Midland Computer Club

Midland Michigan

BITS AND BYTES

JULY 2020

https://mcc.apcug.org/

ARTICLE INDEX

GENERAL CLUB MEETING
Via ZOOM

Wednesday, July 22, 2020
6:00 P.M.

Is “Refurbished” Worth the Price?

News and/or Opinion from Paul Baecker, Newsletter Publisher & Editor
Sterling Heights Computer Club — October 2019 issue, WYSIWYG www.sterlingheightscomputerclub.org — newsletter (at) sterlingheightscomputerclub.org

I recently went shopping for a cable modem to eliminate the rental cost of the one supplied by my ISP. After doing some online research, I decided on a capable Arris model and found it at a local retailer. The store had some new ones but also had some refurbished ones for about half the price of the new ones.

I thought to myself, well, they’ve simply been returned by shoppers who had changed their minds because they didn’t like the color or style, and the units were probably basically unused. I inquired and learned that they had previously been used in a business somewhere (how would the salesman know?). So next I thought, well, do I want to save a few bucks by buying this so-called refurbished unit? Surely the items would have been repaired (if necessary) and tested by an OEM (Original Equipment Manufacturer) facility so that they operated as though they were new, even if they did have some wear marks on them. A no brainer to save the money, right?

But for whatever reason, I got a bit more inquisitive and asked about to what extent these items were refurbished. To the original manufacturer’s specifications? In this case, nope. Well, then, surely the store could vouch for the level of refurbishment done by the third party. Nope again. I learned that there are businesses that exist to refurbish electronic products to their own specifications, and they are not necessarily noted as to their relationship to the product’s original specs. My excitement in getting a great deal was gradually waning. Finally, the store rep tells me that they offer a 14-day return on a purchase of this item, but no warranty beyond that return option. I eventually passed on this offer. I figured that with my luck, the item would last past those 14 days, but die too soon thereafter.

I also checked the details on the web site of a popular online retailer of computers and accessories. I found similar statements about refurbished products being refurbished to the specs of the refurbishing organization. Some refurbished items came with warranties, some could be warranted at extra cost, and some items were ‘as is’ (such as demos) with no right to complain after the purchase.

So, what this adventure taught me is to carefully vet the retailer of any refurbished item you’re considering (whether electronics, furniture, appliances, etc.) and carefully study the purchase agreement and any (often hidden) disclaimers that apply to the purchase.

A definition I found online for the term “refurbish” is “to brighten or freshen up,”

Yikes!!!

This is an online article about doing your homework when shopping for refurbished products. You can snag discounts as high as 50% off on smartphones, tablets, computers and associated devices when looking for a refurbished unit, but you've got to do your homework. https://lifehacker.com/when-should-i-buy-refurbished-electronics-5885492

Need Help with Windows 10? Try Troubleshooting

Author: Nancy DeMarte, Vice President & Education Chair, Sarasota Technology Users Group
January 2020 issue, the STUG Monitor — www.thestug.org — vp1 (at) the stug.org

Microsoft has issued updates to its operating system for as many years as it has been in the software business. Early updates were primarily security-based. Later, feature updates were included on the second Tuesdays of the month. As Windows became more complex, some updates had errors or bugs which generated complaints from its users. A recent update, 1903, was no exception. First available in May 2019, it was a large update that included new security updates and new features. Immediately, some issues showed up in areas like screen brightness, audio, missing data, and loss of Wi-Fi connection. Most

home users did not have enough knowledge to fix many of these bugs. They had to wait for the next Windows update. (The current update is 1909, issued in November 2019.)

In August 2019, in response to customer suggestions, Microsoft made the 1903 download optional. Users with older computers were encouraged to wait a bit longer before installing this update. Revisions to 1903 came out often during the summer of 2019. My Update History told me that I had 10 updates to 1903 between May and September 2019.

The good news is that not only has Microsoft set up a system to fix problems more quickly, but it also has added some valuable new tools to provide help. One of them is called Troubleshoot. This is not only a helpful tool but also something that I, a moderately low-tech person, can understand and use most of the time.

How Troubleshoot works depends on the seriousness of the problem.

Critical Troubleshooting: If a computer has a "critical problem" like a computer crash, Troubleshoot will fix the problem automatically.

Recommended Troubleshooting: If you find you have a problem that is not critical, you can use Recommended Troubleshooting. Send a message to Microsoft with as many details as you have. At times, you may be asked to give feedback about your computer's operation. Microsoft will diagnose the problem and give you suggestions for fixing it.

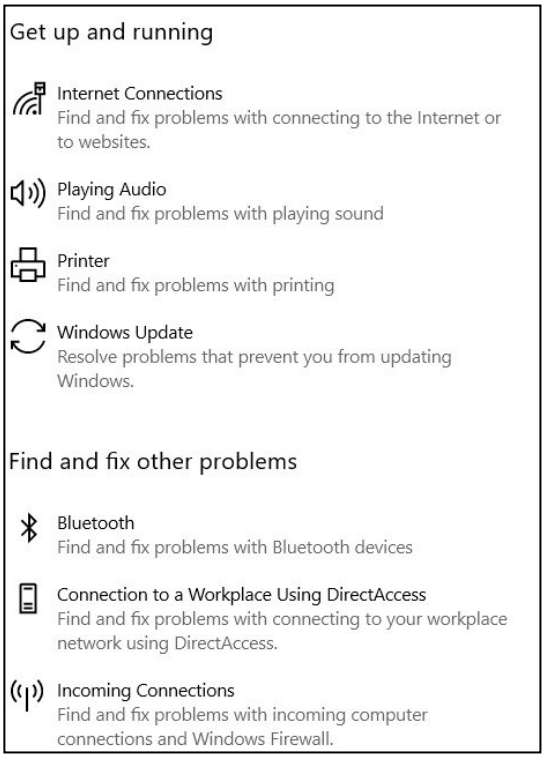
Data is collected from Windows computers on a regular basis. This diagnostic data can be either Basic or Full, depending on the amount of data collected. Basic diagnostic data includes information about your device and its settings, and how well it is working. This data is used to keep your device running reliably and securely. An example of Full data may include how you use your apps or websites that you visit regularly. Full data is collected from only a small number of computers. If you want to find out what data is being collected from your computer, you can download the Diagnostic Data Viewer tool. (Start > Settings > Privacy > Diagnostics & feedback.)

I had a situation that needed Troubleshoot a few months ago. I was trying out the dark mode/light mode feature (white text on a dark background or black text on a light background). At the same time, I was trying to change the color of the taskbar. (Not a smart idea) Before I knew it, I was stuck in the dark mode with a black taskbar. I sent my feedback to Microsoft and was given the steps to get out of my dilemma. To use Recommended troubleshooting, a user must have access to the Internet.

Recommended Troubleshooting has four setting options for the kind of interactions you prefer with Microsoft.

1. Fix problems for me without asking
   Windows will automatically run recommended troubleshooters for problems detected on your device without bothering you.
2. Tell me when problems get fixed
   Windows will tell you after recommended troubleshooters have solved a problem, so you know what happened.
3. Ask me before fixing problems (default) Microsoft lets you know when recommended troubleshooting is available. You can review the problem and changes before running the troubleshooter.
4. Only fix critical problems for me Windows will automatically run critical troubleshooters but won't recommend troubleshooting for other problems. You will not get notifications for known problems, and you will need to manually troubleshoot these problems on your device.

If you have Windows 10 update 1903 or 1909, you can find Troubleshoot by clicking Start (Windows key) > Settings > Update & Security. Click Troubleshoot and a list of possible problem areas will appear. (See illustration.) Select your problem area and click "Run the Troubleshooter button."



Partial list of Windows 10 Problem areas

Troubleshoot was created to address problems more quickly than waiting for the next Windows update. But if you would rather not have data collected by Microsoft, you can disable the Recommended Troubleshoot application. Click Settings > Privacy > Diagnostic & Feedback. Select “Only fix critical problems for me.”

If you want to see what problems have been addressed on your device, you can find a list in Settings > Update & Security. Under Troubleshoot, click “View History.”

If you need more help, try the new Virtual Agent. She may be able to direct you to a solution.

Staying Safe Online - A Rational Approach

Pam Holland, Founder and President, Tech-Moxie
December 2019 — https://www.tech-moxie.com/ — Pam (at) tech-moxie.com

We get *many* questions about online security. And we often get brought in to help clean up after an incident of fraud. As a result, we have developed what we consider 'a rational approach' to online security. Rather than focusing on all of the possible risks, we urge our clients to first address factors that present the highest risk. With respect to protecting from online risk, we apply the 80/20 rule. In short, 80% of the risk comes from 20% of the possible causes. In other words, if we just address the top possible risks, we eliminate the most common ways people are victimized online.

We suggest thinking about protecting your data as you might approach protecting your home. We all take reasonable steps to secure our homes; we lock our doors, close windows, and leave lights on. The goal is to *reduce* risk as eliminating risk is nearly impossible. The same is true in our digital lives. Taking small measures goes a long way towards keeping us safe, but it is nearly impossible to eliminate all risk.

Consider your personal risk factors. This is not unlike assessing your home for the risk of a break-in. If you live on the top floor of a high-rise, leaving your windows open does not present the same risk as if you were on the ground floor. With respect to your tech, do you have people regularly in your home that you need to protect your data from? Do you bank online? Do you have sensitive financial or other documents on your computer? Do you only use your computer for email? Do you or a family member have cognitive issues that might make you more vulnerable to fraud?

Based on our experience seeing the aftermath of fraud, taking steps to cover these six items will go far towards your online safety:

Use Unique Passwords. I know this isn't what many want to hear, but unfortunately, the risk in re-using the same password is increasing. A few years ago, the common advice was to create a unique password that was hard to guess. Today, the risk is not that someone will guess your

password - the fraudsters already know it. Large corporate data breaches (e.g., Equifax and Marriott) may have put our passwords into the hands of fraudsters. If you typically use the same password for multiple accounts (and worse if you have used it for years), fraudsters are more likely to be able to access your other accounts. To return to the home analogy, it is as if you have given out your key to numerous people over the years - it's now time to change the locks. Some options:

* **Use a password manager** - This might mean allowing Chrome or your Mac to save your passwords or using a third-party service like LastPass. I am often asked if they are safe. The only answer that I can really give is that they are safe until they aren't. I have chosen to allow my passwords to be saved on my Mac. For me, it has reduced my risk (because I don't need to reuse passwords) while (somewhat) saving my sanity. *But a caution: If others have access to your computer, they may be able to view your passwords.*

* **Write them down -** This works well for many. Of course, it is important to keep the passwords in a safe place.

* **Develop a unique naming convention -** For example, you might take a short phrase that you will remember then add something unique to that account site.

* **Make your passwords safer by using two-step authentication -** This is an option in most online accounts (email, Facebook, banking). How does it work? When you log in from a new device or location, you'll be sent a code via smartphone or landline. This makes it harder for fraudsters to log into accounts even if they have your password. To set up, go to the account or privacy/security settings in your online accounts.

***Never* Allow Remote Access to Your Computer** (unless you have sought reputable assistance like from Tech-Moxie 😉). Fraudsters would like nothing more than to gain access to your computer. They pretend to be from Amazon, Microsoft, Apple or another company you know well, offering to "help" you with a service issue. Assume fraud if you get an email, call or computer alert from a familiar company or government name. Once in your computer, they can access accounts and passwords. We have seen quite a lot of damage from these schemes.

Think Before You Click. Assume links in the email are fraudulent unless you can prove otherwise by checking with the sender. Fraudsters easily create emails that look like they came from a friend, bank or even the government. The email might be friendly (*"Hey, check this out"*) or intended to provoke anxiety (*"your Amazon order for a diamond ring has just shipped"*) or seemingly innocuous ("*your computer needs service"*). Fraudsters are hoping to get passwords or other personal information. Remember, customer service doesn't come to you! Instead of clicking, go to the website directly via the internet.

Beware of Pop-Ups A "pop-up" is a window or box that opens on your computer - often with a warning. Do not believe pop-up warnings claiming there is a problem with your computer. Never give them remote access. Warnings may claim to be from Microsoft, Apple or another company you are familiar with. What to do? Shutdown and restart your computer and the pop-up should be gone!

Update Devices Regularly. Companies like Microsoft, Apple and Google lookout for software vulnerabilities that fraudsters can take advantage of. They issue updates to fix these issues. Some devices may be set to automatically update, but others may require you to take a specific action. This applies to computers, tablets and smartphones.

Beware the Telephone. Scams change but follow common themes. Neither Apple nor Microsoft will call to alert you of problems. Government agencies such as IRS, Social Security Admin nor the local Sheriff will call claiming you owe money. If you are still in doubt, hang up and call the agency from a number that you have looked up independently.

We hope you find these tips helpful - and as always, we are here to help!

President's Corner

Tech Trek - Traveling with Technology
Part 2 - The Tech You Leave Behind

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

We all use a lot of technology in our everyday lives - various devices and services that make our lives better. They help us communicate, keep us safe and well, inform us, get us where we want to go, get us the things we need and entertain us. When we travel, we usually want to take all those benefits along with us.

Many of the tech devices and services we use every day are the “don’t leave home without them” kind you will insist on taking on your trips. Smartphones, laptops, tablets or e-readers, digital cameras, music players, noise-canceling headphones and GPS devices are all devices that can enhance your travels when you bring them along. Technology has revolutionized travel planning and arranging, with the Internet the main way most people now research and book transport, lodgings and entertainment for their trips. With the arrangements covered and the devices packed, many forget that technology can also help protect the home, possessions, resources and loved ones you may be leaving behind. The tech you take on your travels is important, but also important is the tech you leave behind.

The more you have, the more you have to protect while away. There are plenty of tech products and services to help keep your stuff safe and allow you to have peace of mind while traveling. Your home is often your biggest asset; no one wants to return from vacation to losses from theft or damage. Your resources and data need to be protected and possibly accessed safely while away. You may need to leave pets, elderly relatives or others behind, perhaps under someone’s care, while traveling. Knowing that everything back home is fine can help you have a more enjoyable trip.

Just as with trip planning, making arrangements to protect your assets while away must be done well in advance. There are lots of ways technology can help, but few benefits can come when planning starts the night before. Fortunately, the same things that can help protect your stuff while on a monthlong cruise can also be of benefit when you are just away for the weekend, or simply at work or out to the store.

Your local police can provide plenty of tips to help reduce the chances of your house being broken into while away on a trip. Things like making sure your doors and windows are closed and locked and ensuring your house looks occupied are just common sense. Having lights come on and off, making sure the landscaping looks maintained and not all dried up and preventing packages, newspapers, and mail from piling up out front are important in discouraging burglars from picking your home as a target. Technology can help with all of these.

A home alarm is one important tech item to leave behind when you travel. No matter how simple or complex, whether externally monitored by a company or only by the homeowner, any security system is better than no security system. While you can contract with a security company like ADT to install a system in your home and monitor it, there are also many good systems available for self-installation. Technology has made home security more capable and available at a low enough price point for everyone to have some protection.

I know a lot of folks that have the SimpliSafe system; it has come to define the moderate-cost self-installed security system. Amazon’s Ring Alarm Security System and Google’s Nest Secure are among

others competing in this same space. These systems start in the $200 to $400 range for basic setups, but more sensors, cameras, and accessories can always be added. They can be self-monitored or professionally monitored for $10 to $20 per month. Most can be part of larger smart home setups with other products, including voice-activated assistants.

Network home monitoring cameras are also useful ways to provide home security, with or without an alarm system. They can be set to inform you of unexpected activity or noise, like an alarm system. They are also useful for periodic checks on pets or family members left behind. They are typically Wi-Fi cameras and can be battery or line-powered, with prices ranging from $40 to $300. With apps for setup and monitoring, motion detection, video, and audio monitoring, media and cloud storage, email and push notifications and night viewing capabilities, they can be mini-security systems by themselves.

I've had and used network cameras at home for many years. Like a lot of tech products, however, no device or service is perfect or works perfectly all the time. I'm a big believer in diversity and backups for tech gear. On my most recent vacation trip with my wife, I had three different network camera types set up to monitor our home.

My oldest cameras are Samsung SmartCams; I've had three for about two years now. You can live-view from their web site (through IE only) or app, and store video on the internal micro-SD card or to their cloud account (subscription fee required). They have infrared LEDs for night vision and can be set to provide email or push notifications to your phone if audio or motion is detected (it can attach a captured image to the email, so at least you have that if the camera is taken). These work pretty well, but I have not found a way to set them up to completely avoid false triggers (I'd get a few each day). There were also a few days on our trip when something must have been wrong with their web service, as I could not access any of these cameras. Fortunately, I had others.

My wife gave me four Blink cameras for Christmas last year. At the time they were a private company, but now they are owned by Amazon. They are waterproof and battery-powered, so they are more versatile in terms of placement. Because they are limited by battery power, they should not be viewed in continuous video mode for long. I mostly take snapshots on them or use their motion detection to send notifications to my phone. They have free cloud storage, so you will have video clips to show the police if your cameras are taken in a break-in. The batteries are supposed to last 1-2 years under normal use. They work very well as a security system, less so if you just want to observe a live stream of someone you left at home.

My third camera is a Panasonic HomeHawk indoor camera. It is a lot like the Samsung, but is newer, costs less and seems to work a bit better. While its notification and recording functions seem to work well, its app menus make it less convenient to use. The Blink camera app is the most convenient, as each camera has a single button in the app to enable/disable detection, notification, and recording. For Samsung and Panasonic, you must enable motion detection and sound detection separately, in addition to notification and recording; these are on several app pages. The Panasonic camera seems to work well as a security camera, but like the Samsung, it is more difficult to switch between "home" and "away". It also can't preserve an image or video of a break-in anywhere but on its own internal memory.

Another important aspect of protecting your home is making it look like you are not away when you are. Lots of new smart home devices can help with that. There are sophisticated systems that can control lights and draperies, but simple and inexpensive smart bulbs and light controllers can provide much of the same capability. There are many companies that make these items. They are all typically connected through Wi-Fi, controlled through apps and almost always can integrate with Alexa and Google Home Assistant.

Again, for robustness, I currently use three different smart light products. Belkin makes Wemo smart home products, including smart plugs and light switches. I have several of these smart plugs with lamps connected to them. There are many companies making smart bulbs, which simply replace Edison-base light bulbs in lamps and light fixtures. I currently have smart bulbs from TP-Link and Feit Electric. These are easy to install and many have dimming and color-changing capabilities. While the apps often provide

the ability to schedule light events, on my last trip I simply switched lights on manually through the evenings with my apps. The apps give feedback that the light was switched, and I could also confirm this by looking at my network cameras. I've found these smart light products work very well.

For those with extensive landscaping, Wi-Fi smart sprinkler controllers can keep your irrigation going while away or at home. They often have rainfall sensors or weather monitoring capabilities to help save water as well.

Indoor water should also be considered for control when traveling. Many years ago, a good friend returned home from a trip to find a stream of water running down his driveway. A plumbing failure has caused a leak; his prolonged absence had allowed water to flood the inside of his home, resulting in major water damage and extensive renovation costs. Ever since I've always shut off the main water valve into the house (and shut off the water heater) right before leaving on a trip. It also serves as a plumbing test on our return; if I hear a flow when the valve is turned on again, it means I have a slow leak somewhere that I need to locate.

Leaks can cause damage anytime, whether you are away on vacation or just to the store, or even while you sleep at night. There are many new smart home electronic water shutoff systems available to continuously monitor and protect your home from water damage. Some, like Belkin's Phyn device ($600), are connected in line with your water supply pipe and can monitor the flow and cut off the water to the house if a leak is detected. Others, like the Guardian Leak Prevention System ($200), use water sensors placed at likely leak sources to automatically rotate your existing main water shutoff valve (no plumbing change required) and shut off the water. The Xenon Smart Wi-Fi Water Valve mounts on your existing water valve in a similar way, allowing your water to be shut off by Alexa, Google Assistant or through an app. The Streamlabs Wi-Fi Home Water Monitoring System ($140) takes a different approach, ultrasonically monitoring the flow in your home supply line (it clamps on the pipe with no plumbing changes) and alerting you via a notification on your smartphone to shut off your water valve manually. Even Zircon's $44 Water Leak Detector could provide a useful warning to your smartphone if it detects water where it is placed.

Electronic locks and safes can help provide additional protection for your home's contents and valuables while traveling. The Schlage Encode Smart Wi-Fi Deadbolt replaces your front entry lock and allows remote management of the lock through an app. This allows you to lock your door while on the way to the airport if you forgot to or let in a trusted friend to check on that possible leak while away. Electronic safes are great for locking away valuables and that computer backup you should have made before traveling; many are not expensive. A USB external hard drive with hardware encryption, like the Western Digital My Passport drives, provide an easy way to protect your most valuable data while away. Simply copy all your important data or backups to the encrypted drive and leave it with a trusted friend before departing (with encryption, you don't have to trust them absolutely).

While you can get a neighbor to pick up your newspaper and mail when on travel, some of us, unfortunately, may have closer relationships with fellow online gamers in other countries than with the people that live across the street. It is good to have a neighbor watch over your place, but if you are not sure you want your neighbors to know your home or apartment is temporarily vacant, technology can still help. I now get the newspaper electronically as a pdf so I can read it remotely, help the environment and avoid a pile of papers on the driveway while on vacation. You should contact the USPS to stop your mail delivery while you are away (you can set it up online). If you are concerned about mail theft, you can also sign up for Informed Delivery on the USPS web site. This allows you to view images of letter-sized mail that will be delivered to you and manage package deliveries. This could allow you to determine if mail is being stolen from your box.

No matter where you travel, you'll want to know everything you left of value will be there when you return. If you leave the right technology behind, you can monitor and control your home and property remotely and be assured there is no place like home to come back to.

Why Is My Computer So Slow?

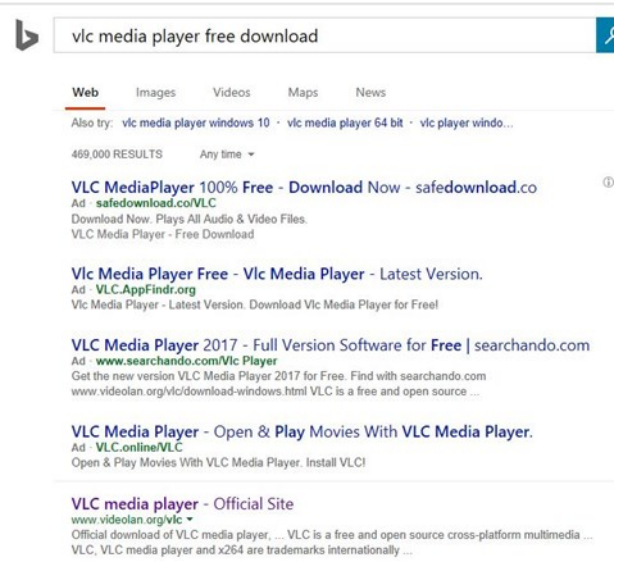
(Updated from April 2017)

Author: David Kretchmar, Computer Technician, Sun City Summerlin Computer Club
November 2019 issue, Gigabyte Gazette — www.scscc.club — dkretch (at) gmail.com

There are plenty of computers being used that are performing much more slowly than they should. One of the quickest ways to turn a fast, new computer into a slow system crippled by malware is to start downloading what you think is good software from the wrong sites, or by downloading the wrong software from what appears to be the right site.

Newer computers being slowed by unwanted programs is a bother, but the damage done by PUPs (Potentially Unwanted Programs) can be much more serious; PUPs can be responsible for programs that lock up your system and make it impossible to access any of your files, or otherwise ruin your system.

Every time you download anything from the Internet you first issue permissions that enable the opening of a conduit between the Internet and your computer. The series of complex events is mostly invisible to you, except for your clicking on that virtual button that starts the whole process.



Bing and Google searches often can take you where you don't want to go. When searching for popular software, sponsored search results (which result in unwanted programs) often appear at the top of the search results page, along with links from the actual software source sites. Often those ad links try to install software on your computer that you do not want. It could be anything; it could be a fake driver update program or a scam system cleaning program. Note that my Bing search for VLC media player (left) first showed 4 sites NOT associated with VLC – places that have a high potential for providing bad software.

Testing Misleading Advertisement links

How bad is it? To find out, I installed a fresh Windows 10, plus all Windows updates, on a freshly formatted hard drive. I downloaded and installed the free version of Avast! Antivirus software that brought a hitchhiker of its own - Google Chrome. OK, I wanted Chrome, but not every user would so I considered this an invasive act by a program I downloaded for protection.

I used Edge, Firefox, and Google Chrome and started using Google and Bing search engines to start searching for popular free programs. The programs I sought are often the first programs that get installed on a PC; Firefox, Google Chrome, OpenOffice, iTunes, Adobe Flash, Java, Adobe Acrobat, VLC, and WinZip. Then, I carelessly clicked on ad results, which appeared above or on the same first page as “real” search results. These paid ads were identified by notes and highlighted in a very pale color to differentiate them (slightly) from the actual search links that appeared nearby.

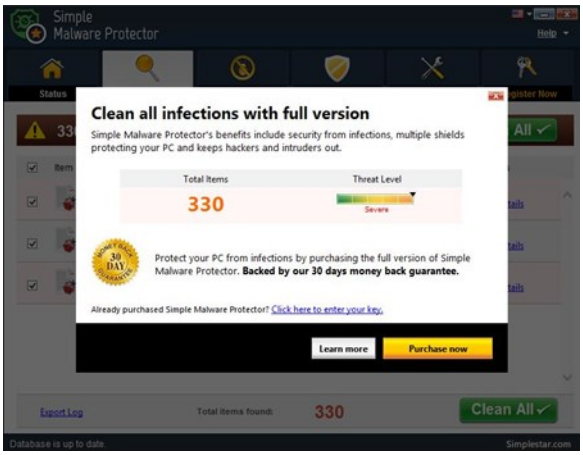
The ads didn't appear after every search and the ones that appeared varied among searches and were different for different browsers. Sometimes, the first paid ad link actually took me to the software's true source site (i.e. searching for Google offered www.google.com first). Often Avast would block a download it recognized as harmful, but Avast did not catch many problems.

For all of the searched for programs, I was able to bring up more questionable sponsored search results within seconds of repeated searching. Misleading results showed up in all search engines and I could not determine that any browser offered better or worse protection than others.

For each ad link, I clicked through and installed the respective programs via the link or button provided. Instead of delivering just the application I was looking for, all of the paid links attempted to tack on unwanted programs. In some cases, if I was careful to read all of the fine print and uncheck boxes, I could get the files I was looking for without a bunch of extra "added value" software, but it was very difficult.

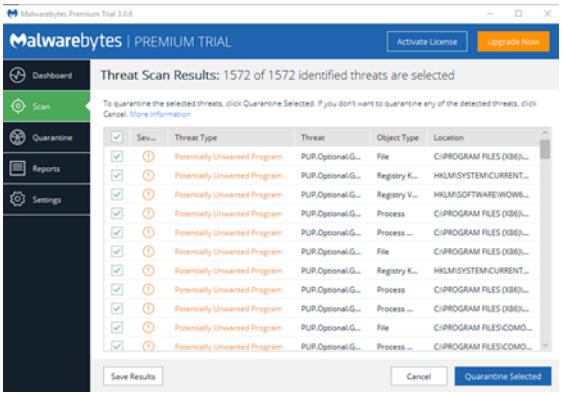
For the purposes of this article, I acted as an inexperienced user (or an experienced user who's not paying attention) and clicked my way through ads and dialogue boxes that looked like the End User License Agreement (EULA) we're used to seeing through when installing software.

And …They Got Me!



After installing just a few programs this way, I started accumulating browser toolbars (Bing, Yahoo, and Google) and noticed my search engine and home page had been hijacked to something unwanted. As I continued the process, Windows started slowing down to a crawl.

After installing all of the programs on my list, I opened Windows 10's Programs and Features and each browser's extensions and add-ons and counted 39 items that had been installed in addition to the programs I intended to get. On rebooting, three new programs launched popup windows at startup, including two that started running virus/registry scans as soon as they launched, and a couple that flashed warning windows and offered fixes if I registered and/or upgraded to the full paid version.



Remember this was originally a clean install of Windows 10 that needed nothing.

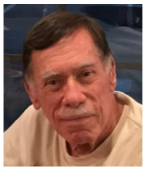
Within a few minutes, my computer became noticeably slower, plagued by numerous popups, and was becoming essentially unusable.

A Malwarebytes scan disclosed 1572 unwanted programs were present on my system. I'm sure not all of these were nasty, but if even a small fraction of them were, I would be in real trouble.

Conclusions and Recommendations

Most of us will occasionally have reason to download and install some third-party (non-Microsoft) software from the Internet. This does not have to be dangerous if you pay attention that the software is being offered from the true home site of that product. NEVER download software from any sponsored link unless the desired software creator is the sponsor.

Do not depend on your anti-malware program to protect you. It will catch some issues, but not all.



Wi-Fi Security – Which one, WEP, WPA, or WPA2?

Author: Phil Sorrentino, Contributing Writer, The Computer Club, FL
October 2019 — www.scccomputerclub.org — Philsorr (at) yahoo.com

Well, it finally happened. I tried to add another device to my home Wi-Fi network and I couldn't. I have been in fear of this happening for the last few years. No, it is not the fact that I tried to add one more device and that went over a limit. The limit on the number of devices you can have on a Wi-Fi network is only limited by the local IP addresses you set up, which was much higher than the number of devices I had on the network. I have had my current Router since July 2010. I bought it shortly after the 802.11n standard found its way into reasonably priced routers (around 2009). The "n" version followed the "g" version and increased the bit rate (speed) from about 50mbps to somewhere in the 100 to 300 Mbps area. (The actual speed you get from the router to a device is dependent on many things.) When I set up the Router I had a few older (legacy) devices that I still used. Some of those older devices didn't support the latest Security. So when it came to set up Security for the network, I chose the older Security standard "WEP." Although WEP is not nearly as secure as WPA2, every device supported WEP so there was no problem, until today, when I tried to add a device that did not support WEP. The new device, a security camera, only supports WPA and WPA2. So, now I have to change the Security used by my Router to either WPA or WPA2. This may not sound like much of a problem, but once I change it in the Router, I have to change every device that wants to use my Wi-Fi network. Yes, all the laptops and tablets, all the cell phones, all the Streaming devices, all the Smart TVs, all the smart bulbs and plugs, the wireless printer, any Wi-Fi extender access points, Alexa, Google Home, and all the phones and tablets owned by friends and family that use my Wi-Fi network when visiting.

The first thing I'll have to do is change the security used in the router. For this, I will need the Username and Password for the router. Many router's Username can be left blank and the default password is typically "Admin." (If you have changed either of these on your router, this is a good time to resurrect the correct Username and Password for future use.) Now, using a Browser, I'll go to the IP address of the router. Many routers use http://192.168.1.0 or http://192.168.1.1. Once at the router page, I'll put in the Username and password. Once in the router setup, I'll find Wireless or Wi-Fi Security and look for the Security type. Then I'll choose the desired Security type and put in a passphrase. I'll make a note of the new Wi-Fi Password for the future (a very important step). Now I can go around to all the devices that use the Wi-Fi and make the appropriate changes in their setups. Wish me luck.

So, what really is Wi-Fi security? Well, directly from Wikipedia "Wireless (Wi-Fi) security is the prevention of unauthorized access or damage to computers or data using wireless networks." Basically, Wi-Fi Security protects the data that goes between a Router and a Device. The device could be a computer, a wireless phone, a smart TV or DVD player, a smart LED bulb, any device that connects to the router, even a smart refrigerator. The most common types of Wi-Fi security are Wired Equivalent Privacy (WEP), and Wi-fi Protected Access (WPA). WEP, which is the older standard (Circa 1999), provides fairly weak security. It is well known that the WEP password can often be cracked within a few minutes with a basic laptop computer and widely available software tools. WEP used a 64-bit (or 128-bit) encryption key. The key was manually inserted into the device and it remained constant. WPA was introduced around 2002 to solve some of the problems with WEP. Even if your router is six years old, it most likely supports WPA. WPA2 is a further improvement over WPA and is the current Security standard. WPA2 employs an encryption algorithm that encrypts the data with a 256-bit key, the longest of all the keys used, and the longer the key the stronger the security. WPA also employs a per-packet key, meaning that it dynamically generates a new key for each packet that is transmitted. In early 2018, WPA3 was announced. WPA3 will have several security improvements over WPA2, but it will take some time for it to show up in routers and devices.

To use WPA or WPA2, you provide the router with a "passphrase" between 8 and 63 characters long –the longer the better. The passphrase can be a collection of alpha and numeric characters, including special symbols like $, %, and #. (Actually, if you are familiar with the ASCII code, all ASCII printable characters; those decimal values between 32 and 126 can be used. Which, by the way, also

includes “space”.) The router will then use the passphrase and the network’s name to generate unique encryption keys to be used on the network. The keys will constantly be changed to avoid being cracked. WPA2, the second version of WPA uses a more advanced encryption algorithm that is more efficient and more resistant to cracking. (All Wi-Fi products have been required to support WPA2 since about 2016. It was intended that WPA2 essentially replace WPA.) Although it is true that “the longer the passphrase, the stronger the protection, it may not be the practical way to go. A passphrase only 9 or 10 characters in length may be adequate for most home use. I can’t prove it, but I have seen some research that showed that it would take a fast PC over 15,000 years to crack a WPA2 passphrase of only 10 characters. (Maybe you could do it in a year with 15,000 computers.) That kind of security would probably be enough for most of us.

So, now that we know what’s behind Wi-Fi security, what shall I do about the original problem of what Security selection to use in place of WEP. Well, I guess the obvious answer is WPA2, as long as all devices support WPA2. Unfortunately, I may not find this out until I attempt to have all devices re-setup with WPA2. I only have a few devices that are older than six years old, so it may just work out. Wish me luck.

Postscript: The upgrade to WPA2 worked out just fine. Unfortunately, about 2 months later I had to replace the router. I had to do the whole upgrade all over again, so now I’m really good at updating all my Wi-Fi devices.

Windows FREE Snip and Sketch Tool is new and replacing the old

Author: Jim Cerny, Forums Coordinator
December 2019 issue, STUG Monitor — www.thestug.org — jimcerny123 (at) gmail.com

The new Windows “Snip and Sketch” tool was part of the Windows 10 October 2018 update. This tool is intended to REPLACE the old “Snipping Tool” of previous Windows editions.

But they (Microsoft) did something to actually help us users this time – they kept the old tool! So you can play and learn the new Snip and Sketch and keep the old Snipping Tool too! Maybe they learned not to force users into using updated or changed apps right away – we need time to adjust and learn, right?

Everything you could do in the old Snipping Tool you can do in Snip and Sketch, plus you get a few more tools and options. Thankfully these new additions are easy to see and use, and they can be ignored if you do not want to use them. Microsoft promises more options to come. Be sure to search Google for videos on how to use Windows Snip and Sketch! I am including here only the basic options.

Click on the Windows logo in the lower-left corner of your desktop and you will find Snip and Sketch in the alphabetical list of apps that appear. It is not inside the Windows Accessories folder of apps (where the Snipping Tool still remains).

I recommend dragging this app to your desktop screen to always keep it handy. But you can also open it anytime by holding down the Windows key + Shift key + S on your keyboard.

Upon opening the app, your whole screen goes gray and you will see the small controls rectangle at the top. Here you select HOW you want to select what you want to snip or capture. From left to right you can select a rectangular area, freeform selection, the entire window, or your full screen.

If you select the rectangle, you drag your mouse on the screen to select whatever you want. As soon as you release your mouse – presto, your selected image has been captured and saved on the clipboard to do with whatever you want!

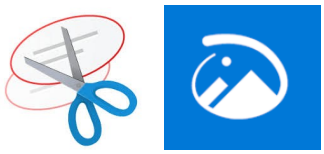
You can open a Word document for example, place your cursor where you want, and “paste” your clip right in your document. Or you can open the Windows Paint app and you can “paste” it there if you want to

do more editing. At the same time that your snip is placed on the clipboard, you will also see a message stating that you can edit, draw, or markup your selection.

Click to do that and Snip and Sketch opens in its own window with its own menu of options. Various easy marking tools are available for you to play with and try. There are highlighters and markers, and clicking on the down arrows will open things like color choices, etc.

Once you have “sketched” on your “snip” you can save it as a “.jpg”, “.png”, or “.gif” format by clicking on the old floppy disk save icon and selecting the file type you want.

The new Snip and Sketch is easy to use and very helpful for saving and sketching on any image on your screen for any purpose. Why not give it a try?



Interesting Internet Finds February 2020

Steve Costello — scostello (at) sefcug.com

In the course of 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 January 2020.

How to Make Gmail Your Default Windows 10 Email Client
https://www.techjunkie.com/gmail-default-windows-10-email-client/
I know I don’t want Outlook to be my default email on Windows 10, so as soon as I saw this post, I followed the instructions and can now use my Gmail account.

The Wonders Of Wordpad – Cyn Mackley
https://cynmackley.com/2020/01/15/the-wonders-of-wordpad/
You don’t have to go out and buy a word processing program or learn a whole office suite just to write simple documents if you have a Windows operating system. The Wordpad program is built right in. Cyn explains some of the basics in this post.

What Is Creative Commons & Explanation Of Each License
https://www.online-tech-tips.com/computer-tips/what-is-creative-commons-explanation-of-each-license/
Every once in a while I like to remind anyone who blogs, edits a newsletter, or wants to use information or photos, that there is a legal way to do so. There is a great amount of good information and images available for use under Creative Commons licensing. Check out this post to learn more.

How To Upgrade From Windows 7 To Linux
https://www.howtogeek.com/509508/how-to-upgrade-from-windows-7-to-linux/
With the last Windows 7 updates being January 14, 2020, there are probably some of you still wondering how to replace Windows 7. This post does a good job of showing how to upgrade to a Linux operating system. (Note: I ended up getting a new Windows 10 Home desktop, upgrading my Windows 7 Home laptop (4GB RAM) to Windows 10 Home, and setting up my old Windows 7 Home desktop (2GB RAM) as a dual boot Linux Mint 19.3 desktop to be able to still use some older Windows software, yet still be able to securely access the internet when necessary via the Mint O/S.)

The Best Antenna Set Up For Cord Cutters
https://thestreamingadvisor.com/the-best-antenna-set-up-for-cord-cutters/
There seems to be more and more interest in cutting the cord these days. If you are thinking about going with an antenna, you should check out this post first.

Is A Microsoft Office Subscription Worth It?
https://askleo.com/microsoft-office-subscription-worth/
If you have moved up to Windows 10 and thinking about Microsoft Office, check out this post from Leo Notenboom before making the final decision. Leo talks about cost factors in this post.

****

APCUG WORKSHOPS

The next series of workshops will be on Home Automation for Seniors—second Wednesday of the month at: 9 am PT, 10 am MT, 11 am CT, 12 pm ET

September 9, 2020
October 14, 2020
November 11, 2020
December 9, 2020

There will be how-tos, hands-on demos, and discussion with ample time for Q&A.

We will use the same Zoom password encrypted meeting URL for each workshop. You will receive the URL after you have registered by completing this form.

Judy will be the contact point for these workshops and will be available to assist you in connecting to the Zoom sessions.

The registration list will be used to identify everyone in the Waiting Room before being admitted to the session.

Week 1 - Why do I need it?
Week 2 - Where do I start?
Week 3 - Lights, doorbells, locks, and cameras
Week 4 - Doing It Myself vs Having It Done

We will begin by explaining why home automation is important to Seniors. What products are on the market, costs, security, and some real-world testimonials. In the second week, we will talk about how to go about planning your home automation project and best practices. In the third week, we will talk about applications using lights, doorbells, locks, and cameras. Lastly, we will talk about the benefits of making it a DIY project or having a professional install.
