THE WYSIWYG

March 2017 Volume 29, Issue 3

STERLING HEIGHTS COMPUTER CLUB

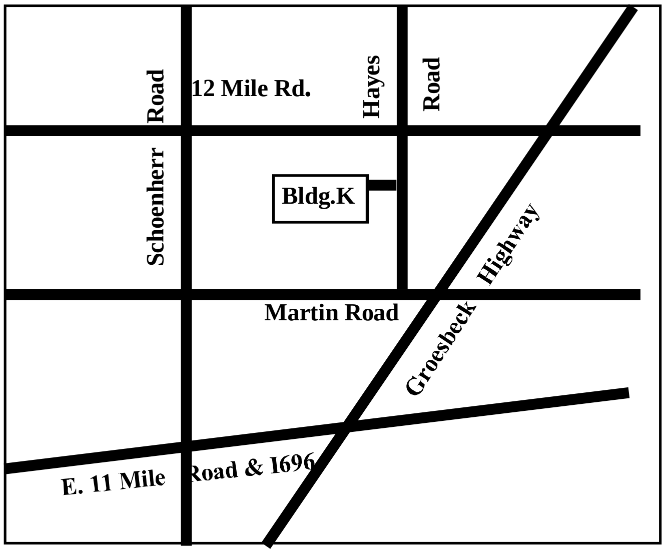
PO Box 385
Sterling Heights, MI 48311-0385

$3.00

MAIN MEETING: TUESDAY MARCH 7

6:30 PM

Macomb Community College
South Campus
14500 E 12 Mile Road, Warren
John Lewis Community Center
(Building K)



IN THIS ISSUE:

This Month's Main Meeting Topic:

"Using Technology For Good And Evil" by member Mike Bader

PC SIG Meeting:

Tuesday, March 21 starting at 6:45 at the Sterling Heights Public Library

(Meet in the second floor conference rom)

Sterling Heights Public Library

The Sterling Heights Public Library, at 40255 Dodge Park Road, is located just south of Utica Road. A large sign reading "City Center" marks the driveway to the library and parking. The Programming Center, where the meeting is held, is just inside the front door of the library.

Guests and visitors are welcome. People can attend any SHCC meetings during two consecutive months before deciding to become a member or not. Meetings include the main meeting and SIG. July and August don't count since there is no main meeting. Membership includes admission to all SHCC functions and the newsletter. Membership is open to anyone. It is not limited to the residents of Sterling Heights.

DUES: $25/YEAR

CLUB ADDRESS: PO Box 385, Sterling Heights, MI 48311-0385
CLUB E-MAIL ADDRESS: Info@SterlingHeightsComputerClub.org
CLUB WEB PAGE: http://www.SterlingHeightsComputerClub.org

Resource People:

Family Tree	Rick Schummer
Firefox	Don VanSyckel
FoxPro	Rick Schummer
General Computer Questions	Jack Vander-Schrier
Hardware	John Rady
MS Publisher	Rick Kucejko
MS Word	Rick Schummer
Spreadsheets	Rick Schummer

SHCC Coordinators:

Associate Editor	Rick Schummer
Door prizes	Don VanSyckel
Greeter for visitors	Jim Waldrop
Newsletter publisher	Rick Kucejko
Program Coordinator	Mike Bader
Publicity	Patrick Little
Resource People	open
PC SIG	Jack Vander-Shrier
Welcome & check-in desk.	Jim Waldrop
Web Site	Don VanSyckel
Web Watch column	Paul Baecker

2016 SHCC Officers

President: Don VanSyckel
Secretary: Rick Kucejko
V. President: Mike Bader
Treasurer: Bernie DeFazio

Contact Information:

Paul Baecker	586-286-2314	webwatch@sterlingheightscomputerclub.org
Mike Bader	586-447-6683	mdbader@flash.net
Bernie DeFazio	586-864-6558	berniede1@wowway.com
Rick Kucejko	248-879-6180	rick@kucejko.com
Patrick Little	586-264-1497	pblittle@wideopenwest.com
Rick Schummer	586-254-2530	rick@rickschummer.com
Don VanSyckel	586-731-9232	don@vansyckel.net
Jack Vander-Schrier	586-739-5952	jvanders@comcast.net

(**Call Jack after noon)**

Four Month Meeting Schedule:

MARCH 2017
1 - COMP meeting
7 - SHCC – "Using Technology For Good And Evil" by member Mike Bader
12 - SEMCO meeting
21 - PC SIG

APRIL 2017
4 - SHCC- **"Quad-copter With Computer Control" by Sam Chapatwala of the Detroit Beagle-bone Community Meetup**
5 - COMP meeting
9 - SEMCO meeting

MAY 2017
2 - SHCC—Main Meeting
3 - COMP meeting
14- SEMCO meeting
? - PC SIG

JUNE 2017
6 - SHCC—Main Meeting
7 - COMP meeting
11 - SEMCO meeting

THE CLUB DOES NOT MEET IN JULY AND AUGUST

Other Computer Clubs:

As a member of SHCC, you can attend meetings of other clubs where we have reciprocating membership agreements, at no charge.

Computer Club of Marysville and Port Huron (COMP)
Time: 1st Wednesday, 7:00PM
Place: Mackenzie Bldg, Room 201, St Clair Community College, Clara E McKenzie Library-Science Building, 323 Erie St.
Port Huron, MI (810) 982-1187
Web Page: http://www.bwcomp.org
Reciprocating: Yes

South Eastern Michigan Computer Organization (SEMCO)
Time: 2nd Sunday at 1:30PM
Place: Altair, 1820 E Big Beaver Road, Troy, MI 48083
(248) 840-2400
Web page: http://www.semco.org
Reciprocating: Yes

Royal Oak Computer Club
Time: Every Wednesday at 12:30
Place: Mahany/Meineger Senior Community Center 3500 Marais Ave. Royal Oak, MI 48073
248-246-3900
Reciprocating: No

Newsletter submissions are due 10 days before the club meeting, but the earlier the better. They should be sent to :
WYSIWYG Publisher
5069 Fedora, Troy, MI 48098
OR at the e-mail addresses: newslet-

The President's Pen

by Don VanSyckel

None this month. Don is still recovering from his past mishap.

The Ripple Coffee Maker

by George Harding, Tucson Computer Society
www.aztcs.org georgehardingsbd@earthlink.net

One of the most unusual products at CES was demonstrated by a coffee maker!

The result is a cup of coffee with an image floating on the surface of the coffee. It has to be a latte, cappuccino or other foam-based beverage in order to show the image. It's called Ripple and I saw it at a booth at CES, In fact, I was served a latte with an image of the Mona Lisa floating on the surface!

The first step is to make a latte, or whatever. The second step is to download an image of just about any sort to a machine that does the "engraving." The result is your image in the foam of the latte.

It's a unique operation and, while interesting, doesn't seem to have much in the way of actual use, outside of being an unusual offering at parties.

They are currently processing orders for customers in the U.S. and Canada.

The Ripple Effect
http://www.coffeeripples.com/

USB Advances

by Bart Koslow, Channel Islands PCUG, CA

USB-C? USB 3.1 generation 1 and 2? The USB interface is changing. It is becoming more versatile, faster, smaller and easier to use. Always interested in new computer developments, I decided to check out these latest developments.

USB long ago replaced the old serial, parallel, and other computer ports. Now it is set to replace many more types of connectors and ports and add functionality.

USB 2.0 (maximum speed 480Mbps) and USB 3.0 (now called USB 3.1 gen 1) are being replaced by USB 3.1 gen 2. USB 3.1 gen 2 doubles the data transfer speed from USB 3.1 gen 1 from 5Gbps to 10Gbps. This will cut data transfer

This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.

VISIT THE SHCC WEB PAGE:
http://
www.SterlingHeightsComputerClub.org

Presenters Wanted

The officers invite any member to make a presentation at the main meeting.

If there is some software you have been using and think others may be interested as well, or there is a computer topic you would like to present to other members, please call or e-mail Don VanSyckel. Making presentations is not that difficult. The hour goes by before you know it and there is always enough material to cover in a software package so that the hour is easy to fill.

If there is a topic you are interested in or something you would like demonstrated, please see any of the officers. They are always interested in what the members would like to see.

Door Prizes

Door prize drawings are held at regular club meetings. The winner's circle for February included:

Ed Zaremba won a 10 foot network cable

Sharon Patrick won a flashlight

Don Hjelle won a Chromecast antenna (for watching free TV)

Mike Bader won DVD's

Richard Katnik won white cable ties

Paul Baecker won a safety light

Rick Kucejko won cleaning cloths

Richard Bauman won Hoyle Slots software

Warner Mach won AVG Antivirus software

Vulnerable Points On The Path To Privacy

From the Ask Leo Newsletter
https://askleo.com

Privacy and security: tracing the path from your fingertips through the services you use to your information's final destination.

Privacy and security are more important, and under greater threat, than ever before. We manage an ever-increasing amount of sensitive information and tasks, while the number of ways our information can be exposed seems to be exploding.

There are five major areas in which your security and privacy can be both exposed and protected:

1. Your computer, including all the software on it, and the hardware itself.
2. Your network, the vital link that connects your computers to each other and to the internet, and a potential point of major exposure.
3. Your ISP, the provider of that vital link, wielding more power and subject to more scrutiny than most realize.
4. Your online services: they hold your data, but do they know what they're doing, and will they defend your privacy if needed?
5. Your friends and acquaintances: often the weakest link in the chain. Do the people you interact with value (or understand) privacy and security as much as you do?

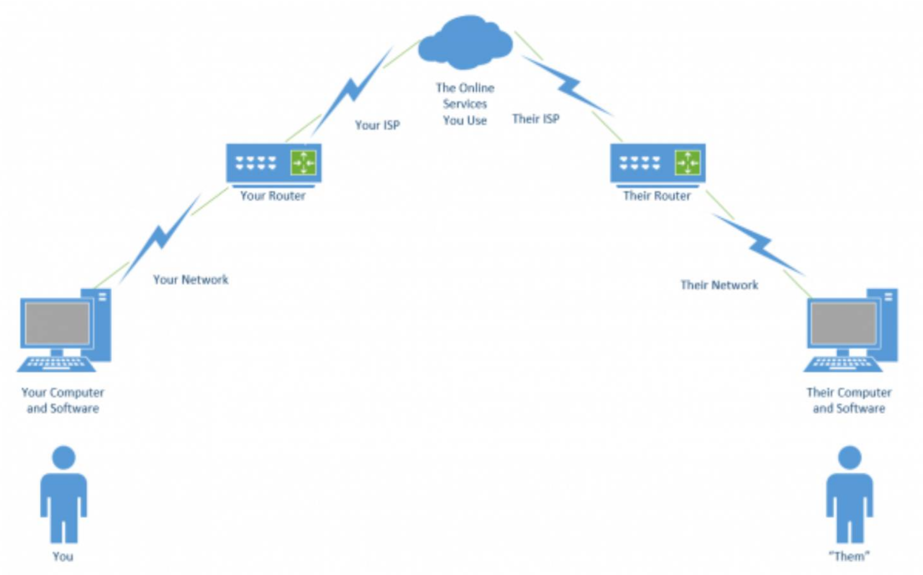
Let's review each of these points of risk, exposing the technological hazards we (perhaps unknowingly) face every day.

1. Your computer

Privacy and security start at home (or in your pocket).

Software

For every piece of software we run, we trust that the right decisions have been made in terms of maintaining our privacy and security. We also trust that the vendors themselves have our best interests in mind. This is true not only for our desktop and mobile computers and phones, but for the surprising number of network-connected devices in our lives, including televisions, cars, security cameras, and even baby monitors.


The Online Services You Use
Your ISP
Their ISP
Your Router
Their Router
Your Network
Their Network
Your Computer and Software
Their Computer and Software
You
"Them"

The operating system

Be it Windows, Linux, Mac OS, or something else, most of our technology runs some form of base operating system software, or "OS". Even those devices we consider to be single purpose, like a baby monitor, often run a "general purpose" operating system (typically, a Linux variant).

When Windows 10 changed its approach to privacy, it became shockingly clear how much we rely on Windows for privacy and security. Many felt Microsoft had crossed a line, collecting excessive amounts of information in ways outside our control. Exactly what was being shared was unclear, and there were no trustworthy, easy-to-use solutions to avoid it. While Microsoft appears to be adding more privacy controls to more recent versions, the fact remains that for many, trust was irrevocably breached.

The most important take-away, however, is not that Microsoft may or may not be trustworthy; it's that *every* operating-system vendor has the power do any or all of this, with or without letting us know. The amount of trust we place in any OS vendor to properly manage our privacy and security is *enormous*.

Aside from being vigilant, managing the privacy and security options that are available, and paying attention to reliable, objective news sources, there's little we can do if our trust is misplaced, other than switching to a more trustworthy alternative.

Applications

Everything I've just said about operating systems applies to *every piece of software* running on your computer, phone, or other device – including security software.

The average computer user has dozens, if not hundreds, of apps and applications installed across various devices, from nearly as many different vendors – and each vendor has its own approach to privacy and security.

That's a lot of trust spread across a lot of different companies. Besides trusting that they're competent at whatever it is we use their software for, we're also assuming they're competent at keeping our information safe and secure, and that they're not, themselves, malicious. We give them much more access to our information than we might realize.

The best defense here is twofold: Don't install things you don't need. Only install from reputable vendors.

Malware
When people think about privacy and security on their own computers, the first thing they think of is malware: malicious software that somehow makes it onto their computer and proceeds to steal information (or worse).

I've placed it last in the software category, because by now, most people understand malware and the concepts behind it. More importantly, we know how to combat it. It's something that makes the news almost every day. And while protecting yourself from malware is terribly important, it's a topic already well understood.

You know how to combat malware. You know how to avoid malware. You know how to be skeptical. It's something this industry talks about every day, so I won't belabor it here.

Hardware
An often-overlooked aspect of security is what I refer to as "physical security". One of my frequent statements is, "If it's not physically secure, it's not secure." If someone untrustworthy can touch your hardware, they can do amazing amounts of damage.

Physical access
If someone can walk up to your computer (or phone, or router, or many other networked devices) and start using it, that's a privacy and security hole bigger than anything I've listed so far. If someone malicious has access to your device, they can do *anything*.

Most of the time, our concern is theft. The good news here is that most thieves are unsophisticated. They're just looking to turn around the hardware for some quick cash – they don't really care what you have stored on it. However, that data is certainly accessible to them – or the person they sell it to – should either of them have a little technical expertise.

More commonly, the risks are closer to home: spouses, co-workers, children, and friends. Be they malicious or nosy, the people around us often have the greatest incidental access to our things. It's one thing to go snooping around our medicine cabinet, but something else entirely to poke around in our email, spreadsheets, or other personal data.

How much of a problem this is varies, of course. At one extreme, you may not feel the need to take much action. At the other, a combination of encryption, software locks, and perhaps even hardware locks might be appropriate.

Hardware compromise
We usually trust that the hardware we use hasn't been compromised. That may not be a safe assumption when using devices in public.

A good example is a hardware keylogger inserted between the computer and keyboard. Undetectable to any software on the machine, and hidden behind the computer itself, it can passively collect massive amounts of information until the perpetrator comes along to pick it up and act on the data.

While it's significantly less common than other forms of compromise, hardware hacking can take many forms. It's one reason I never use a public computer for anything remotely sensitive.

2. Your network

Much of the risk we encounter every day is due to being inter-connected, or networked. It's also what enables so many of the features, functionality, and rich experience we enjoy with technology. Your network is how your computers are connected to each other and to the world.

Router
The first device the internet reaches on entering your home or workplace is, typically, a single router. Its job is to allow your multitude of devices to share a single internet connection. As a side effect, it also acts as a security device itself: routers are great firewalls, protecting your network from many of the threats out on the internet.

Routers are powerful devices. In fact, they're powerful *computers*. They're often based on general purpose operating systems. Before even plugging the device in, we're trusting that the router vendor is competent and has factored in appropriate measures to protect our privacy and security.

Even then, routers are interesting to hackers, because by compromising a router, they can compromise all the devices connected to it, or misdirect people into visiting malicious sites or downloading malware.

Beyond getting a reputable device from a reputable vendor, the single most important solution in your control is to secure your router. Every router comes with default settings that may or may not be the most secure configuration for you.

Wireless connections
Wireless connections are often controlled by your router but deserve additional attention. They're an easy point of compromise, particularly in public.

Because the range of a wireless connection is a function of both the wireless access point and the computer attempting to connect, it's possible to connect from a distance further than most people might realize. Particularly if someone is dedicated to the effort and trying to connect to a relatively close access point, it's unwise to rely on distance alone as a security measure.

The most important thing you can do in your home and business is to never have an open Wi-Fi hotspot; always use a WPA2 key or password for the connection.

The most important thing you can do when traveling is to know how to use an open Wi-Fi hotspot safely.

Other computers
I mentioned earlier that your router protects you from many of the threats coming from the internet. What if the threat is more local?

Many people fail to realize that their computers and networks are often set up to give locally connected machines – machines on the same side of the router – a high level of trust. Sometimes, that trust is unwarranted.

Consider your child's computer. He or she may not have the sophistication to know not to download and run malware, and a lack of adequate protection could infect other machines connected to the same local network. The same could be true of a visitor, or even a less-than-tech-savvy spouse. Sometimes, the threats come from within.

Solutions involve making sure your computer has its own defenses set properly, including its own firewall. Today these are on by default for most devices. More extreme might be segmenting your network into trusted and untrusted zones, using an additional router or a router that provides this functionality natively.

Other devices

In recent months, there's been much made of the so-called "internet of things", or IoT. I alluded to this earlier when I discussed devices we would consider dedicated to a single task – such as your refrigerator – that, nonetheless, run general purpose operating systems.

It turns out neither privacy nor security were at the top of many IoT vendors' feature lists.

The good news is that their negligence has (thus far) mostly been limited to those devices becoming part of botnets used to cause havoc elsewhere. Other than using their owner's internet bandwidth, little damage was done at home. Unfortunately, the potential still exists for more localized damage, should hackers ever decide to focus their attentions on it.

The bad news is that, aside from avoiding these devices completely, there's little in our control. Once again, we're limited to using information sources we trust to provide us with reviews and recommendations, now with an eye to privacy and security – an odd concept to consider when looking at an internet-connected television or kitchen appliance.

3. Your ISP

ISP: Internet Service Provider. Depending on where you live (or how you travel), you may have several options, or very few. Regardless of which you choose, you place a tremendous amount of faith in your ISP.

Home internet connection

Connecting to the internet at home has become one of the fundamental utilities folks rely on. Your ISP provides your digital lifeline – your connection to the internet.

Here's the catch: your ISP can monitor your traffic. All of it. Unless you take additional steps, just about anything that travels over your ISP-provided connection can be examined – often in detail – or even recorded by the technicians operating the equipment.

Normally, that's not much of an issue. Your ISP is too busy just keeping the lights on, so to speak, to pay attention to your emails or web browsing. Of greater concern are those situations when your ISP can be compelled to disclose your location and web usage by government demands or court orders.

The average computer user probably doesn't need to be concerned. I know I'm not. But if you are, then the steps you can take generally revolve around encrypting the data that travels between your computer and your ISP.

https encrypts the connection between websites that support it and your computer. Your ISP can still see that you connected to askleo.com, for example, but they can't see what it is you asked about or looked at.

A **VPN** encrypts all traffic between your computer and the VPN service. Your ISP only sees that you've connected to the VPN, but can see nothing beyond that.

TOR – The Onion Router – is a web proxy (most securely used with a dedicated TOR browser) that encrypts all your web activity, and routes your traffic in such a way that the server to which you are connecting has no idea who you are, unless you explicitly tell them. Once again, your ISP can see that you're using TOR; they just can't see what you're using it for.

One of the most overlooked aspects of this topic is the very literal nature of the term "ISP". *Anyone* who provides you with a connection to the internet is your ISP. Be it at home, in a hotel, at a coffee shop, or at work (which I'll discuss next), anyone who provides you with an internet connection can examine what you're up to.

Work internet connection

When you're at work, a separate set of rules often apply. Thus, there are several other aspects related to your privacy and security to consider.

If you're using employer-provided equipment, everything I said about hardware compromise could be at play. It's possible, and possibly quite legal1 for an employer to install either hardware, software, or both, to monitor your activities at any level of detail they wish.

- If you're using employer-provided internet, then in addition to being your ISP, with all the power that entails, they may be legally allowed to monitor your traffic, even to the point of using techniques to intercept encrypted https traffic.

- When at your place of employment, your private equipment may or may not be subject to your employer's rules and abilities.

- Regardless of whether or not the company cares to monitor what you do, or even compromise your security, you'll still be required to abide by the companies' rules.

The best advice I can give here is to have a clear understanding of your workplace's rules and capabilities and follow them to the letter. Then, depending on your level of trust, take care to isolate anything personal from their network, equipment, and possibly even facilities.

Coffee shops and public locations
Open Wi-Fi at coffee houses is rife with well-known security and privacy issues. You likely already know what to do to stay safe using open Wi-Fi.

It's important to realize that those steps may not protect you from the owner of the coffee shop, or Wi-Fi provider. When using their internet, *they are your ISP*, and as such may have access to all the abilities I mentioned above.

To avoid the issues surrounding wireless connections, many people choose to use a wired connection instead. Unfortunately, the provider of that connection still has all the capabilities of an ISP, and could compromise your privacy and security. In the worst case, they could also be slightly incompetent, and expose your connection to other network users, making it just as vulnerable as open Wi-Fi.

Remember to treat any internet connection from an unknown or untrusted source with skepticism.

Shared connections
One scenario I often hear is what I'll simply call a "shared" connection. Sharing can take just about any form the name implies:

Using (with or without permission) the internet connection belonging to a neighbor.

Using the internet connection belonging to your host when visiting friends or family.

Using the internet connection provided by a landlord.

Etc.

Unfortunately, many people don't realize that each one of these situations, and many others like them, place the owner of the internet connection in the role of internet provider. In other words, they're the ISP, and once again have all the capabilities associated with that.

Keep this in mind: when visiting a friend, your ISP is not their ISP; your ISP is your friend.

4. Your online services

When we talk about privacy, many people immediately think of online services. Given the regular news reports we hear of breaches at major providers, it's important to keep the online services we use in mind.

But the topic is both deeper and wider than that. We often fail to consider *all* of the online services we use. On top of that, we fail to recognize that these services are themselves subject to various laws and regulations that can further put our privacy and security at risk.

Email
Email is a lifeline that almost everyone online relies on2. It's been around for decades, and represents what might be considered the first cloud service, before "the cloud" was even a thing. We regularly share our lives, our stories, and of late, our private information with friends, family, businesses, and more, all via email.

For the most part, email is all unencrypted. Our email provider can read it all. In fact, anyone with access to the servers between our email interface and our message's destination can access it as it passes through.

The good news is that there is so much email that, once again, we'd need to be pretty interesting for anyone to bother paying attention to what we have to say. Chances are, we're not.

I'd love to be able to provide a simple, easy solution, but I don't have one. Encryption is key, but email encryption is a mess. There are techniques, but they're often cumbersome and not universally compatible.

Most important to your privacy and security is to simply be aware of the limitations of "plain old email".

Social Media
Overshare much? When it comes to social media – meaning services like Facebook, Twitter, Instagram, and others – we are often our own worst enemies. Not understanding the ramifications of such visibility, people often share more than they should. This isn't just about pictures of the drunken party that come back to bite someone when they apply a job; it runs a range from unexpected embarrassment to online harassment.

Social media providers have a wide variety of terms and conditions that allow them to do pretty much whatever they want with the information you post. Most aren't interested in doing anything, but be it accidental or under legal pressure, providers have been known to take action that unexpectedly exposed more than the user intended.

The key things to remember when it comes to social media are:

You're probably sharing more than you think.
You're almost definitely sharing to more people than you think.
The provider can be compelled to provide your access logs and what you post to the authorities.
There is no "undo". Once you post something, it's stored somewhere, for much longer than you think.
Share wisely.

Storage
Cloud storage is awesome. It really is. As backing up is one of the themes I beat to death regularly, the number of additional options that online storage created is wonderful. There's little excuse these days to lose more than a few minutes of work, even in the worst of disasters.

With that convenience comes privacy and security issues.

The single biggest issue with cloud storage is that the provider of the storage service has access to your data. When you think about it, they *must have access* to provide the service. That, then, exposes two risks:

The service provider (or its employees) can peek at your stuff.

The service provider can be compelled to provide your stuff to the authorities.

One of the themes you might recognize here is the solution: encryption. For example, using a utility like BoxCryptor to transparently encrypt the files you store online ensures those files are accessible only to you.

Connectivity services
One of the solutions for many types of network risk is the use of a VPN, or Virtual Private Network. This is often a fine and appropriate solution. It ensures that your entire internet conversation, from your computer to the VPN service itself, is encrypted and hidden from prying eyes. It's a solution often recommended for people who travel a lot, who might need to make use of questionable internet services.

What most don't realize, however, is that using a VPN simply replaces one set of risks with another.

In a very real sense, the VPN service becomes your ISP. They provide a private, encrypted connection between you and their service. From that point, your connection continues onto the public internet.

The VPN has provided your connection to the internet, and like any ISP, that implies *they* can see what you're up to.

Many people focus on speed when choosing a VPN provider. VPNs add additional processing and latency to your online communications, and can slow it down – sometimes significantly – depending on the provider.

More important, I would assert, is choosing a VPN service you can trust. Not only do you need to trust their implementation of VPN technology, but also that they're not accessing, or otherwise allowing others to access, your data. Realize, too, many VPNs are based in other countries, or have a presence in other countries, which means they may be subject to the laws of countries other than your own.

Professional services
The banking industry frustrates me. In fact, I'll just say that I find the whole financial sector frustrating at times. While there are some good players out there who really understand privacy and security and manage it well, there are many who aren't quite as on top of things as they should be. Everything from sending out legitimate mail that looks like spam, to outdated password requirements that are fundamentally unsecure, much of the industry is still playing "catch up" compared to many others.

My feeling is, it's no real coincidence that many of the major hacks we hear about are in financial services.

Fortunately, your money is generally protected in the banking world. With other professional services, such as online bookkeeping, bill paying, financial reporting, and more, things are more haphazard.

When choosing an online professional service, or whether to use one provided by your bank or someone else, I'd recommend looking for a few things:

The ability to use arbitrary length password, including spaces.

The availability of two-factor authentication.

Telephone support that gets you to real people who speak your native language.

If applicable, the availability of real-time transaction alerts.

And of course, http**s**, and only https, on every related website and page.

Online services can be used safely. I use them myself regularly. But here more than anywhere else, privacy and security is a partnership between a service that knows what it's doing, and you, making appropriate security-related choices.

Account management
Once again, you may be your own worst enemy.

In my experience, most incidents of account hacking, theft, and loss are *completely preventable*. I see people making mistakes every day that eventually lead to account compromise. The service involved isn't at fault, and the hackers are simply taking advantage of those mistakes.

Ultimately, privacy, and most assuredly security, is *your* responsibility. You may feel like it's someone else's – the service, the software, or the coffee shop – but ultimately, **you** choose which services, software, and coffee shops to use, and you choose whether or not to use them in a secure manner.

Sometimes I wonder if people *want* to get hacked, because I see them neglecting the basics of safe account management:

Choose appropriate passwords.
Manage passwords appropriately to keep them private.

Set up account recovery, especially two-factor authentication, and don't let such options expire.

5. Your friends and acquaintances

One of the odder yet relatively common questions I get is whether video chat can be intercepted and recorded. The short answer is, as long as you're using a reputable service, it's highly unlikely.

But there's a bigger risk that most of the folks asking seem to overlook: the person at the other end. *They* can record it. It's a common method of extortion: someone is lured into a salacious online chat, which is recorded by the person at the other end, who threatens to release the video unless payment is made.

This highlights one of the greatest risks we face: the person at the other end.

I'm not saying they have malicious intent. But when you communicate with someone, your information is flowing across their network and devices as well as your own. Ultimately, we're assuming this other person is not being spied on, and knows how to keep his or her system and environment secure.

In addition, we're trusting they don't actually have malicious intent. Everything we send, every picture we share – even with a limited audience – they can in turn share with whomever they please, including the entire world.

Your Responsibility

At first glance, privacy and security issues may seem overwhelming and disheartening. It's easy to feel beleaguered, and even annoyed, that the digital world isn't a safer place.

Personally, I feel the privilege of playing and working on the internet, and the multitude of opportunities it presents, makes it worth staying on top of what I need to do to use it safely.

That includes learning who to trust, and taking the steps I need to take to keep my identity, reputation, data, and devices protected.

This article is republished, with permission, from the Ask Leo! Newsletter.

Smartphone & Tablet Apps - A Few Basic, Useful Ones

by Phil Sorrentino, The Computer Club, Florida
http://scccomputerclub.org / Philsorr.wordpress.com   philsorr@yahoo.com

Over 10 Billion Served. Remember this kind of advertising? It used to be said of hamburgers, but now it can be said of Android and Apple Apps. Apps, or what used to be called "Programs" or "Applications", are the software that makes Smartphones and Tablets do their magic. Apps either come pre-installed on the device, or are downloaded from either the Android Play store for Android devices, or the Apple Store for Apple devices. About two years ago, the Android Play Store boasted over 600,000 Apps, and the Apple Store said they had over 1 million. (The App number probably represents the total number of Apps and Widgets.) Recently, I checked and the Android Play Store is now the leader with about 1.6 million, closely followed by Apple, at about 1.5 million. That's a lot of Apps. We, as users of Smartphones and Tablets, typically use only a small number of Apps. I read somewhere that the average Smartphone user has about 90 Apps on their phone. I just counted the Apps on my phone, and I have 84 Apps and 27 Widgets. If you're not sure of the difference between an App and a Widget, talk to someone who has attended the Android Smartphones and Tablets class.

So, it's Apps (and Widgets) that really makes these devices worth the investment. Without the Apps, the Smartphone would just be like a flip-phone - a portable device used to make telephone calls, and Tablets might not even be viable products. The other factor that makes these devices so valuable is their ability to connect to the Internet. And, it is this connection that allows many of the Apps to do so many wonderful things. (Both Smartphones and Tablets can connect to the Internet via Wi-Fi, and the Smartphone has the added capability of being able to connect to the Internet through the cell phone towers.) But, back to Apps. (Because the Android family of devices has the lion's share of the market (around 65%), the rest of this article focuses on that family. However, much of the discussion of Apps, also holds for the Apple family of devices.)

Many of the Apps that you need to do basic things are pre-installed on the device, and available right out of the box. But many other Apps will have to be obtained from the Google Play Store (more on that in a minute). Because a camera is an integral part of both Smartphones and Tablets, a Picture Viewer is one of the very basic Apps. After all, most of us want to see the pictures right after we take them. (Instant gratification; can you imagine, it wasn't that long ago that we would send film away to a developer and we wouldn't get to see the pictures for two weeks, or so, after the pictures were taken.) Three popular and useful Picture Viewer Apps are "Photos", "Gallery", and "QuickPic". And by now, most of us realize that these cameras are capable of taking videos, as well as pictures, so a Video Viewer App is also a basic necessity. Two popular Video Viewer Apps are "Play Movies", and "VLC". And while we're talking of entertainment, most of us have digital music collections. The same digital music (.mp3 files) that we use on our home computers can be played on our mobile device, so you will need a Music Player App. Two popular Music Player Apps are "Music", and "Play Music". Another activity performed by these devices is to allow access to the internet, and as is similarly done on a computer; a browser is used for this. A browser is, maybe, not as useful on these mobile devices as it is on a computer, because when internet access is needed, the App knows the exact internet address to use. Apps rarely browse the internet; they typically do a limited set of things, usually with only one specific internet site. (For example, a Banking App only knows how to get to its specific Bank's Server and no other server, and similarly the OneDrive App only knows how to get to the OneDrive Server and no other.) But sometimes a browser is needed and so "Chrome", "Dolphin", and "Firefox" are browser Apps available for mobile devices.

Book reading is another form of entertainment that can be enjoyed with either a Smartphone or a Tablet, although the smartphone screen size may make this impractical. In order to read an electronic book, you will need a Book Reader App. The "Kindle Reader" App is a popular choice. With this App, electronic books of many different (file) types can be read on your mobile device. If you want to borrow books from the County Library, you'll also need a special App that helps you accomplish that task. This App is called Overdrive. These two Apps, for book reading, may not originally be installed on your device, so both of these Apps will have to be downloaded from the (Google) "Play Store". The

Play Store App is probably the most important Apps installed on your device. This App is pre-installed on all Android devices and provides the ability for you to download and install any of the Apps that are available at the Google Play Store, all 1.6 million of them. (By the way, most of the Apps that are popular and useful are free. Some Apps do have a cost, but it is typically low, usually under $10. All of the Apps mentioned here are free.)

One final App that I find to be useful is a File Manager. This may only be useful or interesting to those with a technical interest into the workings of the Android Operating System. But, if you are interested, this type of App provides insight into the organization of the files and folders on the device, somewhat similar to the way File Explorer provides insight into the organization of a Windows computer's files and folders. Two useful File Manager Apps are "Astro" file manager and "ES File Explorer". Both of these file managers provide a basic view into the Android organization, but not near the capability that is provided by File Explorer on home computers.

So, in summary, the basic useful Apps types are a Picture Viewer, Video Viewer, Book Reader, Music Player, Browser, and File Manager. A search of the Play Store will yield many, many possibilities, for each of these types. The specific Apps mentioned here are just suggestions to start with.

This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.

Open Source Software

by Geof Goodrum, Potomac Area Technology and Computer Society
www.patacs.org linux@patacs.org

crosti/Stitch Designer – v1.13.2. https://sites.google.com/site/crostiapp/.

Free GNU General Public License source code and executables for Microsoft® Windows®, Apple® macOS™, Google Android and GNU/Linux® by Sergey Levin. This tool allows you to make your own unique cross stitch scheme from a custom image. You can resize and rotate the image, reduce the number of colors, change image palette, make cross stitch scheme, preview it, save and print. Cross stitch scheme edits include changing colors and icons, adding new color, color fill, scheme pixel draw, lines and half-stitches.

Features include:

- Convert custom image to cross stitch scheme
- Edit cross stitch scheme
- Save and print the scheme that you created
- Input pictures: BMP, GIF, ICO, JPEG, JPG, MNG, PBM, PGM, PNG, PPM, SVG, TIF, TIFF, XBM, XPM
- Output cross stitch scheme: BMP, ICO, JPEG, JPG, PNG, PPM, TIF, TIFF, XBM, XPM, PDF, CST (crosti scheme text file)

Screenshots at : https://sites.google.com/site/crostiapp/desktop

jGnash – v2.24.0. https://sourceforge.net/projects/jgnash/.

Free GNU General Public License source code and executables for Microsoft® Windows®, Apple® macOS™ and GNU/Linux® by Craig Cavanaugh. jGnash is a cross platform personal finance application in Java.

Features include:

- Double Entry Accounting with reconciliation tools
- Budgeting with multiple scenario options and export to spreadsheet capability
- Investment Accounts and automatic import of Stocks, Bond, and Funds price history
- Nestable accounts with automatic rollup of totals and intelligent handling of mixed currencies
- OFX, QFX, mt940, and QIF import capabilities
- Reminders and automatic transaction entry and notifications
- Intelligent handling of multiple currencies and exchange rates with automatic online exchange rate updates
- Printable reports with PDF and spreadsheet export capability
- XML and relational database file formats
- Operates on any mainstream PC operating system

Screenshots at: https://sourceforge.net/projects/jgnash/

Kernel Source – v4.7. http://www.kernel.org/.

Free GNU General Public License source code for all platforms by the Linux community.

PDFsam – v3.1.0. https://sourceforge.net/projects/pdfsam/.

Free Affero GNU Public License source code and executables for Microsoft® Windows®, Apple® macOS™ and GNU/Linux® by Andrea Vacondio. PDF Split and Merge (PDFsam) is an easy-to-use desktop tool with graphical, command line and web interfaces.

Features include:

- Merge PDF files together
- Split PDF files specifying the page number
- Split PDF files specifying the level of bookmarks
- Split a PDF in files of the given size
- Rotate PDF files
- Mix two PDF files taking pages alternately
- Extract pages from PDF files

Screenshots at: https://sourceforge.net/projects/pdfsam/

SuperTuxKart – v0.9.2. https://supertuxkart.net/Main_Page.

Free GNU General Public License source code and executable for Microsoft® Windows®, Apple® macOS™ and GNU/Linux® by Joerg Henrichs, Marianne Gagnon, Jean-Manuel Clemençon and the SuperTuxKart Team. SuperTuxKart is a 3D open-source arcade racer with a variety characters, tracks, and modes to play, focusing on fun and ease of play.

Features include:

- Race with Tux and friends
- Explore several tracks
- Play against AI or in split-screen mode against your friends
- Play in various modes, including Time Trial, Grand Prix and 3 Strikes Battle

Screenshots at: https://supertuxkart.net/Pictures

This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.

All About Streaming

by Pam Holland, President & Instructor, TechMoxie
Pam@tech-moxie.com www.tech-moxie.com

Looking to detox from election news or just looking for more interesting content? Streaming is a great way to be in control of the what, where and when of what you view.

What is 'streaming'?
It is easiest to start with traditional TV viewing. There are two options: Cable or a digital antenna to pick up VHF or UHF channels. Streaming, on the other hand, is done via the Internet - the same service that brings you email, google, and access to websites.

Why is it called streaming? Because it flows to our devices much like water streams through our pipes. Due to variations in the speed with which data comes over the internet, a little extra is stored ("buffered") as we watch so that we see a steady stream of video. Otherwise what we are watching would start and stop with annoying frequency. Plus, the content is not downloaded and stored on our devices - it streams through and out.

You can stream content simply by going to your computer. Go to PBS or YouTube on the web and click a video - this is streaming. But sitting in front of a computer isn't terribly cozy.

Streaming from a TV - what equipment do I need?
Streaming can be done from any device that has an internet connection. Your computer, a tablet or a smartphone can easily stream video content. TVs can stream video if they are internet enabled. ("Smart TVs" are internet-ready). Older (non-smart) TVs can easily be connected to the internet by attaching a relatively inexpensive device such as a Roku, Amazon Fire Stick, Google Chromecast or Apple TV (most available for under $50). Roku device

Newer Smart TVs connect to the internet wirelessly over Wi-Fi, which is great if your TV isn't near your internet router. Older Smart TVs might need to be plugged into your cable modem - much like computers needed to be wired before Wi-Fi. If you have an older Smart TV, you might want to consider purchasing a Roku-type device which will allow you to connect the TV to the internet to wirelessly.

As Roku-type devices all connect to the internet wirelessly, you will need Wi-Fi. Newer modems include Wi-Fi capability. If you don't have a Wi-Fi modem, you can get one from your internet provider or an electronics store.

How to get content?
There are many sources for great streaming content. Some are free, but many involve a monthly subscription such as Netflix or Amazon Prime. We think it easiest to set up these accounts using a computer. Once your TV is set up for streaming, you can access your subscriptions by turning on your TV and Roku-type device or accessing the Smart TV functions. Roku, for example, will display a menu of available subscription services. Click on the service you subscribe to (e.g., Netflix) and you will be prompted to enter your user name and password. (Happily, you do not need to enter these passwords each time you watch!)

If you have cable TV, consider subscriptions that will supplement what you have on cable such as Netflix and Amazon Prime. For those who don't have cable TV (or want to eliminate it), consider a subscription to SlingTV which offers packages starting at $20 that include cable news, sports channels and other cable channels such as Comedy Central. Even HBO and Showtime can now be purchased a la carte via a monthly subscription.

One of the great advantages of these subscription services is that you can access them from any internet device. I often start watching a Netflix program on my computer and then continue later that evening from my TV. Netflix automatically saves where I left off.

What about "cutting the cord"?
Most of the cable companies bundle services (e.g., the Comcast's Triple Play) making your telephone and internet more expensive if you don't opt for the bundle. Cutting the cord is best for those who are willing to eliminate their telephone (landline) service as well. Doing a careful cost comparison is necessary. But, if you pay for premium content via cable, you might do better to stream that content rather than pay for expensive cable upgrade packages. One huge advantage of streaming is that subscriptions are month-to-month and therefore can be cancelled and restarted at any time.

This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.

Tracking And Third-Party Cookies

by Melanie Birnbom, Editor, Century Village Computer Club, FL
www.centuryvillagecomputerclub.com nbirnborn@yahoo.com

What are "tracking and third-party cookies?" Should I delete them? How can I prevent them from getting there in the first place? A cookie is a small bit of information a website saves on your computer when you visit. That's how sites remember your settings and preferences between visits.

For the most part, cookies are harmless. For example, news sites use them to tell which stories you read and suggest related or updated stories. Ad companies buy space on dozens, hundreds or thousands of sites, which means they can see your traffic habits and learn your likes or dislikes. All of this happens independently of the site you're actually visiting.

For example: third-party cookies enough to guess that you're a **(insert gender here)** from the **(insert location here)**. That's why you probably see ads for attractions or restaurants in your area.

It gets worse. If you browse a vegetarian blog that the advertiser buys space on, ads for steakhouses on sites you visit after that can disappear and be replaced by ads for vegetarian restaurants. The cookies could even track down allergies or food sensitivities you have and target those.

While you can delete the cookies, advertisers can hit you with them again if you don't change your browser's settings.

Each browser has a way to stop them:

Internet Explorer
Click the wrench in the top-right corner
Internet Options
Go to the Privacy tab
Click "Advanced"
Select "Override automatic cookie handling"
Click Block under third-party cookies

Microsoft Edge
Click the three-dot (Hamburger)
More Actions button on the top right
Select "Settings"
Click "View Advanced Settings" (you'll need to scroll down to the bottom of the page). Click the dropdown arrow under the "Cookies" field
Select "Block Only Third Party Cookies"

Firefox
Options
Privacy tab
History
Select Use Custom Settings for History where it says "Firefox will."
Uncheck "Accept third-party cookies"

Chrome
Click…
Three-lined (Hamburger) icon in the top-right corner of the window
Show advanced settings
Content settings in the Privacy menu
Choose to block third-party cookies and site data.

Opera
Menu Tab
Click
Settings
Cookies
Select Block third-party cookies & site data

This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.

Member Classified Ads

None this month. Please send any classifieds to the WYSIWYG Publisher at his e-mail address posted on page 2 of the newsletter.

SHCC Emergency Cancellation

Sterling Heights Computer Club meets at Macomb Community College (MCC). We will meet if MCC is open and will not if MCC is closed. MCC closure is announced with other school closings on many local TV and radio stations and on their web site. All members of SHCC have an email address. One of the SHCC officers will send an email to the addresses SHCC has on file alerting members to the event cancellation. If your email is broken, call an officer; don't leave a message, call another officer if you don't talk to someone live. It is your responsibility to keep the email address you have listed with SHCC current.

WYSIWYG WEB WATCH (www)

by Paul Baecker webwatch@sterlingheightscomputerclub.org

This column attempts to locate sites containing valuable, amusing, and free content, with no overbearing pressure to purchase anything. Club members are encouraged to submit favorite sites (a description is optional) to the e-address noted above, for inclusion in a future WYSIWYG issue. Also check the SHCC web site ("Web Page Reviews") for previous gems.

Experience the 3-year restoration and testing of the Canadian Pacific Railway's Royal Hudson 2816 steam locomotive, and its inaugural, and very scenic, run from Vancouver to Calgary. (Two 1-hour videos)
https://www.youtube.com/watch?v=X0-ni5Lz5hI
https://www.youtube.com/watch?v=oM5QV1cSctQ

Sell me something weird or confusing.
http://weirdorconfusing.com

Panoramic views of and from the Eiffel Tower in Paris, France.
http://www.toureiffel.paris/360-panorama-paris/index-en.html

Watch as hermit crabs trade living places. (4 min. video)
http://www.mypet.world/m/videos/view/Amazing-Crabs-Shell-Exchange-Life-Story-BBC

KDE explained: A look at Linux's most configurable desktop interface.
http://www.makeuseof.com/tag/kde-explained-look-linuxs-configurable-desktop-interface/

Free spreadsheet that tracks your investments and suggests when it's time to rebalance your portfolio. It is in GoogleDocs format, but can be downloaded in .xlsx and .odc formats. Select File...Download As..., and select your preferred file format.
https://docs.google.com/spreadsheets/d/1U7HoZMaPDIaq-4EeXqCljoQhkGm9T0Zt8WZPaYj6KKE/edit#gid=208315194

How to clean up your messy Windows context menu -- the hard and easy ways.
www.howtogeek.com/howto/windows-vista/how-to-clean-up-your-messy-windows-context-menu

HP Photo Creations is free software that lets you easily create photo books, calendars, collages, greeting cards and other keepsakes that you can print at home or have shipped to you.
http://www.hp.com/global/us/en/consumer/digital_photography/free/software/photo-creations.html

A few ways to get photos off of your Android phone. Do it before your phone fails, or its memory fills up.
http://www.pcworld.com/article/2048513/how-to-get-photos-off-of-your-android-phone.html

How to print from your Android device to any wireless printer. (8 min. video)
https://www.youtube.com/watch?v=rTiy-8axMCI&index=9&list=PL1t1XMSpVarf2OafxV2GZ9B2QcLaMOSB0

How to record phone calls on your Android phone -- And is it legal?
https://www.maketecheasier.com/record-phone-calls-on-android-and-its-legality

How to clear the pagefile with every shutdown in Windows 10.
https://www.maketecheasier.com/clear-pagefile-every-shutdown-windows10

What's the criteria to keep hackers out and keep your accounts safe? Here are six recommendations on how to create strong passwords.
http://www.geekersmagazine.com/create-strong-passwords-expert-tips-online-safety/

Learn how to use some Windows 10 Power Tools in this MS video course covering tips, shortcuts, and top utilities for Windows 10. (Much of this is also applicable to Windows 7 and 8.1 .)
https://mva.microsoft.com/en-US/training-courses/power-tools-for-windows-10-16405

Travelers who rely on public Wi-Fi networks or charging points are especially at risk of Cybercriminals attacking their devices. Here are seven tech travel dangers you need to know about.
http://www.techlicious.com/tip/tech-dangers-for-travelers/

What is a “zero-day" virus? How your anti-virus software could fail you.
https://www.maketecheasier.com/what-is-zero-day-virus

13 disappearing laptop ports and how to get them back.
http://www.laptopmag.com/articles/get-back-defunct-ports

Sysinternals is a suite of 69 MS Windows utilities with troubleshooting tools and help files to maintain your computer. See the included readme.txt file for individual tool details.
https://technet.microsoft.com/en-us/sysinternals/bb842062

Mounting hard disks and partitions using the Linux command line
http://www.makeuseof.com/tag/mounting-hard-disks-partitions-using-linux-command-line/

Free WizTree tool finds the largest files on your hard drive, with the option to sort every single file on your hard drive in order of size.
http://antibody-software.com/web/software/software/wiztree-finds-the-files-and-folders-using-the-most-disk-space-on-your-hard-drive/

How to digitize your cassette tape collection by transferring cassette tapes to your computer.
www.wikihow.com/Transfer-Cassette-Tape-to-Computer

The evolution of cell phone design between 1983-2009. Do any look familiar to you?
http://www.webdesignerdepot.com/2009/05/the-evolution-of-cell-phone-design-between-1983-2009/

How to upgrade to a new Linux Mint version. (Don't be too concerned that the sample screens are in German --- just follow the instructions.)
http://www.ghacks.net/2016/12/26/how-to-upgrade-to-a-new-linux-mint-version

60 vintage cars found after 50 years of neglect on French farm. (Photos and a video.)
www.boredpanda.com/treasure-vintage-old-classic-cars-france-roger-baillon

Raspberry Pi: The smart person's guide.
http://www.techrepublic.com/article/raspberry-pi-the-smart-persons-guide/

Free tools to split or merge music files.
http://www.makeuseof.com/tag/top-5-free-tools-split-merge-music-files/

Your wireless security could be at risk! Change your home router's default ID and password now.
http://www.worldstart.com/your-wireless-security-could-be-at-risk/

Are you doing everything you can to protect your personal information and devices? Check out these three short videos — to see what you’re doing right, and where your cyber habits might need some work.
https://www.consumer.ftc.gov/blog/3-videos-help-you-be-cyberaware

Useful tips to cool down an overheating laptop.
https://www.maketecheasier.com/cool-down-laptop/

Do you have a bank account that has had no activity for as few as two years, and now it's officially 'abandoned' per the government? What to do?
http://askbobrankin.com/hey_is_this_your_money.html

Lock-picking videos and tools, reviews of locks, locks to avoid (don't buy!), threat zones around your home, and more about home security.
https://lock-lab.com

Discover historic places and architecture across the U.S.
https://savingplaces.org

NOTE: Many of the links in the digital newsletter connect to the Internet if clicked. For those that do not, copy and past the link into your Internet browser.

World Wide Web Column on the Club Web Site

Check out the WebPageReviews section on the club’s web site. You can see past web sites reviewed in this column on our club web page. They are arranged into various key word categories to help locate a specific site.