- Advanced Rename – With lots of options.
- Change Icon – Changes the icon for the selected folder.
- Change Attributes – Quickly and easily change folder options.
- Advanced Delete – Lets you delete specific file types in a folder.
- Synchronize Two Folders – Lets you synchronize two folders quickly and easily.
- Shred Files – Overwrites several times so it is impossible to recover the file in the future.
- Send to Mail Recipient – Lets you send an e-mail with selected elements as attachments.

These are less than half of the FileMenu commands you can select from. In the configuration menu, a simple check will turn off the commands you don't want. If you can't find the FileMenu function you need, then just add a customized command to run external applications, copy/move to a specific folder or delete specific file types.

FileMenu Tools lets you configure the "Send to" sub-menu. You can add new items, change the properties of the existing items or delete them. You also can disable existing "Send to" items in order to hide them from the menu.

FileMenu Tools will also let you enable/disable the commands which are added to the context menu of the Windows Explorer by other programs. This is the only function that is not one hundred percent reliable.

When it works, it works well, but it doesn't catch all the programs that add a right click.

FileMenu Tools is a 12.90 MB download and runs on all Windows platforms. Open Candy is used during the installation process but can be refused with a check mark. Did I mention the price? This program is freeware and costs nothing.

Download FileMenu Tools and give the program a test. I'm pretty sure that you'll like it. While you're on the Lopesoft website, you can also download and test LopeEdit Lite, an excellent alternative to Windows Notepad. Keep on clicking and thanks for reading 💻

Go to Page 1

# Special Interest Groups (SIGs)

w Work phone h Home phone c Cell phone
* Meets at an alternate location

**Most SIGs will meet at Edina Executive Plaza, Conference Room #102, 5200 Willson Road, Edina, MN**
**Confirm with a SIG group if they meet elsewhere.**
**For more info contact the SIG Leader(s) listed here.**

**Get SIG announcements!**
***Link from www.tcpc.com***

### Board of Directors*
All members are welcome! Check www.tcpc.com for location.
**Selected Saturday mornings**

### Linux on Saturday
This is for the Linux newbie and those trying to come over from Microsoft to a different operating system.
**Second Saturday @ 9 AM-Noon**
**Note: No Meetings June-August**

**Jack Ungerleider 612/418-3494 c**
**jack@jacku.com**

### Tech Topics
**Technical presentation/discussion on various technical topics from the following areas:**
- **Web/Internet**
- **Mobile Devices and Apps**
- **Playing with Programming**
- **DIY (3D Printing, R-Pi, other hobby electronics, etc.)**

**Second Tuesday @ 6:00-7:00 PM**
**Every month**
**Right before the general meeting.**

**Jack Ungerleider 612/418-3494 c**
**jack@jacku.com**

### Microsoft Access
All levels. Presentations by expert developers within the group and by MS reps.
**Third Saturday 9:00 AM—Noon**
**Note: No Meetings June-August**

**Steve Kuhlmey 952/934-8492**
**skuhlmey@hotmail.com**

### Microsoft Office
Addresses the use, integration, and nuances of the Microsoft Office applications.
**Combined with Systems on Saturday**
**Third Saturday of the Month**
**9:00 AM—Noon**
**Note: No Meetings June-August**

**Steve Kuhlmey 952/934-8492**
**skuhlmey@hotmail.com**

Directions to **Summit Place** for **General Meetings**:
Proceed to Eden Prairie Center Flying Cloud Drive . [Flying Cloud Drive runs along the West side of the Eden Prairie Center.] Once you have driven past Eden Prairie Center (on the left) along Flying Cloud Drive you will come to a stop light at Prairie Center Drive. The next intersection with a stop light and left turn lane is Fountain Place. Turn left at Fountain Place and go straight into the parking lot. Turn left again to the first covered entry way of Summit Place. There is plenty of parking in the large parking lot in front of the first Summit Place covered entry way. When you enter the door at the first covered entry way, ask to be directed to the Performance Room for the TC/PC meeting. For a map of more detailed directions and ***info on Web SIG and Board meeting***, check the TC/PC website.

Directions to **Edina Executive Plaza** for **Systems on Saturday, Access, Word and Picture Perfect SIGs**: Take Highway 100 to the 50th Street/Vernon exit. [If you have come from the north, cross back over Highway 100 to the east side.] Take the first right and go past Perkins [The golf course will be on your left.] and continue on the east frontage road (Willson Road) to the next building—5200 . There is ample parking in the building's lot. Conference Room #102 is on 1st floor.

Help yourself by helping others!

Join the team & share your knowledge with others.

**Contact TC/PC at www.tcpc.com**

**Meetings start at 7:00 PM (9:00 AM on Saturday) unless otherwise noted.** ***Meets at Edina Executive Plaza.**

# February

# March

| SUN | MON | TUES | WED | THU | FRI | SAT |
|---|---|---|---|---|---|---|
| | | | | | | 1 |
| **2** | 3 | 4 | 5 | 6 | 7 | 8<br>9am-Noon Linux on Saturday |
| **9** | 10 | 11 General Mtg<br>Webinar-Install, Care & Feeding of Mesh Router<br><br>6pm Tech Topics | 12 | 13 | 14 | 15<br>9am-Noon Microsoft Office (including Access) |
| **16** | 17 | 18 | 19 | 20 | 21 | 22 |
| **23** | 24 | 25 | 26 | 27 | 28 | 29 |
| **1** | 2 | 3 | 4 | 5 | 6 | 7 |
| **8** | 9 | 10 General Mtg<br>TBA<br><br>6pm Tech Topics | 11 | 12 | 13 | 14<br>9am-Noon Linux on Saturday |
| **15** | 16 | 17 | 18 | 19 | 20 | 21<br>9am-Noon Microsoft Office (including Access) |
| **22** | 23 | 24 | 25 | 26 | 27 | 28 |
| **29** | 30 | 31 | | | | |

Twin Cities
PC USER GROUP

# You have just read an issue of The Digital Viking.

*Would you like to receive this delivered directly to your email or business each month?*

As a member of TC/PC, the Twin Cities Personal Computer Group, one of the benefits is reading this monthly publication at www.tcpc.com..

As a member of TC/PC, you may attend any or all of the monthly Special Interest Group (SIG) meetings and be eligible for software drawings. The small membership fee also includes access to real-live people with answers via our helplines, discounts, and various other perks.

Does membership in this group sound like a good way to increase your computer knowledge?

It's easy to do! Simply fill in the form below and mail it to the address shown.
(If you use the form in this issue, you will receive an extra month for joining now.)

**2/20**

**Here's the info for my TC/PC Membership:**

Full name_____

Company name_____

Address_____

City_____ State_____ Zip_____

❍Home ❍Business ❍Change address: ❍Perm. ❍Temp. 'til _____

Home phone_____ Work phone_____

Online address(es) _____

Where did you hear about TC/PC? _____

❍ I DO NOT want any of my information disclosed.
❍ I DO NOT want to receive any mailings

**Administrative Use Only** Rec'd_____ Chk#_____

**I'm signing up for:**

❍ Individual/Family Membership ($18)
❍ Business Membership ($100)
If an existing member your # _____
**Make checks payable to:**
**Twin Cities PC User Group**
**341 County Rd C2 W**
**Roseville, MN 55113**

**http://www.tcpc.com**

❍ Check #_____ ❍ Bill me
❍ New member ❍ Renewal ❍ Prior member
I'm interested in:
❍ Training classes ❍ Volunteering
❍ Special Interest Groups: New User, Access, etc.
List here:

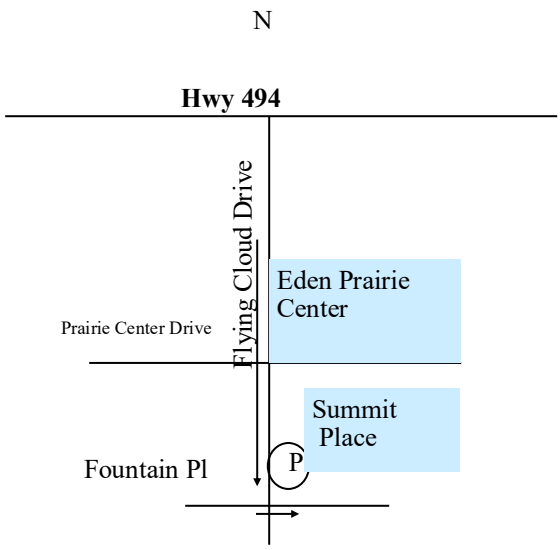
**February 11, 2020**

# General Meeting

## Installation, Care and Feeding of a Mesh Router

## Summit Place
## 8505 Flying Cloud Dr
## Eden Prairie, MN

**More info and map: www.tcpc.com**




Twin Cities PC USER GROUP

341 County Rd C2 W
Roseville, MN 55113

***FIRST CLASS MAIL***