BITS AND BYTES

Midland Computer Club

Midland Michigan

January 2016

http://mcc.apcug.org/

President Piper's Ponderings....

It looks like 2016 is going to be a great year for the Club. We have been having great speakers on great subjects and our meeting attendance has been good.

At the January Board meeting we shuffled the next couple month's projected meetings. January will be "To Back Up or Sync—What is the Difference". If you have more than one computing device (laptop, tablet or smartphone) you will be interested in this topic. The Cloud will also be covered.

February will be short subjects. Right now we have five topics, each about 10 minutes long. I will mention the exact titles at the January meeting.

The Board is thinking, again, of trying to use one of the APCUG online presentations for our March meeting. There are all sorts of topics available. Maybe we can take a poll at the January meeting of which topics you would like to watch. Our limited supply of speakers would like to be able to take a month off.

Bring your thoughts on the recent CES show. There have been all sorts of reviews, so check them out.

We might have a short poll in January of who uses which method of filing their income taxes. We should also mention all the scams going around with the IRS.

Bring your Windows 10 stories. It is here to stay, and Microsoft doubled-down on Windows 10 by dropping support for Windows 8.

See you Wednesday, January 27.

(The above comments are the opinion of the author and do not necessarily reflect the views of the Midland Computer Club.)

GENERAL CLUB MEETING

Midland Community Center, 2205 S Jefferson Ave, Midland MI
Room K111, Barstow Shipps Wing

Wednesday, January 27, 2016
7:00 P.M.
Topic: To Back Up or Sync—What is the Difference

2016 BOARD MEMBERS

MCC OFFICERS

President	Larry Piper	larryp56@chartermi.net
Treasurer	Jan Ensing	btiger6@yahoo.com
Membership	Gary Ensing	btiger6@gmail.com
Editor & Webmaster	Carol Picard	webbyte@yahoo.com

AT-LARGE BOARD MEMBER

Joe Lykowski joseph@lykowski.com

PROGRAM COORDINATORS

Howard Lewis lewis3ha@chartermi.net
Bill Tower tower.w@gmail.com
Please let Howard or Bill know of topics you would like covered at future meetings.

PUBLICITY

Al Adams aladams12@yahoo.com

Board Meeting

First Thursday of the month
7:00 PM
Chapel Lane Presbyterian Church,
5501 Jefferson Ave., Midland MI

Educational, Fun, and Interesting Web Sites (submitted by Howard Lewis)**:**

http://bit.ly/1vjr9yb
Politifact is supposedly a non-partisan, fact checking website. The also host pages rating the truthfulness of all of the presidential candidates. Most of the candidates aren't doing very good.

http://bit.ly/1lelW90
Harvard University has posted to their YouTube channel a series of lectures on "Understanding Computers and the Internet". Most of these lectures are about 90 minutes long.

http://kickscammed.com/
Kickstarter and GoFundMe are great sites for raising money for worthwhile causes. However, they are also excellent ways of falling for a scam. Kickscammed is a site that tries to publicize those projects which are scams on Kickstarter.

http://on.fb.me/234Be26
This Facebook page is like kickscammed.com except it focuses on scams on GoFundMe.

http://bit.ly/1vUfKEQ
A lot of people don't like drones. But I don't think humans dislike drones any more than the wildlife. Watch what this hawk does to this drone!

Membership Enrollment Form

NAME _____ *PHONE* _____

ADDRESS _____

CITY _____ *ZIP* _____

EMAIL ADDRESS _____

Membership dues FAMILY ($20) STUDENT ($15) New Member ____ Renewal ____

Please fill out the above form and mail it along with payment of check or money order to :

MIDLAND COMPUTER CLUB
1816 Bauss Ct
Midland, MI 48642-4023

Attn: Membership Chairman

You may also pay for membership at a regular club meeting

Tips, Tricks & Techniques: (submitted by Carol Picard)

Windows 10 has several settings that I review/customize when setting up a new computer. The following settings are system-wide (not user-specific) and you must be logged on to an Administrator account to make these changes.

Change Network to Public or Private
per-connection setting – have to be connected to specific network to make change

When you first connect to a new network, you are asked whether you want this computer to be visible to other computers. If you chose the wrong option, use these instructions to change.

wireless
This option does not always display. If switching between networks, may have to shut down, power on, and connect to network you want to change.
click Windows logo icon or tap Windows logo key
Settings
Network & Internet
Wi-Fi
Advanced options
under Make this PC discoverable
for Public Network, toggle: Off
for Private Network, toggle: On

wired
click Windows logo icon or tap Windows logo key
Settings
Network & Internet
Ethernet
Click on name of Ethernet connection
under Make this PC discoverable
for Public Network, toggle: Off
for Private Network, toggle: On

Windows Update Settings - change where updates are obtained from/shared to
Windows Updates can be downloaded once and shared between all the Windows 10 computers on your network. However, the default setting is to also send updates to PCs on the Internet, which can affect your data usage.
Search for: update
Windows Update settings
Advanced Options (under Windows Update)
Choose how updates are installed
Choose how updates are delivered
Updates from more than one place
Turn off, or, leave on and chose to get updates from and send updates to: PCs on my local network

Windows Defender – turn off sample submission if you don't want information automatically sent to Microsoft.
Search for: defender
Windows Defender settings
under Automatic Sample submission, toggle: Off

Check if Restore Point turned on
Have seen a few systems where this was turned off by default
search for: restore
Create a restore point
make sure Protection is on for the C:\ drive

Turn off Wi-Fi for computer that is always connected via Ethernet cable so it isn't searching for wireless
right click Windows logo icon
Network Connections
right click Wi-Fi
Disable

Disable Fast Startup
Fast startup helps start your PC faster after shutdown. However, updates that require a restart are not installed when using fast startup. Make sure to check notifications, which will indicate when restart required, or restart the computer at least once a month to make sure updates are installed.
To disable fast startup:
click Windows logo icon or tap Windows logo key
Settings
System
Power & sleep
Additional power settings
Choose what the power buttons do
Shutdown Settings
remove check mark before: Turn on fast startup (recommended)
[may need to click "Change settings that are currently unavailable", and may be prompted for UAC]

Metered Connection - prevent downloading updates over metered connection
per-connection setting and have to be connected to wireless network that you want to set as metered

click Network icon (right side of task bar)
Network settings
Advanced Options
under Set as metered connection, toggle: On

Change other settings for downloading over metered connections:
Printers:
click Windows logo icon or tap Windows logo key
Settings
Devices
under Download over metered connections, toggle: Off

Windows Store Updates – turn off Update apps automatically
launch Store app
click icon to left of Search Bar in upper right
Icon may be generic icon of a person or your Microsoft account image
Settings
under Update apps automatically, toggle: Off
This change applies to all networks, not just metered
If you turn off automatic updates, you need to open the Store app and manually install updates. You will not be notified when updates are available.

Automatically add new network devices on Private networks
If you don't want Windows 10 to automatically set up new devices on your Windows 10 computer when those devices are added to your network, you can change the setting.

search for control
Control Panel
Network and Internet
Network and Sharing Center
Change advanced sharing settings
under Private - Network Discovery
uncheck Turn on automatic setup of network connected devices
Save changes

Change computer name
When setting up previous versions of Windows, you were given the option to name the computer. That is not an option in Windows 10. If you want to change the name, recommend doing it as soon as possible after initial setup as it may cause problems for some applications, e.g., Office 365 subscription may not recognize name change.

search for sysdm.cpl
sysdm.cpl
Change…
Current Computer name will be highlighted, type name you want for the computer
OK

JANUARY TIDBITS FROM APCUG ADVISOR JOHN KENNEDY
January 16 2016

APCUG welcomes you and your group to a new year. I hope everyone is dealing with the winter in their area the best they can. We hope this turns out to be a "sweet 16" of a year for you. I wanted to share a couple of very important bits of technology information with you and hope you share it with the rest of your membership.

With the latest "Patch Tuesday" from Microsoft, some major changes in support has taken place. Effective now, Microsoft no longer will be supporting Windows 8 (the original). If any of you or your members are still running Windows 8, you will no longer be receiving updates of any kind. Windows 8 users will need to upgrade to Windows 8.1 to receive any critical, security, or program updates. REMEMBER, to upgrade from Windows 8 to Windows 8.1 you have to go to the Microsoft Store and not through Windows Updates. And to go to the store you need to have a Microsoft account. Once upgraded to Windows 8.1, you'll get upgraded to Windows 8.1-Update (what might have been called SP1 or SP2 if you call upgrading to 8.1 as equal to SP1) through the normal Windows Update system. This is all part of the plan of moving everyone they can to Windows 10.

Also in the Patch Tuesday updates is the announcement that Microsoft will no longer support versions of Internet Explorer less than 11. So anyone that is using Internet Explorer 7, 8, 9, or 10; will need to upgrade to Internet Explorer 11. The one exception is for those users still running Vista SP2, your IE9 will still be supported for a short time longer. If for some reason your version of Windows will not upgrade to IE 11, then it is recommended that you switch to using either Firefox or Chrome.

The exciting news to pass along is that the Winter Virtual Technology Conference is just weeks away. APCUG will be having another afternoon (for the East and Central time zones) filled with excellent technology presentations.

ARTICLE INDEX

Book Review: The Dark Net: Inside the Digital Underworld

Reviewed by Jim Scheef, Director, Danbury Area Computer Society, CT

The Dark Net: Inside the Digital Underworld
By Jamie Bartlett
2015 Melville House Posted on www.dacs.org – September 12, 2015 dacseditor (at) dacs.org

Cyberspace, if I may use that term, is often divided into distinct parts. The news media does this every day, providing convenient compartments into which they stuff everything from politicians to television programs to even criminals. The netherworld of the Internet is so far from our frame of reference as typical users, we cannot conceive what it's like. Of course that does not stop the news media. What we hear about in the news then is just the tip of the iceberg. The Internet's underworld is actually far worse than the news stories depict. Fortunately The Dark Net is well researched and written with sensitivity to the real people depicted in the stories. The author's thoughtful analysis makes this book a valuable read for anyone interested in the human side of the Internet. The author lives in the U.K. where The Dark Net was researched and written.

The Dark Net book has seven chapters plus significant Introduction and Conclusion sections. Each of these cover a significant part of the why and what of the digital underworld. The Introduction covers the impetus – what inspired people to write the systems that make it all possible. The cause was and remains liberty – individual freedom. In the 1980's, as the ARPAnet evolved into the Internet, users realized that this government-sponsored network made possible communication that seemed to be anonymous but in reality is not. Encryption is needed to ensure both privacy and anonymity. Phil Zimmerman provided one of these tools in the form of PGP or Pretty Good Privacy, a program for the exchange of encrypted emails. Ironically, the US government provided the research that led to TOR, or The Onion Router, a system of multiple proxies that first add and then remove layers of encryption making it virtually impossible to trace the origin of Internet packets. TOR was developed to allow secure US military communications. The same

technology has been implemented by volunteers all over the world to allow secure and anonymous communication all over the world, Chinese citizens, dissidents and whistle-blowers to mention just a few, can browse the web and communicate securely. Of course it provides these same features to criminals and terrorists. To use TOR you install the TOR browser and you are good to go.

Chapter 1 covers Trolls, the bullies of the Internet. Trolls date back to the formation of Usenet news groups, the original Internet bulletin boards. “Flame wars” soon followed where one or more people posting anonymously attack another user. Today this can be unmerciful bullying or worse. The author covers where a user is “doxed.” This is where the user’s true identity is uncovered and the user’s online behavior posted for the world to see and emailed directly to the user’s family, coworkers and employer. This can literally destroy someone’s life in the “real world”. I cannot give more detail in here; you need to read the book to fully understand the context. The most common trolling we see covered in the news is on social media between junior-high and high school kids. The suicides that can result from this online bullying show the depth of the harm.

We hear in the news about how “lone wolf” terrorists are perhaps the most serious threat facing society today. This is always followed by pundits talking about people becoming radicalized “on the Internet”. In Chapter 2 the author documents online forums supporting both extremes: the nationalists (sometimes “Christian”) on the right and the “antifa” or anti-fascists on the left who compete for control of cyberspace. Both sides use their forums and chat groups to fuel and amplify the prejudice and fears of like-minded people. Both sides infiltrate and spy on the other side. A few of these forums are on the regular Internet, but most can only be accessed using TOR making it essentially impossible for law enforcement to identify and locate these people. The book covers British groups thru the author’s interviews of people on both sides by email and in person. A must-read chapter.

Moving along, we come to the cyberpunks. These are the people who continue to develop new technology to solve problems of privacy and security. In this case security means freedom from state surveillance. The extreme of the cyberpunks are anarchists – the far, far-out end of libertarians. They see the crypto currency Bitcoin as a path to a future where people are totally free to live as they please without the constraints of government.

They may be right! Bitcoin’s ability to allow virtually instantaneous movement of cash between individuals, whether locally or across continents at extremely low cost can hide transactions not just from governments but from banks as well. Remember that governments cannot tax these unseen transactions. If an entire society were to adopt Bitcoin, it would de-fund government.

Even Bitcoin transactions must be recorded somewhere to prevent a same lump of currency from being spent twice. Any transaction must irrevocably transfer the wealth represented by the Bitcoin from one person to another. This requires that the transaction be recorded in something called the “block chain” but this record does not name the people involved as does a bank check or credit card. [Please accept that this is true as the mechanics of Bitcoin are way beyond this article.] The catch in this process is that at some point, you must buy your Bitcoins with dollars (or other currency) in an exchange. Bitcoins only exist as long strings of seemingly random numbers, so it is not possible to exchange Bitcoins for a national currency like Dollars without using a computer somehow connected to the exchange. These transfers become the anonymity weak points from which Bitcoins can be traced.

In Chapter 3 we learn about Amir, a cyberpunk, and his project “Dark Wallet” which aims to make these transaction points more anonymous. This is a world of mathematics and cryptography that dates back to 1976 when Whitfield Diffie and Martin Hellman invented the public key encryption that we use every day to keep our online banking and other transactions safe and secure. What we see here is that this and any other technology can be used for both good and evil. Yes, drug cartels can launder money but foreign laborers can avoid the vampire currency exchanges that charge exorbitant fees at both ends to send the laborer’s money to their family back home. Using Bitcoin the family can receive the money directly to a cell phone!

I'm going to skip Chapter 4 where the author discusses the darkest part of The Dark Net: the world of child pornography. I'll only pass on the author's finding that child porn had become almost impossible to obtain prior to the widespread availability of TOR. Unfortunately both the market for and the supply of have grown in recent years.

I found Chapter 5 to be the most interesting part of the book. Ross Ulbricht, the person allegedly responsible for the Internet market place, "Silk Road", was tried and convicted this past February. Except for the charge of attempted murder for hire, most of his crimes centered on excessive capitalistic free enterprise. Before the final gavel bang, several new markets, including "Silk Road 2", were opening for business in a much more competitive online market. The author makes a strong case for these markets as the safest place to buy drugs.

What is it about eBay that gives us the confidence to buy things offered by people we do not know? Well, eBay keeps track of both the sellers' and the buyers' reputations in the form of a "feedback score". You know to stay away from any seller who has received bad feedback from other buyers. The mere threat of bad feedback keeps sellers honest in the descriptions of their listings. The Silk Road brought this same concept to the world of illegal drugs. A dealer who shorts his customers or misrepresents the quality of the goods does not last long. A clever three party system of escrow ensures that buyers pay and sellers cannot just run away with the money, which, of course, must be Bitcoin. Silk Road can only be reached using TOR, making anonymity "virtually" assured for everyone involved. That virtually part came to an end for Ross Ulbricht after months of investigation by Federal agencies. Regardless of your opinion about whether drugs should be legal or not, Silk Road and its successor markets make buying drugs far safer than "scoring" in person on some street corner. If the "icky" parts of the book bother you, this is one of the chapters you must read.

Chapter 6, entitled "Lights, Camera, Action", is about another market-based, free enterprise part of the underworld, the world of web-cams where mostly young women provide live entertainment for a fee. I get the impression that most web-cam sites are not porn in the hard-core sense usually associated with the word. Instead entrepreneurial young women earn a few extra pounds (which is the U.K. currency) entertaining regular viewers in exchange for "tokens". Practiced as described in the book, everyone "wins" and no one gets hurt. Again, this is a chapter you must read.

The last numbered chapter is about websites and forums that are the opposite of self-help. Sites that promote anorexia, cutting or self-mutilation, and suicide all have the ability to make the unthinkable seem not just normal, but desirable. "Pro-ana" sites promote the eating disorder anorexia nervosa. I can't summarize this here, you must read it.

The Conclusion is a comparison between two men, Zoltan and Zerzan. Zoltan (his real name) wants to live forever. He wears a medallion inscribed with instructions on how to preserve his body for the freezing process he anticipates will allow him to "survive" until his mind can be transferred to computer memory – sort of like the movie Transcendence, but not really. Zoltan is a "transhumanist". On the other hand, Zerzan is an "anarcho-primitivist", the Luddite opposite who fears our society is sliding into dependency on technology and wants us to reverse this trend all the way back until society is mostly hunter-gatherers. The fascinating aspect to these polar opposites is that they both describe the same problem – we are destroying our planet. The difference is the solution.

From the conclusion: "It's their views about human freedom rather than technology that constitute the real dividing line between the techo-optimists and the techo-pessimists. For the transhumanists, there is no "natural" state of man. Freedom is the ability to do anything, to be anything, to go as far as our imagination can take us." … "For anarcho-primitivists, technology tends to distract and detract from our natural state, pushing us ever further away from what it really is to be free humans. It's freedom in a radically different sense: a freedom to be self-reliant, a freedom to be human without relying on technology."

The book is 240 pages plus 68 pages of acknowledgements, notes and suggested further reading. ISBN 978-1-61219-489-9. Released in the U.S. just a few months ago, it is available in book stores, both physical and online. I borrowed it from my local public library.

To SSD or Not to SSD? – That is the question.

By Phil Sorrentino, Member of The Computer Club, Florida
June 2015 http://scccomputerclub.org Philsorr.wordpress.com philsorr (at) yahoo.com

Whether 'tis Nobler in the mind to suffer the Slings and Arrows and stay with Hard Drives, Or to take arms against a sea of troubles and Convert to a Newer Technology (Solid State Drives). Well, maybe that's not quite what Shakespeare had in mind, but it does bring up the question. Should we begin to move to Solid State Drives in our computing devices? (Are we starting to see a replacement for the traditional mechanical Hard Drive?) Mechanical Hard Drives have been around since the beginning of Personal Computers. The IBM PC XT in 1983 included an internal 10MB (yes, that's Megabyte) hard disk drive. Anyone remember the name "Winchester Drive"? The term Winchester actually comes from an early type of disk drive developed by IBM that had 30MB of fixed storage and 30MB of removable storage, so the inventors labeled it a Winchester disk, after the Winchester 30/30 rifle, but I digress.

The question is shall we upgrade to SSDs? And I think the answer is "yes", where it makes sense. So, let's look at where it might make sense. Consider that our computing devices fall into the following categories; desktops, laptops, tablets, and smartphones. Right off the bat, tablets and smartphones only come with solid state memory, so there is no decision to be made there. So that leaves desktops and laptops for our consideration. Though the number of desktops and laptops are expected to drop over the next few years, many of us will have at least a laptop for the foreseeable future. (A forecast made by International Data Corporation, a provider of market intelligence for information technology markets, indicates that around 85% of the Worldwide Connected devices by 2017 will be Smartphones and Tablets. For the other 15%, Laptops will outnumber Desktops by about 2 to 1.)

So, let's look at why we might want to upgrade to an SSD in the first place. An SSD is a replacement for a traditional, mechanical disk drive. An SSD is a mass data storage device that uses solid-state memory to store non-volatile data for future access, in the same manner as a traditional hard disk drive. Traditional hard drives are electromechanical devices that employ spinning disks coated with magnetic material, and moveable read/write heads which "fly" over the disk at a height of less than 1 millionth of an inch. (A human hair is approximately 2,000 millionths of an inch.) In contrast, SSDs use microchips which retain data in non-volatile memory chips and contain no moving parts. SSDs allow for easy replacement because they are manufactured in the same physical form factor, and use the same electronic interface, as traditional hard drives. SSDs are typically more reliable, they are less susceptible to physical shock, and with no moving parts they are silent. But it is the fact that SSDs store and retrieve data faster than traditional hard drives that make them a desirable upgrade. On the down side, SSDs are more expensive and typically support a limited number of writes over the life of the device, which is probably only a consideration for a super power user.

So, let's consider the question of upgrading a laptop or a desktop. Two common reasons for upgrading either of these might be lower cost or some type of improved performance. Today, for larger SSDs, lower cost is not in the cards. In fact, currently, large SSDs (say 1TB) are about four to five times as expensive as the equivalent hard drive. A large 1TB traditional hard drive would currently be about $75 and a 1TB SSD would be about $400. However, for smaller drives (say 100GB) the cost difference is much less. A small SSD might cost only around $50 but here a comparison is difficult because traditional hard drives only start at around 500GB. So on the low end, the SSD begins to be cost competitive. (Keep this in mind when we look at the desktop upgrade.)

So with cost not an advantage, then the reason would have to be improved performance, and in fact this is where the SSD really shines. A PC with an SSD will boot in tens of seconds, definitely less than a minute. The same PC with a hard drive will take much more time to boot and will be slower during typical use. So, the PC with an SSD will boot faster, launch applications faster and will generally exhibit faster overall performance. A minor side benefit with the SSD is that there is no need for de-fragmentation; because of the way the data is stored, the effects of fragmentation are negligible. (In fact you should never defragment an SSD because the defragment activity will lower the number of writes available.)

Now that we know that the main benefit of an SSD will be increased speed, and to a lesser degree increased reliability (remember no moving parts), what else should we consider. First, let's look at a laptop upgrade. Most laptops have space for only one drive, so we should probably put in a drive large enough for the laptop's intended uses. With only one drive, the Operating System and Applications and Data all have to share that one drive. The OS and Applications could take 80 to 100 GB, so a 256 GB drive might be the smallest to consider. Currently, 256GB drives can be had for somewhere in the $100 to $150 range. For someone with large music, picture, and/or video collections, a drive closer to 1 TB may be in order. Currently, 1TB drives can be had for somewhere in the $350 to $550 range. It is always good to have more space, but with the price premium of SSDs it may pay to buy only what you think you will need. 512 GB may be enough for most users. Currently, 512 GB drives can be had for somewhere in the $250 range. If this cost is no problem, then the laptop upgrade probably makes sense.

Finally let's consider a desktop upgrade. (I bet the audience for this upgrade is a whole lot smaller than for the laptop, but let us press on.) The nice thing about the desktop is that there is usually space for multiple drives. Two, three, or four spaces are not unusual. In this arrangement, the C: drive can be separated from the other drives. This allows the C: drive to be only as big as needed for the OS and Applications (data can go on the other drives). Maybe 120 GB is all that is needed, so this upgrade may be less than $100. The other drives can still be traditional hard drives. With this mix of SSD and mechanical drives, the boot speed and the general operation will definitely be improved. (Although some data intensive operations where the mechanical drives are being used a lot may not show as much of a speed improvement.) This is a really inexpensive upgrade and it affords a lot of bang for the buck, so it, too, probably makes sense.

The Best Virus Protection…ever

By Phil Sorrentino, Member of The Computer Club, Florida
http://scccomputerclub.org Philsorr.wordpress.com philsorr (at) yahoo.com

Virus Protection isn't really a very popular topic, until you've concluded that your computer has just been infected by one of those nasty viruses. You know the symptoms: strange pop ups, abnormal operations, and/or very slow responses. It seems like computer viruses have been around for a very long time. As it turns out, computer viruses have been around longer than personal computers. Here is just a little computer virus history. The first experimental self-replicating program, called "Creeper", was written in 1971, and was intended to infect Digital Equipment Corp. (DEC) PDP-10 computers running the TENET Operating System. How's that for a bit of history trivia? Fast forward to the personal computer era, when in 1981 a virus called "Elk Cloner" was written for the then very popular Apple II personal computer. Followed, in 1983, by a very early Trojan Horse designed for the IBM PC. This virus deleted all of the files on the computer's diskette (remember 5 1/4'" floppy diskettes?), cleared the screen and typed ARF – ARF. (ARF was a reference to the common "Abort, Retry, Fail" message you would get when a PC could not boot properly.) Also, in 1983, the term "virus" was coined, to describe self-replicating computer programs. And in 1984 the operation of these viruses, that of including a copy of itself, was termed "infection". And so computer viruses have been with us, infecting our computers ever since.

The term "Malware, which is short for malicious software, is currently used as an umbrella to describe any software that is used to disrupt computer operation, gather sensitive information, or gain access to private

computer systems. (Malware usually does not include software that causes unintentional harm due to some design deficiency; that's just bad design.) Malware does not usually include all those programs that come along for the ride when you are downloading something of interest. These are typically termed Potentially Unwanted Programs, or PUPs. And, just for completeness, the term "spyware" refers to malware that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the owner's consent.

So, even though we all use virus and spyware protection, most of us, maybe all of us, have been the victim of some type of infection. So, what's a person to do when all of a sudden the computer seems to be operating strangely or unusually slow? Well, as most of you know there are a few very useful tools that you can try. Tools like MalwareBytes, SuperAntiSpyware, and Panda. Sometimes they may do the job, by eliminating or quarantining the virus, and sometimes they just may not help at all. What happens when they don't help? I know there are some very capable computer experts out there who have toolboxes full of very capable software tools that could probably fix any type of virus infection, but those experts may not always be available when you need them. And, virus removal by an expert may be a very costly undertaking.

So, we need to have a fall back plan for this eventuality if, or rather when, our computer becomes infected and there seems to be either no easy out, or the cost is too dear. This kind of plan would truly be the best virus protection. One plan of approach is to have a recent Image of the computer System, so that it can be restored to the computer. Yes, I know this will take time, and you will have to reload anything that isn't included in the recent Image, but this will always work, no matter what type of virus is present (as long as the virus hasn't been included in the previously saved Image). Note too, this is also a good solution for a crashed disk drive, a hardware problem. This is a good solution only if you have backed up all of your valuable data, but I'm sure you regularly do this.

There are a few ways to get a System Image. The first possibility is that you may have an original Image of your system. It may be a D: partition that may be called a Rescue or Restore partition or something similar, or it may only be labeled with the manufacturer's name. Restoring this Image will bring your computer operation back to the way it was when you bought it. Unless you've had an unusual early disk drive failure or just bad luck to have become infected with a nasty virus, this Image is probably not very "recent". If the computer has been around for a while, the update process that needs to follow the restored image will probably take a good amount of time. I've restored some computers that needed 12 to 14 hours of updates to get back to current operation. So, though this operation will always work, it may be very time consuming, and take a lot of patience.

The second way of getting a System Image is to use a commercial System Imaging application to create a system image whenever your software system changes (or at least every 6 months). Most of these have a one-time cost, usually between $40 and $50, but it will probably be less than an hour or two of an expert's time needed to try to remove a virus. Some of these applications are Acronis True Image, Paragon Hard Disk Manager, O&O Disk Image, Active@ Disk Image, and Macrium Reflect. If you create an Image every 6 months, your latest Image will always be less than 6 months old and the time to update the restored software system should be reasonable. Always keep the last 2, 3 or 4 images, just in case something unexpected happens to one of them.

The third way of getting a System Image is to use Microsoft's "Backup and Restore" software included in Windows 7 and 8.

–In Windows 7 you can find "Create a system image" on the Backup and Restore Applet, in Control Panel. Click this and you can select a hard drive or set of DVDs as the destination for the Image. An external hard drive is the best destination, but sometimes it feels good to have a copy on DVDs also. Once the destination is selected, select the C: drive as the Image, and finally click "Start backup". Make sure you get back to the Backup and Restore screen to "Create a system repair disk", which is what you will use to boot up the system in order to restore the Image.

–In Windows 8, you will find “Create a recovery drive” on the Recovery Applet, in Control Panel. Click this and click “Yes” at the “User Account Control” window, then uncheck “Copy the recovery partition from the PC to the recovery drive”, click Next, and then choose the destination drive, and finally click “create”.

Creating the Image in either OS is relatively straightforward. Restoring the Image is a little more complicated, but with perseverance and maybe some advice and direction from someone who has previously done it, it will be easy enough to do, and it will become routine. Now, with an Image on an external drive, bring on the viruses.

Is Windows 10 Spying on Us?

Sandy Berger, CompuKISS www.compukiss.com sandy (at) compukiss.com

Is Windows 10 spying on me? I have been asked this question over and over. My answer may surprise you!

There has been considerable publicity about Windows 10 being used as a spying tool for Microsoft. Blogs and even some fairly reputable websites have jumped on this bandwagon. Most of this publicity is aimed at making headlines to increase readership. As you well know, today’s news is dominated by racy headlines, even if they are sometimes trumped up. Some of this bad Microsoft publicity is focused on increasing public paranoia to sell products.

One of my followers recently sent me a copy of an audio interview of Dr. Katherine Albrecht in which she trashed Windows 10 in an article entitled “Windows 10 is full blown electronic tyranny.” Dr. Albrecht is a very intelligent, articulate, and well-educated lady. In this interview she says that Windows 10 keeps the microphone turned on all the time to bug homes and offices across the country. She says that Microsoft is making a copy of every file you create with Windows 10. However she also uses this interview to promote her Startmail product which is supposed to keep you safer.

Let’s see if I can negate a few of her claims. First, Windows 10 uses your microphone to let you verbally communicate with Cortana, their new virtual assistant. Cortana is not listening all the time unless you change the settings and request that she does so. With the default settings, Cortana will only listen when you press the microphone button just like you would press the home button on an iPhone or iPad to ask Siri a question. Also, it is very easy to turn Cortana off or alternately to turn off your microphone completely.

Dr. Albrecht also says that Microsoft is sending the entire contents of all Windows 10 hard drives to their servers. Simply put, Microsoft is not copying all your files or documents. In the last month Windows 10 has been installed on 75 million devices. If Microsoft were to keep a copy of every one of those hard drives, we would be talking about thousands of Petabytes of data. To give you an idea of how much data that is, it is estimated that the entire written works of mankind from the beginning of recorded history in all languages would take up about 50 Petabytes. Simply copying that amount of data would take years plus an astronomical amount of storage space and electricity.

Another complaint is that Windows 10 can be set up to share Wi-Fi passwords. Again this is not turned on by default. You must choose to use it, and when you do, you must authorize it and the passwords are encrypted.

I can sum up the reality of this situation in one simple statement. With Windows 10, Microsoft is doing no more snooping, spying, or collecting data than other large companies like Apple, Google, and Amazon. I have read the Microsoft Services Agreement, the Windows license agreement, and the Microsoft Privacy Statement carefully. I have also looked at several privacy documents from Google and Apple. They all have similar clauses.

The bottom line is that if you use any cloud storage like Microsoft's One Drive or Apple's iCloud, if you use an online email system like Gmail, Outlook, etc., or if you use services to sync your documents between computers and/or mobile devices, there is a copy of your data out there in the Cloud. Your cell phone provider, your ISP, your cable provider, your smart TV, and even your car knows a lot about you, as well. Facebook, Twitter, Instagram and other social media sites probably know more about you than you might ever expect. Most companies are using your data to learn more about you, whether to give you better service or to send you targeted ads. If they are subpoenaed, they will give your information to the lawful agencies, but then if you have drawn that kind of attention to yourself, those agents may be busting down your door and seizing your computers as well.

Right now Microsoft, Google, Apple, and Amazon are not spying on you or willfully giving the contents of your hard drive to anyone. Of course, an entire company could go bad, but currently you are at more of a risk from the bad guys and hackers than you are from the major companies. There are a lot of really good security people constantly monitoring the dealings of all the major companies.

So don't worry about Windows 10. It is no worse than Windows 7 or Mac OS X. If you want to be more secure, don't subscribe to any cloud services, don't use online email, and don't expect your data to sync between devices. If you want to be really secure don't access the Internet on your computer or tablet, don't use a cell phone, and don't buy a smart TV or any of the new Internet-connected devices, including a car.

Of course, if you do that you will be going back in time about 30 years. I know I wouldn't want to give up the knowledge, connectivity, productivity or entertainment that we have gotten from these devices.

If you want to keep using Windows 10, but want a little more security, here is how you can adjust the settings.

How to Set Windows 10 Privacy & Security Options

Sandy Berger, CompuKISS www.compukiss.com sandy (at) compukiss.com

Windows 10 has many Security and Privacy options that you can quickly and easily change. In fact, you have more control over these options in Windows 10 than you do in most other operating systems. Want to get started? Just follow these simple instructions.

Once Windows 10 is up and running, you can still set many of the Security and Privacy options. Just click on Start and go to the Settings, then click on the Privacy control panel icon.

You will see a long list of options and you can turn each of these off if you like.

In the Privacy area you can even quickly turn off the camera, microphone, and location information. And you can stop sending some information to Microsoft. Click on "Manage my Microsoft advertising and other personalization info" and you will get more information on how that works and also get the ability to turn off targeted ads.

Actually Windows 10 gives you more control of the privacy options than most other operating systems. As far as privacy goes, Windows 10 is no better or worse than many of the other operating systems that you use on your other connected devices. Yet, if you use Windows 10, you should check out the Privacy and Security options.

Tech Support Scam – Received a Tech Support call lately?

By Phil Sorrentino, Member of The Computer Club, Florida
October 2014 http://scccomputerclub.org Philsorr.wordpress.com philsorr (at) yahoo.com

This is a very nasty, and possibly costly, scam. It preys on people's concern that their computer might be running slow or might be infected with a virus or some other type of malware. It typically starts with a call from, ostensibly, "Microsoft or Windows or Dell or some other, known Computer Manufacturer's Tech Support" organization. And it can end with the computer owner paying for basically nothing, and giving the scammer his credit card information.

Let's make the point here: Microsoft says "You will never receive a legitimate call from Microsoft or our partners to charge you for computer fixes." So, never respond to a call of this nature; just hang up.

There seem to be many variations on how the scam can get started. Sometimes you will get a call from the "Microsoft or Dell Tech Support Desk" saying that they have noticed that there is a virus, or errors, on your computer. Sometimes it is started with a pop-up window on your screen while you are browsing the internet. The window (in a variety of different wordings) indicates that you have been infected by a virus and you should call a particular number to remove the virus. Calling that number puts you in contact with the scammer's bogus "Tech Support Desk". Once you are on the phone with the "Tech Support" technician, the scam begins.

This scam is very insidious because the victim may never even realize that he has been scammed. There are many variations on the details of the scammer's interaction with the computer owner once the call has been made; but basically the steps are: the scammer demonstrates, to the computer user, that there is a virus on the computer; the scammer offers to remove the virus for a fee ($199 to up to $549, which may be negotiable); the computer user accepts the offer to remove the virus and pays for it with a credit card; the scammer charges the credit card for the agreed upon fee; the scammer "fixes" the computer; the scammer demonstrates that the computer now has no viruses; the computer user thanks the "Tech Support technician" for his help.

The scammer uses a variety of ways to show you that there is a problem. One such ploy is; the scammer asks you to open the computer's Windows Event Log Viewer to show that there is problem. The scammer attempts to win your confidence by showing you that your system has "Errors". When you open the Windows Event Log Viewer, you see errors which lends credence to the scammer's statement that you have a virus. (The scammer relies on the fact that whenever you open the Windows Event Log, you will see some type of error or warning listed, which is quite normal.) Another way the scammer shows you that there is a problem is to have you view files that look like problems, but are really just views of a file that are not typically seen by the average user, but are quite normal. Still another technique is to have you run the Configuration Utility. You see "stopped" next to some services or programs and the scammer states that "the fact that those programs or services are stopped indicates that there has been some damage to the computer". (In truth, it is normal to have some programs or services that are stopped, which may not be obvious to the average computer user.)

So, how can we tell if a scam attempt is in progress? Here are some tip-offs to help you recognize a scam attempt. The first tip-off is that they, the scammer, called you. Note well that, Microsoft, Dell, or any other major company's tech support organization is not very likely to use their resources to get in touch with users to fix their computers. (The scammer may tell you that they are doing this as a Public Service; don't buy into it.) If a Tech Support issue arises with a computer, it is incumbent on the user to contact the appropriate Tech Support organization. The user should make the contact with a known phone number!

A very strong indicator that a scam attempt is in progress is that the "Tech Support technician" will ask you to go to a Website and Install a Tool so that they can Remotely Connect to your computer in order to "fix" the problem. This can be a very good, legitimate, way of having a legitimate Tech Support technician fix your problem, if you truly have a problem, and if you called Tech Support. (There are a few free remote

control software tools available just for this purpose, such as TeamViewer and GoToMyPC.) However, if they called you and you then give the scammer control over your computer, the scammer now has the ability download malware (viruses, rootkits, Trojan horses, key-loggers, etc.) to your computer. This malware could then lead to future problems.

This may be another tip-off: the Caller ID on the phone says “Microsoft, Tech Support”, or something similar, which gives the appearance of a legitimate number. Remember, he called you. (Spoofing Caller ID information, I’m told, is extremely easy to do, with Voice Over IP technology. Brighthouse or Verizon phones employ VOIP technology.)

A strong indication that a scam may be is progress is that the “Tech Support” technician claims that your computer is “sending out errors”, or is “sending out SPAM”, or is “infected with a new virus that is undetected by current virus protection software”, or something similar. This is an attempt to create fear that the computer is infected and to scare you into taking action to correct the situation.

Another tip-off may be that the Tech Support technician has a heavy foreign accent, but he uses a name that sounds like it is of western origin. He will definitely have an explanation for why he does this, but don’t buy into it. (Though, I have talked to a legitimate Tech Support technician, “Bob”, with a heavy foreign accent from Dell who was very helpful, so this may not be the best way to identify a scam.)

I haven’t gotten a call, yet, but I have heard of many recent experiences. If you do get a call from “Microsoft Tech Support”, just hang up. If you are having a problem with your computer, call the appropriate Tech Support organization, using a number you are confident is correct (not one that you get from a pop-up window). With the number of people in Sun City Center receiving these calls, this area code may be a prime target for these scams.

I’d like to thank Computer Club Member and Instructor, Matt Batt, for bringing the severity of this scam to my attention. Matt has seen the results of many of these scams and has heard of many computer users experiences with this scam.

Back To Basics
Fun with Spreadsheets

By Jim Cerny, 2nd Vice President, Sarasota TUG, FL
April 2015 issue, Sarasota Technology Monitor www.thestug.org jimcerny123 (at) gmail.com

Most people do not associate the word “fun” with anything like what a spreadsheet program can do, but I hope by reading this you will decide to at least open a spreadsheet program just to see what it can do and if it is really “fun” for you to use. I use a spreadsheet program to keep track of my monthly expenses. It is really simple to use for this purpose and helps you organize anything with numbers. Let me introduce you to the basic use of spreadsheets.

What is a “spreadsheet” program anyway? It is a program that allows you to organize numbers in a matrix array of boxes called “cells”. You can put ANY number or words in a “cell”. The beauty of a spreadsheet program is that it can do calculations and is easy to sort or change the contents of any cell. You have probably heard of Microsoft Excel (part of the Microsoft Office set of programs), but there are many other FREE spreadsheet programs that you can use as well, such as Google Drive (called “Sheets”) and Open Office (Google these to find out more about them).

What can a spreadsheet program do for me? I enjoy using a spreadsheet program to help me keep track of my personal home monthly expenses, my investments, and lists of club members. Although a spreadsheet program is intended for use with numbers, you certainly can use it to organize and sort a list of anything. Let me introduce you to a simple basic use of a spreadsheet by using one to track monthly expenses. I will use Excel 2013 in this example.

The basic elements of a spreadsheet. All spreadsheet programs work the same way. Once you learn how to use one, it is not difficult to use another. The basic screen of a spreadsheet (see sample) is an array of cells with the cell columns labeled with letters (A, B, C, etc.) and the cell rows labeled with numbers (1, 2, 3, etc.). Thus every cell has a unique "address" such as B5 or D3 for example. Above this array of cells are the many menus, tools, and options that are available for you.

Use your mouse to click on a "cell" in the array. You will see the "address" of that cell displayed just above the top row in the far left of the menu area. This is how you know what cell you are working with. The box or area to the right of the address is the "function" bar and it shows the contents of the cell here. You can enter and edit the contents of a cell in this area if you want, I find it most helpful.

For our example, I am going to put words in the first row and column cells. This serves to "label" or give a title to the numbers I am going to put into the other cells.

Click the mouse (the left mouse button) in cell A1 and then type in the work "Expense". In the following cells in row 1, click in each cell to enter in the name of the month. So in cell B1, type "January", in cell C1, "February", in cell D1 "March", etc. (see example).

In column A, in each row from 2 on down, enter the text of the expense (bill, service, or company) that you pay each month. So, for example, in cell A2 I will enter "Electric", in cell A3 I will enter "Water and Sewer", in cell A4 I will enter "Gas", etc. When I entered "Water and Sewer" the column was too narrow to hold all the words, so I had to widen the column. I did this by positioning my mouse on the vertical line between "A" and "B" (the mouse changes to a double arrow) and then I dragged the mouse to the right. I will end up with a list in column A of all my monthly expenses. All you are doing, really, is making a simple table with labels on the first row and column. This table will be filled with a number (your expense) in each cell.

Note that if you click on a cell to select it, the contents of the cell will appear above the array of cells in the "function" bar.

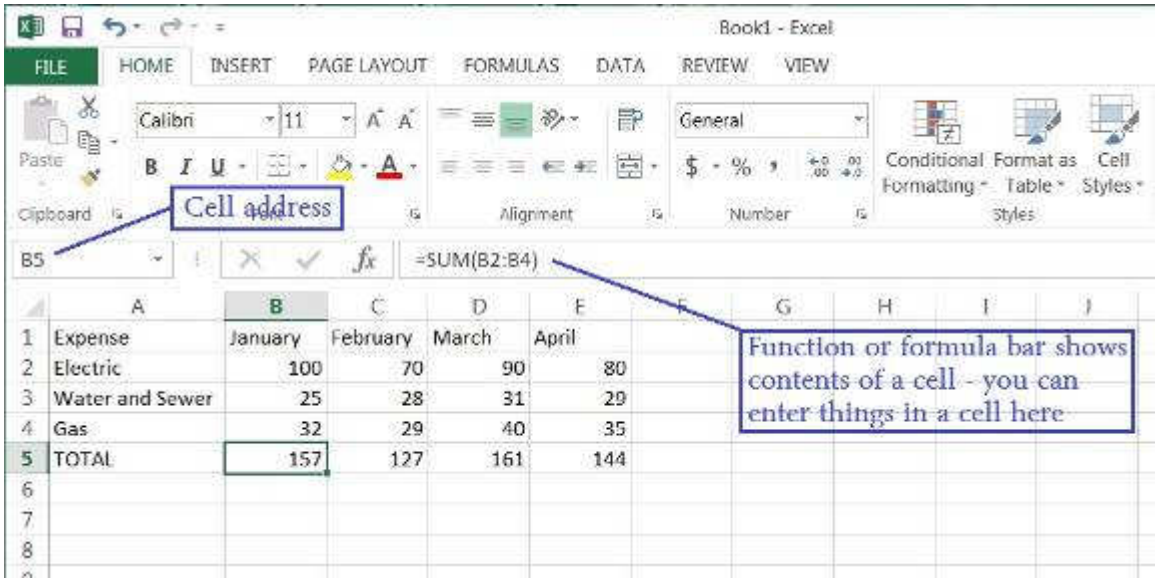
Enter numbers into the cells. Just click your mouse (left mouse button) on any cell to enter something into that cell. You can enter what you want in that cell by using the function bar if you wish. If you make a mistake, you can delete what is in that cell by hitting the "delete" key on your keyboard or use text editing. I did not use the decimal (the period key on your keyboard) in this example, but you can pick the "two decimal point" option if you want, and the "$" option as well.

Adding up the total. Now we come to the good part. You would like the spreadsheet to add or sum all the numbers in a column (or row). So, let's enter a new row label in column A as the last row in our spreadsheet and enter the text "TOTAL". In my example spreadsheet there are only three monthly expenses, so my "TOTAL" row will be row 5. You can have as many rows (and expenses) as you like. Now click on cell B5 which will contain my total of all the "January" expenses and I will enter the following FORMULA or FUNCTION into that cell: =SUM(B2:B4). You should enter this formula in the "function bar" at the top, above the spreadsheet, in the menu area. Note that the equal sign "=" indicates that this is NOT text or a number like we entered in our other cells, but a formula or function. We are telling it to ADD or SUM the numbers in all the cells from B2 to B4, and it will put the total in this cell, B6. In my example, you can see the formula that is in cell B5 in the function bar above. I find it easier to always enter things into a cell by entering it in the formula or function bar.

Try doing this in the remaining total cells in row 5, totaling the numbers in each column above.

What's the Big Deal Anyway? Well, the big deal is that you can organize and work with ANY array of numbers OR text. Not only can you total numbers, but you can average them or perform any mathematical calculation you want with them. It is easy to insert new rows or columns and the formulas will still do the calculations correctly. You can sort your spreadsheet by text (the "labels") or by numbers.

Your spreadsheet can look (that is, can be “formatted”) any way you want. You can color or highlight text, numbers, or cells; make the text larger, use any font, make the size of the cells any size you want, and much more.There are hundreds of formatting options and hundreds of “built-in” formulas and functions. Excel, for example, can even draw graphs and charts. Well, I will let the accountants use all the fancy stuff, I just want to track some of my basic expenses, and a spreadsheet is perfect for doing that. Why not give it a try? You can learn more about the spreadsheet that you are using by using the “help” option or by asking Google. YouTube will have many video lessons as well. Hey, maybe this can be fun after all!



	A	B	C	D	E
1	Expense	January	February	March	April
2	Electric	100	70	90	80
3	Water and Sewer	25	28	31	29
4	Gas	32	29	40	35
5	TOTAL	157	127	161	144

Interesting Internet Finds – July 2015

Steve Costello, President / Editor, Boca Raton Computer Society
www.brcs.org http://ctublog.sefcug.com/ editor (at) brcs.org

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 July 2015.

How To Create An Animated GIF Using Your Own Pictures, With GIMP
http://www.7tutorials.com/how-create-animated-gif-using-your-own-pictures-gimp

Have you seen animated GIFs, and wondered how you could make your own? This 7tutorials post explains how to do it (provided you have at least two pictures, of course.), using the free GIMP application. It should be similar with any good image editing software.

USB Type-C Explained: What it is and What it Can Do
http://www.guidingtech.com/45984/usb-type-c-explained/

I keep hearing about this more lately, so if you want to know more about it too, check out this GuidingTech post.

If You Give a Kid Linux…
http://fossforce.com/2015/07/give-kid-linux/

I thought it was interesting that kids who had no prior experience with any other operating system just took to Linux.

Still Getting Spam? 4 Email Mistakes to Avoid Today
http://www.makeuseof.com/tag/still-getting-spam-4-email-mistakes-avoid-today/

I still hear people complaining about how much spam they get. If you are one of those, or have someone close to you who is, check out this MakeUseOf post, and see if you are making any of the mistakes shown.

What is Wi-Fi Sense and should you be using it?
http://www.ghacks.net/2015/07/28/what-is-wi-fi-sense-and-should-you-be-using-it/

Wi-Fi Sense will be enabled by default with Windows 10, so if you are jumping into the upgrade, you should check out this Ghacks post first. (Note: I am going to wait a while before upgrading any of my machines to Windows 10)

Make Your Passwords More Powerful: Lessons from a Locksmith
http://www.groovypost.com/unplugged/make-passwords-more-powerful/

Learn from a locksmith about some things to do to make sure you are as secure as possible online. He explains that securing yourself online is pretty much doing the same type of things you do to secure your home or other property, only you are doing it with software and passwords rather than locks and bolts.

****

Most Fridays, more interesting finds will be posted on the Computers, Technology, and User Groups Blog:
http://ctublog.sefcug.com/tag/interesting-internet-finds/