Midland Computer Club

Midland Michigan

BITS AND BYTES

OCTOBER 2019

https://mcc.apcug.org/

ARTICLE INDEX

APCUG 2019 Winter Virtual Technology Conference
Saturday, November 2, 2019 - 1 PM ET to 4 PM ET
Schedule, Information on presentations, and to Register

Articles in this Newsletter have been obtained from APCUG with the authors' permission for publication by APCUG member groups. The Midland Computer Club has not verified the information contained in the articles nor tested procedures or hardware/software. Articles do not necessarily reflect the views of the Midland Computer Club.

GENERAL CLUB MEETING
Midland Public Schools Administration Building
600 E Carpenter Street - Room D
Wednesday, October 23, 2019
6:00 P.M.

President's Corner

Bad Memories

Author: Greg Skalka, President, Under the Computer Hood UG, CA
September 2019 issue, Drive Light - www.uchug.org - president (at) uchug.org

We are our memories. Our personalities and identities are tied to the information stored in our brains. We are who we are due to our memories of experiences, remembered preferences and lessons learned over our lifetimes. Without our brain's ability to store and retrieve memories, we could not learn, improve ourselves or differentiate ourselves from others as individuals.

Almost everything we do has to be learned, and thus remembered in some type of memory, and there are several types used by our brains. Some things, like the beating of our hearts or breathing, may not relate to memory, as we don't have to learn these things. A lot of other physical things, from simple things like walking or picking up objects to more complex activities like riding a bike or speaking, require memory, as we must learn them, as opposed to being born with these capabilities. These are attributed to what we sometimes call "muscle memory", something we remember how to do but don't consciously have to think about. We also appear to have a "scratchpad" short term memory, which can be used to store a small number of items (5 to 9) for a short time (maybe 15 to 30 seconds). This is what we use to remember a phone number read to us; without some reinforcement the information quickly bleeds away.

In more complex learning and in remembering experiences, the mind uses short term memory and then converts some short-term memories to long term. Long term memory is usually defined as memory lasting longer than 30 seconds, although long term memory of the last few days or years is also often referred to as short term memory. In some cases, injury or disease can affect memory, especially short-term memory. General aging, Alzheimer's disease and other dementias, brain tumors, blood clots and infections around the brain, head injuries and substance abuse can all cause short term memory loss. A common situation in these cases is a person that can remember in great detail events and people from 20 years in their past but is unable to remember recent events or people known for a short time.

Amnesia is a form of memory loss where the subject retains their identity and basic motor skills such as walking and speech but loses some memories or the ability to form new memories. One very common type is infantile amnesia, in which you cannot remember the first three to five years of life. In retrograde amnesia, you lose previously created memories, typically starting with most recent ones. Diseases like Alzheimer's gradually cause this type of amnesia. With anterograde amnesia, new memories cannot be formed. This can be a temporary condition, as in a black-out from excessive alcohol consumption, or permanent, when due to a brain injury. The 2000 movie "Memento" portrays anterograde amnesia.

A good friend recently told me about an incident he had not long-ago involving memory loss. He went to the gym after work one day as he was in the habit of doing, but he does not remember what he did there on that visit. His wife was called to the gym by the manager, out of concern that something was wrong with my friend. The manager said my friend was looking for his gym bag and had repeatedly asked for the manager. He had asked for the manager's name several times during their interaction, even though the manager told it to him each time. Concerned that he'd had a stroke, my friend's wife took him to the emergency room, where after extensive testing it was found he had experienced TGA, or transient global amnesia. For about an hour and a half, my friend's brain made no short-term memories. Although he could otherwise function and knew where he was, he could not remember anything of his time at the gym or why he was there and was confused by it. He could remember his past and recognized his wife, but still has no recollection of events at the gym that day. It is not known what causes TGA, though it seldom results in a repeat incident.

I've since learned that another friend's wife had a TGA incident about 20 years ago. Hearing about these incidents and the stories my sister has told about her mother-in-law's Alzheimer's makes me wish there were some way to back up our human memories. I guess the closest we can get to that now is to take lots of photos and videos of our lives.

Computers and other tech devices also rely on memories to function, and there are a number of parallels to humans in the way memories are used and the problems they have. There are different types of electronic digital memories, and they are used in computers in different ways.

The two main types of digital memory are volatile, which retain their information only as long as power is applied to them, and non-volatile, which retain their information even without power. Volatile memories include both types of RAM (random access memory): static (SRAM) and dynamic (DRAM). Non-volatile memories include Flash memory (USB Flash drives and solid-state drives or SSDs), magnetic hard drives, floppy disks and optical discs. Memory is located in many places in most computing devices, including small blocks of high-speed cache RAM inside the microprocessor component, fast DRAM modules for main memory, SSD modules or magnetic hard drives for main OS / program / data storage and peripheral removable storage (USB, floppy and optical discs).

Just as with humans, computers and tech devices without memories cannot function. It is the information stored as operating systems, apps and data in our tech devices that give them their “personalities” and capabilities. A computer or smart phone with blank memory devices is just an empty, inert shell.

Memory failures can cause big problems for computers, as they do for humans. An unreliable main memory DRAM module can result in errant program operation and computer crashes. SSD or hard drive failures can mean data loss, programs that won’t load and OS crashes.

Our electronic digital memories give us two advantages over our human memories - the ability to easily replace faulty components and the ability to back up our data, so faulty components don’t result in a serious loss. Important data in non-volatile memory devices should be backed up or copied to other devices, so that a failure of the original device can be easily corrected by replacing the device and restoring the data from the back-up copy. Bad volatile memories like DRAM modules can easily be replaced so computing can resume.

I got my first camera in grade school and have always enjoyed taking photos. I have taken quite a few over the years, and the quantity increased greatly once I got a digital camera and no longer had to worry about the cost in film and developing each shot represented. I now take thousands of digital photos and hours of digital video each year. It does provide that additional assist to my memory when I want to know when an event occurred, as I can check the date stamped on my slides or photo prints or the time/date stamp in my photo jpeg files.

Having digital photo files is great, as they don’t degrade and can be backed up, but over the years the file size of photos has greatly increased. My first digital camera was just 1 Megapixel, and the photo files were only about 100 KB each. My latest camera takes 18 Megapixel photos, resulting in 10 MB files each. Such large files make great photos, but they have become difficult to share, at least in their full-size form. These files are really too big to email as an attachment, and while I have often put them up on a file sharing site to allow others to download, some folks I send them to have problems getting them. Even for those tech savvy recipients, downloading 30 GB of data can be a pain.

My son was recently married, and I took a number of photos and videos of the event and days surrounding it that I wanted to share with relatives. I wound up with about 20 GB of data to share. Since this was a one-time event with files going to only about eight recipients, some of which were out of state, I decided the best way to share was to copy the files to relatively inexpensive USB flash memory devices and give them out in person or mail them.

All I needed was about ten 32 GB Flash drives, which could be had for around $8 each. I had previously bought some loose Patriot 32 GB drives from Amazon; these came in a cardboard envelope. I needed more, so I also bought some from Fry’s Electronics; I got 32 GB individually packaged Samsung drives for about the same price on sale.

Our group's board meeting was just a few days after I bought the Fry's drives, and so I told the board about my need for USB Flash drives and the purchases I'd made. Our vice president then warned me about buying Flash drives online, as the quality can sometimes be poor. He claimed that parts that fail manufacturing tests can be intercepted from the dumpsters and sold online as "good" drives. I thought that unlikely from Amazon, but I soon found our VP's warning to be credible.

A few days after the board meeting, I started copying the files onto the USB Flash drives. I had used some of the Amazon drives and had only one left, and so started with it. During the copy process, however, it stopped and said the drive was full. I was only copying 20 GB onto a 32 GB drive, yet it had stopped with only about 4 GB put onto the drive. Windows File Explorer indicated the drive was 32 GB in size, but with only 4 GB on it, it said it had 27 GB of used space and 4 GB free. Something was definitely wrong with this drive. I recalled no problems with the others I'd bought in this Amazon batch, but also recalled that I had only put no more that 2-3 GB on any of them before giving them out.

I pulled out my Fry's drives and all worked fine with the full 20 GB of files. I considered that it was possible that my Amazon drives could have been "counterfeits" pulled from the manufacturer's dumpsters and resold; after all, they came in unconventional (meaning no) packaging. The Fry's drives were shrink-wrapped onto cardboard holders, and so were more likely to have gone through the manufacturer's full process.

It is unfortunate that the Fry's drives are sold with additional packaging that winds up in the landfill, but it may be an additional indicator of an authentic, fully functional product.

Lock Up Those Photos

Author: Bill Crowe, Director, Sarasota Technology User Group, FL
October 2019 issue, STUG Monitor www.thestug.org director1 (at) thestug.org

Last month I lost my wallet. Not a good day. I knew the last time I had used the card, and from there I went straight home. They did not have the card at my last stop, so I had either lost it on the way to the car or at home. After an extensive search, I had to go about cancelling and replacing all my credit cards. I had to do the same for all my other cards like medical cards, Driver's license, Costco's, and others. Not a fun job. The job would have been so much easier if I had kept a record of all my cards. I got to thinking that if I had taken a picture of each card (front and back), I would have had them on my iPhone. That would have solved the problem.

Thinking about it further, what if someone got my phone or was able to access my iCloud and gain access to my info? All my cards were there for the taking. I was hoping that there was a way to lock photos on my iPhone, but Apple has not yet provided one. I knew there must be an app for that, and 'By Golly' there is.

Credit: www.privatephotovault.com

There are, of course, many applications that can do it, but one of the best is called Private Photo Vault. The following is a brief introduction to Private Photo Vault.

Private Photo Vault is one of the best free applications to protect your personal photos and videos by password/pattern-locking. This feature-rich app allows easy album organization by allowing you to transfer images and videos from iPhone's photo app to your new protected album. All you need to do is select photos you want to hide and password-protect them on your private album.

Private Photo Vault has a tri-protect system. You can either hide your photos via a secure password system or a nifty pattern lock system. There's also a pin lock option that lets you hide an image by entering a 4-digit pin.

Of many additional features, my favorite is the decoy password option. It allows users to enter two passwords – one for general access and another for those albums you want to really secure. With a smooth interface, and simple yet extremely secure protection option, the app is a good way to hide your photos on your phone.

By the way, the end of my story is that after I cancelled most of my cards, I found the wallet. It was in about the only place in the house I had not turned upside down.

See the tutorials at https://privatephotovault.com/tutorials/

President's Corner

Security is Important - Why Does it Take So Long (and Cost So Much)?

Author: Greg Skalka, President, Under the Computer Hood User Group, CA
October 2019 issue, Drive Light www.uchug.org president (at) uchug.org

I am a technology user. I use all sorts of tech products, applications and services. I have laptops, desktops and Chromebooks. I have mobile devices - smart phones and tablets. I have home Internet access and I access the web from other places as well. I have a home network and I have smart home devices (cameras, TVs, voice-controlled assistants, smart lights and appliances). I use lots of software. I search the web, bank and buy things online and send emails and texts. I'm not much for social networks, but I do appear in posts by others, especially my wife. I've got a lot of the things a typical middle-class American would have.

I use a lot of technology, but all I want to do is use it. I don't want to have to struggle to make it work, fix it or spend a lot of time and money keeping it working safely. I want it all to work every time as I expect it to work. Unfortunately, there is a lot more to our tech lives than that. None of the tech revolution we have seen in the last decades would have been possible without money. It is commerce, capital and the desire to make a profit that brought us most of this, including Microsoft, Google, Uber, Tesla and all the rest. Some key government investments in technology, in the space program, DARPA and the military-industrial complex helped with fundamental research, but the capitalist entrepreneurs filled in the rest. Money made tech great, but money also made it unsafe.

Entrepreneurs take legal risks to gain rewards; criminals try to find the least risky ways to make money, legal or not. Each new tech device, app or service that comes out is studied for vulnerabilities by the criminal elements intent on exploiting it for monetary gain. Now that technology has interconnected the world, we can be the victims of crime originating from all over the globe. Even nation states can get in the game, trying to steal information for economic and political purposes.

All this leaves the poor tech user vulnerable. The rapid rate of change, the ease of use and ubiquitousness of these product and services just add to the risk. How does a user evaluate the threat and defend against it? Is it all worth the cost?

The criminals are out there, ready to hack, snoop, steal and deceive. They want your personal information to steal your identity and your passwords to steal your money. They want to trick you into sending them gift cards and Bitcoin. Who is going to protect the tech user from all the cyber threats? Can the government protect us? Laws may be passed, regulations put in place and enforcement attempted, but citizens are still victimized. Unfortunately sometimes the government is part of the problem, not protecting the sensitive data we entrusted to them.

Can the companies we buy products and services from protect us? Their desires for profit over all else have created some of our tech problems. They will sell us devices that are not secure if they think it makes business sense. They'll collect and monetize our personal information and then often fail to protect it adequately. It seems we as tech users must find ways to protect ourselves, as no one else will take responsibility for our security. Unfortunately, that means additional costs in terms of money and time are required to keep our assets (money, identity, personal safety) secure when using all these tech items and services in the new global digital electronic world.

There is no practical way to remain 100% secure in our modern connected world. Even if you turn off all of your devices, disconnect them, put them in a box and seal it up (and cancel all your related services), you are not safe. The government still has your personal information, and even if you are not on Facebook, others could post about you. You will have to go back to paying with cash, shopping and banking in physical locations and communicating through personal visits and letters. Unless you want to step back into the 1950's, you will have to adopt some additional safeguards with every new tech item you acquire.

Safety as a tech user is not an absolute, but a matter of degree. More time and money spent to safeguard our activities will provide more relative safety and security, but trade-offs will need to be made. More security comes at a higher cost and usually a greater inconvenience as well. A user can make their tech life more resistant to attacks by cyber criminals and become more resilient should bad things happen, but it will require more time, money and effort on their part. Lots of articles are written about protecting ourselves online and describing precautions we all should take, yet cybercrime is still prevalent.

I think I take care of my tech household pretty well, though there is always more that can be done. The things I value most (finances, identity, property) I protect the most, while things of a lesser consequence I am a bit looser with. In some ways I probably go overboard in caution, but there are probably some risks I don't take as seriously as I should. I'm pretty careful with physical security, using strong passwords, encryption, a VPN and two-factor authentication where appropriate.

I'm pretty resistant to social engineering threats and am very careful with my personal information. Exercising care and vigilance online is good, but it requires effort and some investments. I have several laptops and desktops that my wife and I use, as well as a couple of Chromebooks. All the computers we regularly use run Windows 7, so I am presently working towards replacing at least some of them with Windows 10 computers ahead of the Windows 7 security sunset in January 2020. This considerable cost in new hardware and software and in time to set everything up is strictly due to Microsoft's desire to make Windows 7 obsolete; I would be perfectly happy staying with Windows 7 otherwise. I'll be spending money on new systems, probably buying new software and spending time teaching my wife how to use the new OS. I'll probably compromise by keeping a couple of old Win7 computers or laptops to run software I can't convert to Win10 or don't want to spend more on. I still have a Windows XP computer that I keep off-line to run certain programs. I'm actually writing this article on it; I've yet to find a Microsoft Word version I like overall as much as version 6.

Even when security updates are provided for free, our time is usually required to oversee their installation. If nothing else, the time required to install updates represents time we are unable to use our devices. While Windows 10 may force automatic security updates, they can wind up being applied at the most

inopportune times. I don't mind as much the automatic updates my Chromebook gets from Google, as they are downloaded in the background and quickly applied on the next power-up.

In addition to computer updates, our network items often require security patches. Few users may pay much attention to updates for their routers, however, unless they are alerted somehow. I have a Netgear Orbi mesh Wi-Fi router, which I love for its performance and ease of use (but not so much for the initial cost). Because I'd registered the product and downloaded their app, I recently received an email that an update was available for my router's firmware. I initially tried to apply the update through the app (on my smart phone) but was unsuccessful. I was able to enter into an online chat through the app with their tech support, and thus began a two-hour process to finally get my router system updated.

I assumed I would be able to easily update through the Orbi app, but the support tech told me my installed firmware version was too old, and I instead would need to download and install an intermediate version from a web link. I find the small screen of a phone too difficult to use for this kind of activity, so pulled out a Chromebook, logged into my Orbi router and went to the web link. This also allowed me to keep the support chat going separately through the app on my phone.

Once I got to the web link, I found I would be downloading a zip file. There may be ways to unzip on a Chromebook, but I don't know them, so I switched again and logged in with my Windows laptop. The support tech said to apply the update first to the satellites (my mesh system consists of one router and two satellite units) and then to the router. The update page was a bit confusing, and I inadvertently updated the router first. Fortunately I was still connected to the tech support person, so after a number of additional steps, I successfully updated all components.

It is almost time to renew my anti-virus, and I need to make some decisions about it. I've been using ESET Internet Security for many years and really like it (and think it protects me, but who really knows). I'm not sure what I should use going forward on Windows 10, as I've heard that Microsoft's Win10 built-in protections are as good as anything else, and obviously are at no extra cost. I always buy ESET on sale ahead of when I need it, so I already have new copies to put on my Win7 computers. That seems like a waste, as I won't have these computers on the Internet past January. Still, I shouldn't cut corners on protecting my online banking computer, at least until I am switched over completely to Windows 10.

Though I may be spending a lot of time and money getting my new computers set up, it hopefully will increase the odds that I'll have secure systems that will help protect my data.

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-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.

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.

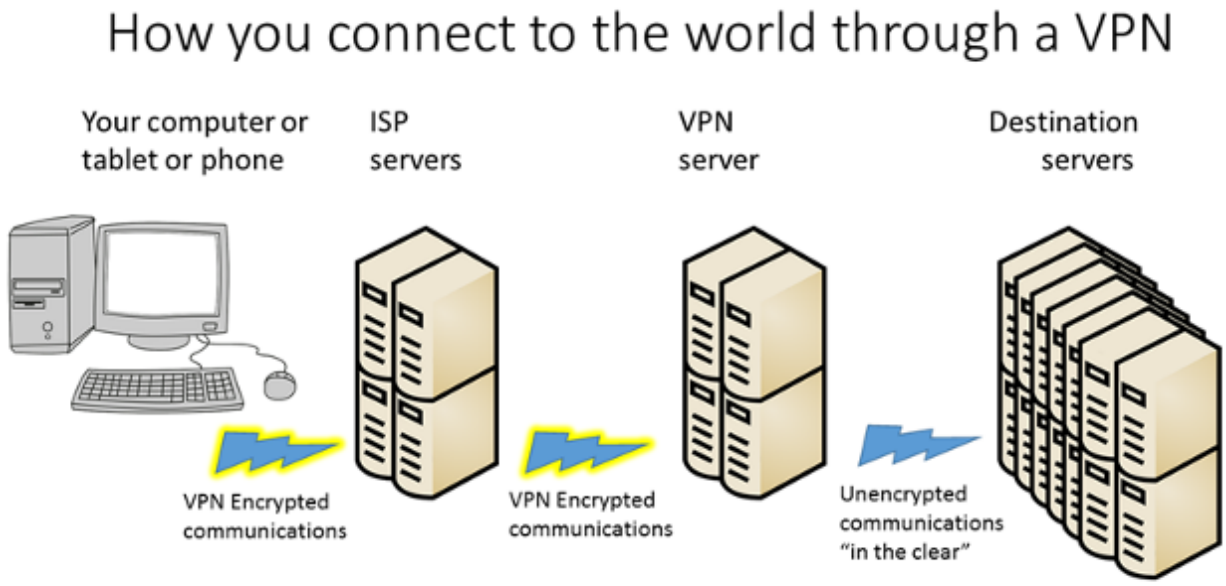


Illustration 1.

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.

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**.

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 bowers 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.

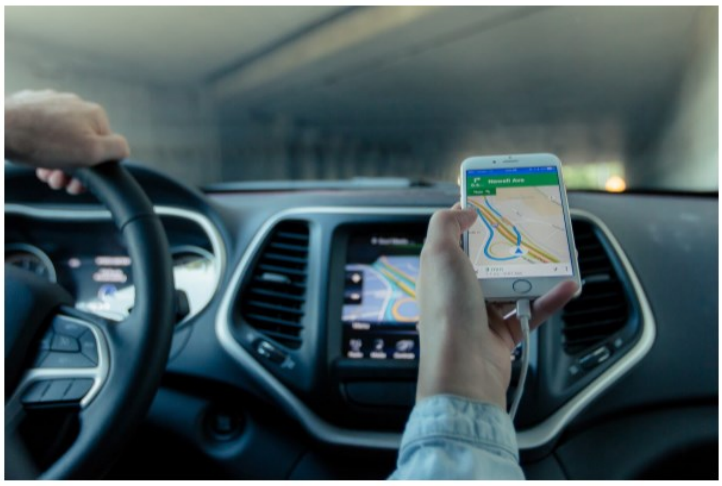
Service	Service type	Boston VPN server	London VPN server
Netflix	Video streaming	Success	Success
www.Citicards.com	Credit card issuer	Success	Success
www.Americanexpress.com	Credit card issuer	Success	Success
www.usaa.com	Credit card issuer	Success	Success
www.bankwithunited.com	Checking account bank	Success	Success
www.schwab.com	Stock brokerage	Success	Success

Illustration 3

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.

Smartphone Map Apps vs. Dedicated GPS Devices

Author: Dorothy Fitch, Green Bytes Editor, GVR Computer Club, AZ
October 2019 issue, Greenbytes www.ccgvaz.org Newsletter (at) ccgvaz.org



public domain image from pxhere.com

I recently heard an interesting report on a local television station about the pros and cons of using your Smartphone vs. a GPS device to find your way when you travel. I am certainly not an expert on this topic but wanted to share a few things I discovered as well as some links so that you can learn more, too.

I hadn't really thought about it, but perhaps the biggest difference between the two is that Smartphone map apps use cell tower signals to provide your location and generate maps. GPS devices, such as Garmin or TomTom, use satellites for positioning.

What this means is that if you are in a remote area that doesn't have cell coverage, maps on your phone will likely not work.

Other interesting considerations:

GPS devices are more accurate—to within 15 feet your location— because they are using satellite technology.

Smartphone locations are accurate to about 164 feet. Your location is determined by triangulating signals from several cell towers.

A Smartphone app uses your phone's battery (though you may be able to charge it in your car via USB). Beware, however, that on a recent trip, my Android phone was plugged in. During the half-hour trip, the phone's battery level dropped by 4% because the power used by the app was greater than the rate of charging. A GPS device will plug into your car's cigarette lighter or USB port.

Using a GPS device will leave your Smartphone available for other purposes (though not when you are driving, of course!).

A Smartphone app will use up mobile data, which may be of concern if your phone service doesn't include an unlimited data plan.

GPS devices often come with a way to mount them to your dashboard, which makes it easier to check your route.

The Google Maps Smartphone app gives you up-to-the-minute accident reports. It even prompts you to respond as to whether the accident someone reported earlier is still there. It provides an estimated time delay, as well as alternate routes. Some GPS devices offer traffic alerts as well.

Using the Google Maps Smartphone app, I was surprised one time when I entered the address of my destination, which was a store. I got immediate feedback that the store had already closed for the day. Very useful information to know (and saved me a stop).

Many GPS devices include lifetime map updates. This can be handy, as new housing developments are constructed. You can also download (or purchase) maps for foreign countries. You can likely use your Smartphone app abroad, but I haven't tried that.

Some GPS devices can store your trip data, which you can then download to a map, where it displays your route. This is particularly interesting if you are hiking or on a boat.

If you are car-shopping, you may be offered a package that includes a built-in GPS system. However, that option is likely to cost much more than the price of a hand-held separate device.

Articles on the subject:

- Do I need a dedicated GPS device if I have a smartphone?
- Can you trust your phone's GPS driving directions?
- Smartphone vs. Dedicated Car GPS (PND)
- The 7 Best Traffic Apps of 2019
- 44 Google Maps Tricks You Need to Try

Interesting Internet Finds – September

Author: Steve Costello
scostello (at) sefcug.com

While going through the more than 300 RSS feeds, I often run across things that I think might be of interest to other user group members. The following are some items I found interesting during the month of August 2019.

The Dumbest USB Gadgets You Can Buy
https://www.reviewgeek.com/5774/the-dumbest-usb-gadgets-you-can-buy/

This is not the kind of thing I usually share, but I just couldn't believe some of the things shown. Also, if they are for sale, I assume someone is dumb enough to by one (not you or me, of course).

Here's What You Should Use Instead of CCleaner
https://www.howtogeek.com/361112/heres-what-you-should-use-instead-of-ccleaner/

I still use CCleaner, but others have concerns lately. For those who no longer use it, this post tells you what you should use instead.

Gmail For Mobile: Disable Conversation View?
https://www.askdavetaylor.com/gmail-for-mobile-android-disable-conversation-view/

Did you know that you can disable conversation view on your mobile (Android only for now)? Dave explains what conversation view actually is, and how to disable it in Android Gmail.

What is Android Bootloader? A Complete Guide
https://joyofandroid.com/android-bootloader/

For those of you who like to know the inner workings of Android, this is a good guide to the bootloader.

OneDrive tips and tricks: How to master Microsoft's free cloud storage
https://www.zdnet.com/article/onedrive-tips-and-tricks-how-to-master-microsofts-free-cloud-storage/

This is a great read for anyone who uses Microsoft OneDrive, especially for those who are using an Office 365 Home or Personal subscription.

When 2FA Goes Bad
https://askbobrankin.com/when_2fa_goes_bad.html

Yes, I know that everyone says you should be using two factor authorization on all you accounts that support it even if SMS messaging is the only option. But, I think you also need to be aware of what can go wrong. Bob Rankin talks about what happened recently to Reddit.

How to Install Minimal Ubuntu on Your Old PC
https://www.maketecheasier.com/install-a-minimal-ubuntu-on-old-laptop/

I recently had a friend ask what he should do with an old x386 laptop with only 2GB of RAM. I told him he should put Linux on it. He did install Ubuntu on it and got everything running with only minor problems. If you have an old PC and want to try installing Ubuntu on it, check out this post. (Note: Other Linux distributions should work in a similar way. I have used both Ubuntu and Mint myself.)

****