THE WYSIWYG

October 2015 Volume 27, Issue 8

$3.00

STERLING HEIGHTS COMPUTER CLUB

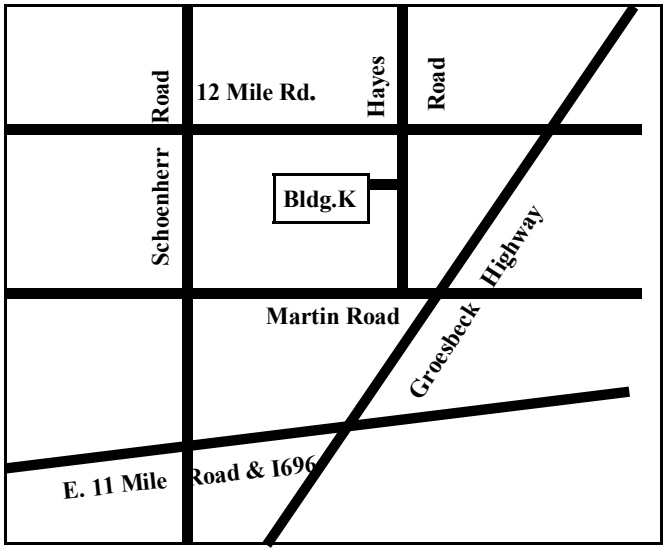
PO Box 385

Sterling Heights, MI 48311-0385

MAIN MEETING: TUESDAY OCT 6

6:30PM (new time)

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



IN THIS ISSUE:

This Month's Main Meeting Topic:

"The Latest in Video Surveillance" by member Jack Vander-Shrier

New club meeting time - 6:30 see page 3

PC SIG Meeting:

October 20, starting at 6:45 at the Sterling Heights Public Library

The meeting will be in the upstairs conference room this month, rather than the regular meeting room.

The SIG will plan to meet every other month, at this location, if people continue to attend.

Sterling Heights Public Library

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

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

DUES: $25/YEAR

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

Resource People:

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

2015 SHCC Officers

President: Don VanSyckel
V. President: Mike Bader
Secretary: Rick Kucejko
Treasurer: Paul Baecker

SHCC Coordinators:

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

Four Month Meeting Schedule:

OCTOBER 2015

6 - SHCC – "The Latest in Video Surveillance" by member Jack Vander-Shrier
7 - COMP meeting
4 - SEMCO meeting
? - PC SIG

NOVEMBER 2015

3 - SHCC – **"What's Hot for the Holidays" by Richard Tapaninen of Micro Center**
4 - COMP meeting
1 - SEMCO meeting
? - NOVICE SIG

DECEMBER 2015

1 - SHCC – **Main Meeting**
2 - COMP meeting
6 - SEMCO meeting
? - PC SIG

JANYARY 2016

5 - SHCC – Main Meeting
6 - COMP meeting
3- SEMCO meeting
? - Novice SIG

Other Computer Clubs:

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

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

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

Contact Information:

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

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

The President's Pen

by Don VanSyckel

There's a lot happening out there and much of it is under the radar. While we are busy having fun with our computers there are computers being deployed out there to do many other things. Many of the things that appear to help could actually have a black side to them. Let's look at a few of these.

Recently the perfectly good traffic lights at Mound and Metro Parkway were ripped down and new traffic signal were installed (with the help of federal money). The new stout and stiff poles have arms that extend out over the road. This is reported to be for mounting the traffic lights. This is all needed because the old setup was said to be totally inadequate. The reality of it is the sturdy non-swaying arms are suitable to mount cameras on. These cameras are capable of recording all the traffic that goes through the intersection. With the cost of storage going down and the capacity going up banking of history is feasible. I'm all for keeping an eye on traffic so issues can be responded to, but the resolution available and the storage is not needed just to monitor traffic. The system is designed to collect information about you and me.

Do you use Gmail? Many people and organizations do. Gmail is owned by Google. That is the organization that attempts to catalog all the information it can find on the web. Anyway, Google has massive amounts of storage. I can't quote a source but I've read several accounts that reported that Google saves all Gmail data; that's emails in and emails out. Combine that with government subpoena powers, and it gets scary. But before a subpoena is even needed, the Google management is sympathetic with certain reigning politicians so information gets passed quietly. Don't put anything important or incriminating in any email going to a Gmail account. There are other places to get email accounts on the web both for free and for a fee.

The third area I'll mention that is becoming computerized is the electric utility meter on you house. Their claim is it's a cost saving feature. To save money the meter needs to report the consumption for the month. One time, one amount. The meters being installed in the area go way beyond this. These meters are capable of profiling your electrical usage and in some cases these meters can determine the devices you have in use in your home. Another feature of these meters is they can receive commands from the control center. The last feature is a switch to turn off the power to your house. These last features the electric companies claim won't be used. Let's be frank, the more features a device has the more it costs. So the powers-to-be would like me to believe that an electric meter with extra features that won't be used but which costs more because of these features were purchased for the most cost savings. Also the claim is out there that their system can't be hacked by someone in China or Russia. If hacked and someone gets in they could turn off the power for hundreds or thousands of homes. I can certainly understand why the electric company claims they can't be hacked when other organizations such as the Pentagon, a major credit card company, and a major retailer have all been hacked.

The last area is personnel surveillance in and around your home. These systems can now report to a security service or be monitored by you from a PC or a phone. Computers make this possible. This is the subject of this month's meeting. The presentation will be "The Latest in Video Surveillance" by SHCC member Jack VanderScrier. Plan to attend this month and learn more about these capabilities.

Last Month's Meeting

Last month SHCC member Paul Baecker presented "Switching from Windows to Linux". Paul covered many programs that are available for PCs running Linux. Considering there are literally thousands of programs available, Paul just scratched the surface. He did cover a wide range of programs most people would use.

New Main Meeting Time

Club meetings will need to start at 6:30, and finish around 8:00. We all need to be done and out the building by 8:30.

Food is not permitted in the room before or during the meeting per our current rental agreement with the college.

Door Prizes

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

Tom Miller (from the June meeting) won a magnetic parts holder

Bill Appleberry (from the June meeting) won a surge protector

Mike Galat won a head lamp

Richard Monk won a pack of CD cases

Richard Jackson won a utility key

Ken Belbot won a USB optical mouse and keyboard

Rapph Osinski won a book titled "Speaking Geek"

Club Officer Election Announcement

It is time to re-elect our officers. Here is the process, the jobs, and responsibilities:

The nomination process is simple. Any member is eligible to run for any office. You can nominate yourself or have another member nominate you for one or more of the offices. All the offices (president, vice-president, secretary, and treasurer) are elected in November for a one year term, January through December. Nominations are taken in September, October, and November before the elections. The elections are held at the regular meeting closest to November 1st.

Only SHCC members can vote. The elections are held during the business portion of the meeting. The person with the majority of the vote for an office is the winner for that office. A person can only hold one office at a time.

The jobs of each office are flexible. Some are defined, some change from office to office depending on the officers' capabilities and availability.

The president is ultimately responsible of everything but being responsible doesn't mean the president has to do it all or even should. Delegation and management is all a part of the president's duties. The president makes sure the meeting topics are set, the speakers are prepared, writes thank you notes to presenters and door prize contributors, runs the regular club and officer meetings, takes phone calls from potential members and sends information to them, audits the monthly treasurer report and membership databases, tracks door prizes, and handles most of the publicity issues for the club. The WYSIWYG column is optional, but a great forum to pass along information to the members. The president also makes sure that the different coordinators are appointed and do their jobs. The president enforces the constitution and club's policies. The president does whatever things cannot be done by anyone else.

The vice president has the catch all job. So far to date the vice-president has not had to step in for the president, and there have not been any state weddings or funerals that they have had to attend. The person must be flexible and be prepared to run the main and officer meetings if the president cannot. This officer usually picks up a project or two during the year to lift the burden from other officers. The vice president arranges for meeting speakers, but help is available as needed.

The secretary maintains the membership database which is tracked in an Access database (SHCC owned). The secretary audits the treasurer report to make sure that the membership money collected matches the membership counts in the database, print the mailing labels for WYSIWYG mailing, prints a report for member check in at the main meeting, and maintains several reports such as a membership list. The secretary makes sure that sign-in table materials needed at each regular meeting are there early before people start showing up.

The treasurer maintains records for all the money taken in and paid out from the club's checking account. The SHCC currently uses Quicken (SHCC owned) to track the funds and generate reports for the officers. The treasurer also audits the secretary's membership counts. The treasurer makes reports to the officers at the officers meeting and four times a year to the club's membership. The treasure is responsible to get all SHCC funds into the checking account and responsible to generate checks for all expenses.

All the officers attend the officer meeting that takes place during the week after the main club meeting. The date, time, and location are flexible to the agreement of all officers. Historically these meetings have been at 7:30PM on the Monday or Tuesday after the regular meeting.

We hope everyone considers this invitation; this call to service. It does involve some work but can be a lot of fun. Normally it takes a few hours a month beyond the main and officers meetings. The president's job takes more, how much more depends on delegation. If you have any questions concerning the duties, feel free to contact any of the officers.

If your e-mail or mail address changes, please e-mail: secretary@SterlingHeights ComputerClub.org

This cartoon was reprinted with permission from the "How To Geek" online newsletter, available online at newsletter@howtogeek.com

New Security Exploits May Threaten 950 Million Android Devices

by Ira Wilsker

WEBSITES:

http://www.forbes.com/sites/thomasbrewster/2015/07/27/android-text-attacks/

http://bgr.com/2015/08/07/stagefright-android-vulnerability-check-app-fix/

https://en.wikipedia.org/wiki/Stagefright_%28bug%29

http://bgr.com/2015/07/27/android-security-flaw-mms-hack/

http://www.engadget.com/2015/08/07/stagefright-patch-detector/

https://play.google.com/store/apps/details?id=com.zimperium.stagefrightdetector

http://www.dailymail.co.uk/sciencetech/article-3189613/Millions-Android-phones-risk-software-installed-handset-makers-Certifi-gate-flaw-let-hackers-listen-conversations-steal-data.html

http://blog.checkpoint.com/2015/08/06/certifigate/

http://www.engadget.com/2015/08/06/android-certifigate/

http://www.ibtimes.co.uk/certifi-gate-massive-android-vulnerability-affects-hundreds-millions-smartphones-tablets-1514398

https://uk.news.yahoo.com/certifi-gate-massive-android-vulnerability-173000973.html

http://www.net-security.org/secworld.php?id=18730

https://play.google.com/store/apps/details?id=com.checkpoint.capsulescanner

http://www.independent.co.uk/life-style/gadgets-and-tech/news/certifigate-huge-android-vulnerability-lets-hackers-take-over-samsung-and-htc-phones-10445228.html

http://www.extremetech.com/extreme/157207-black-hat-hackers-break-into-any-iphone-in-under-a-minute-using-a-malicious-charger

http://www.computerworld.com/article/2473645/mobile-security/mobile-security-black-hat-it-only-takes-a-minute-to-hack-an-iphone.html

Recently at least two potentially frightening new exploits have been discovered that could threaten an estimated 95% of the one billion devices running the Android operating system. The good news is that as of this writing (late August), there have been no documented attacks on Android devices that take advantage of these two security vulnerabilities. The bad news is that now that information on these security vulnerabilities has been widely published as well as presented at the recent Black Hat hackers' and security convention in Las Vegas, it may only be a matter of time until some bad guys start to take advantage of these security vulnerabilities. Google, the progenitor of Android, was promptly made aware of the vulnerabilities as soon as they were uncovered, and has produced patches and fixes for many of the Android devices that have these vulnerabilities. The problem is that with the exception of a few models of Nexus smart phones supported directly by Google, it is up to the phone manufacturers or the cell phone carriers to release the upgrades and patches to close these vulnerabilities. At present, none of the major third party security software publishers provide any protection from these exploits, leaving many of us vulnerable to these exploits.

One of these newly discovered Android vulnerabilities was given the moniker "Stagefright" by its finder, Joshua Drake, vice president of platform research and exploitation at Zimperium. Drake first reported on the Stagefright vulnerability in April, disclosing his findings to Google, which quickly developed and provided security patches to its Android partners. Most of these Google partners who have not yet provided the patches to their respective customers may not do so for months, if they provide them at all; many phone manufacturers and carriers have explicitly stopped supporting and patching older Android phones, which are still in use by the millions. In several media interviews, as well as his Black Hat presentation, Drake explained that, "All devices should be assumed to be vulnerable." As stated in a recent (July 27) Forbes magazine interview, Drake said that he believes that as many as 950 million of the one billion Android phones currently in use may be vulnerable to the Stagefright vulnerability. Drake went on to say that only older Android phones running versions of Android below version 2.2 will not be potentially affected by this bug.

It is important for Android users to understand that Stagefright is not a virus or other form of malware that could infect a phone, but is instead a bug, or unexpected and unforeseen security vulnerability in the Android software itself. This vulnerability is in the heart of the Android software that processes, plays, and records multimedia files.

According to Drake, the security vulnerability may allow a hacker to illicitly access by simply sending an MMS message (text message) or multimedia file to the targeted device. What is especially nefarious about the Stagefright vulnerability is that it can be taken advantage of by a hacker without any action by the user; the victim

does not have to open or click on anything in order for the hacker to access his device. It is also theoretically possible for a hacker to capitalize on this vulnerability when an unsuspecting victim opens a purloined video file on a website. Once a hacker has taken advantage of this security gap in Android, he can access the victim's camera, microphone, and any data or images in the device's external storage. On some devices the hacker can also gain root access to the inner workings of the device.

In order to easily determine if a particular Android device is vulnerable to the Stagefright vulnerability, Zimperium has released a free "Stagefright Detector App", which is available from the Google Play Store.

play.google.com/store/apps/details?id=com.zimperium.stagefrightdetector

A similar detector utility was just released by the security software company Lookout, which it simply calls "Stagefright Detector". While these utilities will detect the vulnerability, it will still require a patch or other fix from the phone maker or the cell phone carrier which is supporting and updating the device. In full disclosure, when I first read of this Stagefright vulnerability and the availability of the detector, I downloaded and installed the detector. My year old Huawei Ascend Mate 2 phone, which had previously been upgraded by Huawei to Android Lollipop 5.1 (from 4.4), had the Stagefright vulnerability; coincidentally, just yesterday (the day before typing this column), I received a patch from Huawei which among other benefits, closed the Stagefright vulnerability on my phone. I reran the Stagefright detector from Zimperium to confirm the fix, and the vulnerability on my phone has definitely been patched by the recent update.

Another Android security vulnerability was disclosed at the recent Black Hat security convention. A well known security company, Check Mate, disclosed this newly recognized bug, which it named "Certifi-Gate", which may potentially allow a hacker to take control of a victim's phone by utilizing the "Remote Support Tools (RSTs)" software that was installed on the phones by the manufacturers, often at the behest of the cell phone carriers selling those particular phones. Check Mate promptly notified the device makers and cell phone companies of the vulnerability.

According to Check Mate, there are millions of phones and tablets made by Samsung, ZTE, HTC, LG, and other manufacturers which have incorporated this vulnerable "remote support" function software on their phones; according to Google, Nexus phones do not have this particular vulnerability. Using a security method known as digital certificates, which allows specifically authorized apps to have special access to the phone or tablet, only those authorized personnel could access these support apps in order to be able to provide the remote support capabilities. The problem now is that hackers can spoof or counterfeit these supposedly secure digital certificates, allowing them the same access to the internals and functions of the phone that had previously only been allowed to legitimate support personnel. Once the hacker has tricked the phone or tablet into accepting his spurious digital security certificates, he now has direct access to personal information stored on the phone, contacts, calendars, emails, text messages, and can turn on the microphone to remotely record conversations, track the location of the device and its user, and otherwise threaten the security and privacy of the victim.

While the device manufacturers and cell phone carriers were promptly notified of the vulnerability, it may be months, if ever, before they push the patches to this newly discovered vulnerability. Users can download a free utility which will show the user if his device is vulnerable to this remote support vulnerability. Written by Check Mate, the utility "Certifi-Gate Scanner" can be downloaded directly from the Google play store at:

play.google.com/store/apps/details?id=com.checkpoint.capsulescanner.

According to Check Mate, in order for hackers to take advantage of this vulnerability, the user must first download and install an application which contains the code which gives the hacker the access that he wants. The Google Play Store continuously monitors the apps which it makes available, checking them to make sure that they do not contain any malware. Check Mate advises, "We strongly encourage users to install applications from a trusted source, such as Google Play".

With the continual battles among users who seem to love arguing iOS and iPhones versus Android devices, iPhone users should not gloat over these Android vulnerabilities. At the Black Hat convention in 2013, which is where many hackers and crackers rub shoulders with security experts, the vulnerabilities of iOS devices, specifically iPhones, was discussed. In one of the presentations, despite the false but widely held belief that iPhones are immune to attack and are very secure by nature, researchers from the Georgia Institute of Technology were able to inject persistent, undetectable malware into iPhones, iPads, and other iOS devices using the latest generation of the iOS operating system. Using a modified USB charger, nicknamed "Mactans", after a type of Black Widow spider, the researchers were able to compromise any current generation Apple device in under a minute. These researchers first found this iOS vulnerability in 2013, and notified Apple of its existence, but there is some question that Apple still may have not yet fully patched this security vulnerability.

Check your smart phone for these vulnerabilities, and do not download apps from any source other than reputable

sources such as the Google Play Store or the Amazon App Store. Do not open any text messages from people that you do not recognize, although text messages can be spoofed just as emails are frequently spoofed. If you find that your device maker or phone carrier is providing a patch, update, or upgrade, strongly consider taking advantage of the offer and update your device immediately.

This article was reprinted with permission of the author, Ira Wilsker.

The Times They Are A-Changin'

by Greg Skalka, Under the Computer Hood User Group, CA
www.uchug.org president@uchug.org

In the 1967 movie "The Graduate", Dustin Hoffman's character was advised that plastics would be the future hot field. Today, I think the hot field to go into may be batteries. Modern technology is dominated by mobile and cordless electronics, which need batteries to supply their power. Cameras, smart phones, tablets, laptops, quadcopters, cordless tools and electric cars all depend on batteries for their primary power source. We probably don't realize, until the batteries go dead, how many of the products we use every day depend on batteries to run. That television on your wall (try using it for any length of time without a remote control), noise-canceling headphones on your head, wireless mouse in your hand, electronic safe in your closet, electronic safety light on your bike and Fitbit on your wrist all need batteries to run. So many other products, like your alarm clock, electronic thermostat and sprinkler timer, require batteries for backing up settings and timekeeping. We are awash in battery-powered products. Keeping all these batteries charged or changed presents a big challenge. And like plastics, they have the potential for harming our environment if not handled and disposed of properly.

Before we mastered electricity, our devices had to be human, animal, water or combustion-powered. Batteries actually predate the electrical grid; Alessandro Volta invented the first true battery in 1800. Early electrical innovations like the telegraph and electric lights were initially powered by batteries. It wasn't until the early 1900's that widespread commercial electrical power generation and distribution displaced batteries in most uses for electricity. Now with our thirst for mobile electronic devices and need for better energy storage, batteries are making a big comeback.

Battery technology has changed and improved over the years. Volta's zinc-copper voltaic pile has spawned zinc-carbon and alkaline single-use battery technologies, as well as many rechargeable battery types. New materials have increased the energy density and battery lifetimes for rechargeables. Nickel-cadmium (NiCd), nickel-metal hydride (NiMH), lithium, lithium ion (Li-ion) and lithium ion polymer batteries have allowed our portable devices to shrink in size and increase in capabilities. Batteries now come in many shapes and sizes, from tiny watch batteries to huge electric car battery packs. The standard AAA, AA, C, D and 9V cells have been supplemented with a multitude of custom sizes to suit new product applications, from large, high-capacity removable laptop batteries to super-thin, non-removable smart phone batteries.

Battery charging has become an important part of the life of every technology user. How long it takes dictates the time you and your cell phone must remain tethered to a wall outlet and determines when you may continue your electric car road trip. Higher capacity and the ability to swap batteries can help users, but eventually everyone must recharge. The most popular place in the airport terminal has become the seating next to the wall outlets. Unfortunately, every new electronic device adds another charging cable to your collection. The 5V USB socket has become the new charging standard for many devices. New upscale homes come with USB charging sockets built into the kitchen outlets; plug-in versions, like the Vivitar Home Charging Station, are also available.

No battery lasts forever. After many charge and discharge cycles, every rechargeable battery begins to lose its ability to hold a charge. Eventually it can hold so little energy that it is useless and must be replaced. For many products, battery replacement is very easy. Laptops and digital cameras have batteries that are easy to remove, and replacements are usually easy to find on the Internet. For other devices like tablets, smart phones and electric razors, changing the battery is much more difficult. Opening the device to get to the battery may be difficult and require special tools, and the battery is sometimes soldered in. Special knowledge is usually required to open the device without damaging it. Sometimes the product can continue to be operated by using it with power cord (like my electric razor), or with an external battery (like my wife's iPhone with a Patriot Memory Fuel+ portable charger). Eventually it may get to the point where either the battery or the device must be replaced.

Fortunately, the Internet comes to the rescue again, not only to help locate a replacement battery, but also to provide the knowledge required to make the change. Lots of step by step instructions and how-to videos are available on YouTube and other sites to help disassemble almost any battery-powered device. Replacing the battery saves the consumer money,

avoiding the purchase of a new product, while continued use of the device keeps it out of our landfills.

I recently had the batteries in two of my electronic devices go bad, requiring a change to continue using them. By doing some research on the web and spending around $20 total on replacement batteries, I gave new life to these items while postponing having to spend the approximately $120 in total to replace them.

An uninterruptible power supply, or UPS, is an almost essential accessory for a desktop computer. While a laptop's data is protected by a charged battery should line power fail while running with the ac adapter, you can lose data and risk hard drive corruption if a blackout occurs when using a desktop computer. A UPS contains a battery which is charged off the wall output and allows the computer and anything else plugged into it to run for a time if the ac is interrupted. The UPS typically monitors the battery's health and emits a loud tone when the battery is failing.

My desktop computer's UPS recently sounded its battery's death-call, so I shut it down and plugged the computer into a power so I could still run it while working on the UPS. I'd changed the battery before, and planned ahead by placing a label with the battery part number on the outside of the case. I found a replacement battery on Amazon for $12; a new UPS of this capacity would cost $40 to $50. Once I'd received the new battery, I removed a couple screws on the back to release the cover and reveal the battery. The battery is connectorized, so changing it is easy, as long as you observe the polarity of the battery connections. Once it was reassembled, it worked as good as new.

My second battery change was a bit more difficult. My Braun Oral-B electric toothbrush had been having charging difficulties for quite some time. The internal battery had developed a memory from going through repeated short charge-discharge cycles, and no longer held much of a charge. Fully discharging it and recharging helped for a time, but it was finally getting to the point where it was essentially unusable. Since it charges inductively from its wall unit, there was no way to use it in a "corded" manner.

I searched the web and found www.fixit1stop.com had a repair video for my toothbrush. It showed how to disassemble the toothbrush and change the battery. This was considerably more involved than the UPS. The case had to be opened to expose the plastic frame containing the motor, circuit board, battery and inductive charging coil. The NiCd battery was soldered to the internal circuit board. Fortunately, I am an electrical engineer and have the skills and tools to perform the transplant. For those that don't, this web site not only sells replacement batteries ($10 for my model's) but also provides a repair service ($25 for mine). I couldn't find the correct battery anywhere else, so ordered it from this site. When it arrived, I performed the replacement per their web instructions and, after a night of charging, the toothbrush worked great.

Batteries contain hazardous materials and must be recycled or disposed of properly. In many places it may be illegal to send old batteries to the landfill. Once again the Internet can provide information on battery recycling in your area. It turns out rechargeable batteries are accepted for recycling for free at many Best Buy stores, including the ones near me. They have a bin just inside the entrance, where I was able to deposit my two old batteries. There were a lot of recycling options for rechargeable batteries in San Diego, but I didn't find any place that accepted single-use batteries without a fee.

Batteries will continue to be an important part of our technology. To save money and the environment, consider changing the batteries in your electronic devices when they fail, rather than toss out the whole thing, and be sure to dispose of the old batteries properly.

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

New Product Can Eliminate Most Annoying Robocalls

by Ira Wilsker

WEBSITES:

http://www.consumerreports.org/cro/magazine/2015/07/rage-against-robocalls/index.htm

http://consumersunion.org/end-robocalls/problems/

https://www.nomorobo.com

http://robocall.devpost.com

https://www.ftc.gov/news-events/contests/zapping-rachel

http://www.consumer.ftc.gov/blog/if-first-you-dont-succeed

http://consumerist.com/2015/07/28/consumers-put-robocall-blocking-devices-to-the-test/

http://www.consumerreports.org/cro/news/2015/06/are-you-a-target-for-robocall-scams/index.htm

http://consumerist.com/2015/07/22/45-attorneys-general-agree-phone-companies-should-give-consumers-ability-to-block-robocalls/

https://consumersunion.org/end-robocalls/

http://consumerist.com/2015/07/07/ftc-and-florida-ag-sue-company-thats-allegedly-behind-medical-alert-robocalls/

http://consumerist.com/2015/06/18/fcc-votes-to-give-consumers-the-right-to-block-annoying-spam-robocalls-and-texts/

I have not heard from "Rachael, at Credit Card Services" recently, nor have I recently received the calls that I will receive a free medical call alert system. I am sorry to say that I will no longer be informed that I have won a free cruise nor will I be told that I can save having my mortgage refinanced at super low rates, or that my computer is infected with hundreds of viruses. The reason is that I am using a free service connected to my phones that automatically blocks most robocalls.

For several years, despite some internet rumors and hoaxes, the Federal Trade Commission's National Do Not Call Registry (donotcall.gov) has attempted to eliminate or minimize many of the "junk" phone calls that we receive on a regular basis. Just as many other laws on the books are only obeyed by honest people and ignored by the criminal element, honest telemarketers have generally followed the regulations promulgated by the Do Not Call program, but illicit marketers, phone spammers, crooks, and scammers still flaunt the law with a blatant disregard for us and our privacy. According to a recent article in the July, 2015 issue of Consumers' Reports magazine online, "Every month more than 150,000 consumers complain to the Federal Trade Commission and Federal Communications Commission about "Rachel from Cardholder Services" or Microsoft "representatives" warning about a computer virus. "Robocalls have eclipsed live telemarketing calls" as a source of consumer complaints, says Bikram Bandy, program coordinator for the National Do Not Call Registry ... . Aaron Foss, founder of Nomorobo, a call-blocking technology, estimates that 35 percent of all calls placed in the U.S. are robocalls. "For every 10 phone calls you get, roughly three to four of them will be unwanted robocalls," he says." Consumers' Reports continues, "Just to be clear: Robocalls refer to auto-dialed or prerecorded telemarketing calls to landline home telephones or cell phones, or unsolicited text messages to wireless numbers. Autodialed informational messages, such as those announcing school closings or weather alerts, are permitted according to the FCC, as are calls to landlines on behalf of nonprofit groups and political campaigns."

I have two distinct VoIP (digital phone service) phone lines from two different providers; one line is our primary family home phone line, and the other dedicated to important family communications. That second digital phone line only for important family communications has an unusual phone number, is provided from a very reputable provider that has a strict privacy policy on not releasing or publishing phone numbers, and only members of my immediate family have that phone number, fully cognizant to keep it confidential. That number has never been posted online, and should be reasonably secure, but over the past several months I have received countless robocalls on that line. My primary household digital phone line, using the same phone number that I have had for nearly four decades, was getting several annoying robocalls per day.

Recently, the number of robocalls and other junk phone calls that I have received on my two digital phone lines has decreased precipitously. I have signed up for a free robocall blocking service from Nomorobo (nomorobo.com). I read about Nomorobo in a recent column in the Consumerist (consumerist.com), an informational blog operated by the Consumer's Reports magazine. In a recent posting, the Consumerist (consumerist.com/2015/07/28/consumers-put-robocall-blocking-devices-to-the-test) reviewed several commercially available hardware devices and online services that claim to block robocalls and other unwanted calls. After reading the reviews I decided to sign up for the free service from Nomorobo. One of the reasons why I chose Nomorobo was the fact that it won the "FTC Robocall Challenge" (robocall.devpost.com), defeating several other hardware and software competitors.

Nomorobo offers its free blocking service for digital phone subscribers connected through most of the major digital phone carriers, including Time Warner, Vonage, Ooma Premier, AT&T U-Verse, Comcast Xfinity, Verizon Fios, and several other VoIP digital phone providers. Nomorobo is currently unavailable for traditional analog land lines and wireless phone services. Signing up for the service was very fast, and no credit card or other personal information was required. Simply choose your type of device and carrier, enter a valid email address, enter the digital phone numbers that are to be protected, verifiy the phone number, and the service almost immediately takes effect. Nomorobo detects and evaluates the caller on the first ring, and asks subscribers not to answer any call on that first ring, and to wait until the second ring before answering. Coincidentally, within five minutes of signing up and activating my Nomorobo service, the caller ID display on my phone, TV, and computer monitor showed a strange number as our primary digital phone rang once; it did not ring a second time as Nomorobo blocked the call. By the end of the evening, Nomorobo blocked three more calls.

Nomorobo only blocks illicit robocalls, and explicitly does not block or interfere with legitimate automated phone calls, and will still receive legal robocalls about prescription reminders, school closings, reverse 911 calls, doctor's appointment reminders, and other valid forms of automated calls. Just this morning I received an automated call from my pharmacy informing me that a prescription auto-refill was ready, and could be picked up,

that call getting through fine, not being blocked by Nomorobo. What is being blocked on a massive scale are the endemic telemarketing robocalls, often being made in clear violation of existing laws and regulations, frequently with "spoofed" (counterfeit) caller ID, and sometimes showing a faux local number on the caller ID. This deception is being done in order to deceive the recipient and encourage him to pick up the phone. According to the Federal Trade Commission (FTC), telemarketing fraud cost American consumers an estimated $350 billion in 2011, predominantly initiated by a robocall.

A pernicious robocall example that I have written about In previous columns here, have been about the robocall scams that victimized local individuals. One of the most common and most egregious robocall scams locally and nationally is from a foreign caller with a spoofed (often local) phone number falsely claiming to be from Microsoft, Windows Technical Support, Geek Squad, or some other legitimate sounding service informing the recipient that his computer is badly infected with viruses and needs to be cleaned immediately. Instructing the recipient to allow remote access to the computer, this pseudo expert (who is really a crook working on a fat commission of whatever he scams from the victim) takes control of the computer and appears to remove hundreds of viruses and other malware. Sometimes the thief also sells and installs useless security software for an extra cost, typically charging a fee from $39 to $600 on the victim's credit card. On several computers that I have personally cleaned after scammer does his nastiness, I have found evidence of identity theft (personal documents, email, spreadsheets, tax information, and other sensitive information downloaded by the crook), as well as new malware installed including key loggers to steal passwords and account numbers, a variety of software hijackers, and other malware. The crook also now has your credit card number, which is often resold on illicit websites by stolen credit card brokers. All of this damage done because the victim fell for the pitch in an illicit robocall.

According to the FTC, 77% of us find these robocalls to be very annoying. For those of us using digital phone services, such as those provided by cable companies, internet service providers, or third party VoIP providers (Vonage, Ooma, and others), this free robocall blocking service from Nomorobo (nomorobo.com) is definitely worthy of consideration. Signup is fast and easy, and the service can be stopped and discontinued at any time. If you are among the 77% that find robocalls annoying, Nomorobo may improve your quality of life by minimizing this common annoyance.

This article was reprinted with permission of the author, Ira Wilsker.

The Tip Corner

by Bill Sheff, Lehigh Valley Computer Group, Pennsylvania
www.lvcg.org nsheff@aol.com

Windows Sidebar Gadgets
Once we graduated up to Win8 the old sidebar gadgets introduced by Windows Vista can be considered a thing of the past. These Gadgets allowed you to do a lot of things such as see the weather, check the stock market and see how much strain you're putting your computer under. And there are a lot more out there. So for those of you who still have them on your computer here is way to uninstall them if they get too crowded.

Click Start and in the Search Box, type Gadgets. The gadget window should open up.

Now, right click on the gadget you want to eliminate and select Uninstall. A confirmation window opens up, so just click Uninstall again.

Balloons, Pop-ups and Tooltips
What's the difference? Well, regardless of the size, shape or color they are all known as screen tips.

So when you see a little text box that pops up over an icon, or a yellow balloon like you see in the comics, or read about a 'description' don't worry about what they are called. If they provide information when you hover over an icon or right click on something relax, you are looking at a screen tip.

Windows 8 Terminology
When is an icon not an icon? When it is a Charm, a Tile or an App.

OK, we know that any small picture is an icon (or GUI) which represents a program or a file. In Windows 8 there are three types of icons that are used, and each has a specific name. First we have the charms. This is a group of five icons called Search, Share, Start, Devices and Settings. When you look at a Windows 8 start screen they are not visible. To open the Charms Bar you can either press the Windows key (Windows 8 keyboard key)+ C key, swipe from the right side of the screen (touchscreen) or with a mouse, point to the upper-right corner of the screen. The charms menu opens on the right edge of the screen.

The charms provide access to the following:

Search charm - Search for apps, settings, or files.

Share charm - share photos, music, movies, or links with other apps or people. For example, when viewing a web page, use the share charm to send it. You do not have to open email, and copy and paste the link. Send a favorite recipe directly from the Recipe app, or photos from the Photo app.

Start charm - The Start charm returns you to the Start screen. If you are already on the Start screen, the Start charm returns to the previous page. You can also shut down Windows using the Windows 8 keyboard key.

Devices charm - use the Devices charm to print, play media on TVs and audio systems, use more than one monitor, and send content to nearby computers and other devices such as phones.

Settings charm – This charm helps to personalize your computer. For example, change the volume or brightness, choose your keyboard type, access the PC settings, and turn off the computer are just a few of the selections.

Tiles are icons of apps that appear on the Start page. Many of them show active screens within the tile. They can be moved and re-sized.

Apps are shown on a secondary screen that contains all the tiles and other apps that were either included with your computer, or downloaded from an app store or some other location. They can be grouped, or dragged onto the Start screen to become a Tile.

Organize Windows 8 Start Screen

We showed you how to remove Gadgets in older systems. And we let you know what the icons in Windows 8 are called. Now, let's look at Windows 8 and see what we can do with the apps that start accumulating.

Of course we can revert back to a Windows 7 screen, and sometimes that is handy, but lets jump into the latest windows format and see how to organize it to our liking.

Windows 8 allows us to move and adjust the size of the tiles on the desktop. So let's start by organizing by category. With a touch screen device, select the app you want to move by pressing down and holding on the tile and pulling down slightly. If you're using a mouse, just click and drag. When you drag the tile, it will appear translucent. You can group tiles such as Kindle, Nook, Overdrive, 3M, Adobe Reader and any other app that allows downloading and/or reading books into one group.

To relocate the group with a touch screen device, you can simply pinch the screen. If you have a keyboard and mouse set up, just hold down the Ctrl key and zoom out with your mouse wheel.

Then select your newly created group of tiles by pressing and pulling down slightly on them or by clicking with your mouse. Drag your group to the desired position. Once in location you click on the group or pull down slightly and you will get the option to name the group.

You can do this with the rest of your tiles until they are all organized the way you want them.

There are other things you can do with Tiles or Apps, which are a snap with a mouse. Right clicking on a tile or app opens up a pane with the following commands: Pin (or unpin) from Start; Pin (or unpin) to taskbar; Uninstall; Open New Window; Run As Administrator; Open file Location, and for the tiles Re size.

With a touch screen you can do the same thing by just holding down the tile for a second (some require that you slide it a little) and the same options appear on the bottom of the screen.

If you have a Windows 8 tablet, you probably use it a great deal for browsing the Internet. It's handy to have tiles for your favorite sites displayed front and center, so you don't have to always open your browser and pull up favorites. This also works for a Windows 8 computer with a mouse or track pad.

Just remember that you can customize the Start Screen of Windows 8, so you can pretty much get it to look just like you want it to.

PDF Security

PDF files are usually document files that cannot be changed from the format that you receive them in. This is a good thing if you want someone to read something that cannot be altered, like a book or an important document. These files are read in what is called a PDF reader. The most common one is Adobe, but there are others that are available. So do you get annoyed when a box pops up telling you that there is an update for Adobe reader? We all do. Get them and get annoyed at them. I do not recommend you downloading these updates that come unannounced on your computer. I do recommend that you periodically go to the Adobe site and click on and download any update. Why? Let's start with the PDF file itself. PDF is one of the most widely used file formats. But unfortunately, hackers have found ways to embed malware in PDF files. New threats are discovered on almost a daily basis. So patches and updates are continuing to be generated. But if it is not from the Adobe site, the notice that you received might even be sent by somebody who does not have our best interest at heart. So rule one is to check the Adobe site periodically and download any updates. Rule two is not to download the notices that pop up on your computer without being asked.

Application Security

With the tip above in mind you should also try and keep all your software up to date with the latest patches and upgrades. However, our computer holds dozens of application programs, so how do we keep up with it all?

First, concentrate on the programs that are most often targeted.- the ones that are most commonly used.

Your browsers, Office suites, etc. The more popular the program the more users that can be reached.

Second, activate any automatic update features that are available. Then your software will check its home site for

patches and upgrades on a routine basis.

Third, you can use a program like Secunia Personal Software Inspector (PSI). This free program comes from a trusted security site, and scans your software for known vulnerabilities. It will tell you which programs need updating and provide links to sites where you can download patches.

Finally, let me add one more tip. When installing a new application, or a new program DO NOT, I repeat DO NOT run the normal installation. Always use the Custom button, and read carefully each screen that comes up. Many applications now carry all sorts of additional programs. Not that they are bad in themselves, but do you need another search engine? Another toolbar? This is becoming very prevalent with downloads from even trusted sites. We don't have to clutter up our computers with stuff we do not want.

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

Computing ... Yesterday And Today

by Phil Sorrentino, Member, The Computer Club, Florida

http://scccomputerclub.org Philsorr.wordpress.com philsorr @yahoo.com

Yesterday, circa 1965, computing was mostly programming to solve simple problems, to do simple accounting like running a payroll, to match items from a list, and maybe even to print results on multi-colored, fan-fold, wide computer paper. (I bet some of you even remember that kind of computer output.) In fact in those days, you never even saw the computer because it was enshrined in a temperature and humidity controlled room or rooms with a flooring system that allowed many, many heavy cables to be run beneath the computers, so they could go the shortest distance between the massive computer cabinets.

Computing in the 70s, 80s, (and maybe part way into the 90s), was still running special software on computers and printing the results. During this time, thanks to integrated circuits, computers got a lot smaller, and some even moved from the cavernous computer room to the smaller computer lab, where it only took up the space of one desk or so. Anyone remember the Digital Equipment PDP-8? And, during this time, we did start to use the computer for many office tasks like word processing (Word and Word Perfect) and data analysis (Excel and 1-2-3). If you are relatively new to computing, you probably are not aware of this, but the first personal computer that showed up in 1975, the MITS Altair 8080, was available as a kit for $395, (soldering iron and tools not included). No keyboard or monitor, input was done by setting a bank of switches and output was just a bank of lights. This was the humble beginning of a major change in computing.

Soon after this, Apple released the Apple 2, which was a major improvement in the way data got into and out of the computer. It had a keyboard for input and the output was displayed on a TV monitor. During this period, the early 80s, there were many start-up computer companies. If you leafed through a computer magazine (like PC Magazine) in 1980 you may have seen almost 100 different manufacturers of incompatible computers advertised. Radio Shack was even a player with its TRS-80 computer system. (Does anyone have or remember the Atari or Osborne or Commodore computers?) Finally, in 1981, the IBM-PC arrived and from then on it has been the platform of choice for computing, (at least from these computers-in-use statistics).

The original IBM-PC was an 8-bit computer, although it did have a 16-bit bus. (Anyone remember the Intel 8088 microprocessor chip?). During this period, Apple also released some very successful computers such as the Apple 2e, and finally the Apple Mac. (The Apple Lisa didn't fare too well, even with its forward looking Graphical User Interface, which, as it turns out, is a forerunner of our modern Windows User Interface). How is that for digital computer nostalgia?

Today, things are a little different in what we wish to accomplish with, and in what we expect from, our computers. Today, we still expect to accomplish problem solving, but we also expect to communicate the results to, and collaborate with, others nearby, and halfway around the globe. Over the last few decades, our computers have gone in several directions and morphed into several "computing devices" such as desktops, laptops, tablets, and smartphones. Today our computing devices have become the focal point of our virtual digital existence and provide, for us, both computing and communications capabilities. These communications capabilities are now an integral part of our computing devices. Where would we be without smartphones, Wi-Fi, cell towers, and Starbucks?

So what is computing, today? Well, computing today is multi-faceted and quite ingrained in our daily lives. Much of it revolves around the home as well as the office. In the office we still use the computer to solve simple and complex problems like organizing a small business's finances, or tracking the latest hurricanes across the globe. The results, however, are typically provided as softcopy output on a flat panel, touch sensitive display, and only sometimes as hardcopy printouts. But, we also expect to communicate with other workers, and sometimes the public, using our computer. Office networks, Wi-Fi, the Internet and Social Networking Apps allow us to communicate with others across the

hall and across the globe. At home we communicate with others, mostly by email, but very often by texting, (especially if we are trying to keep in contact with grandchildren), or video conferencing, aka Skype or Face Time. Our home computer is the repository and focal point for all our digital information: documents, pictures, and videos. Documents that we create or collect are stored on the home computer for easy access, and long term storage. Pictures that we take with our digital cameras, smartphones, tablets, and scanners are all centrally housed on the home computer. At least, that is one way of keeping track of the large number of pictures we take using multiple devices. (When was the last time you moved your pictures from your smartphone to the computer? No excuses now.) Videos that we create or acquire are also housed on the home computer. Where else would you be able to store a bunch of 2 to 3 Gigabyte files? We communicate, entertain, and keep track of our home activities, all with the home computer. Not so long ago, the computer in the home was considered the "personal computer". But, today, the desktop or laptop in our home is really a "home computer" while our smartphone (or tablet) has taken on the role of "personal computer".

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

Get Help From Others

by Sandy Berger, CompuKiss
www.compukiss.com sandy@compukiss.com

Need help with your computer, tablet, or phone? There are actually several places that you can go to get help.

A great place to go is to online communities. These online groups can be very helpful in getting questions answered and learning from others. If you don't know where to look for them, just Google your questions and you will get links to several places that might give you an answer and that you might want to revisit later.

Friends and family are also great resources. If you have the same type of phone or tablet as others you know, start sharing the little tips and how-tos that you discover and they are sure to reciprocate by showing you what they know.

When you are looking for apps for your smartphone, tablet, or computer, you can also take advantage of the opinions of others. The Apple iTunes store, the Google Play store, and the Kindle app store all allow users to rate apps. This is extremely useful for finding new apps. And if you haven't yet played with apps, please start now. They provide a whole new world for you to experience.

Editor's Note: The author missed the great sources available to SHCC club members - our club monthly meeting, our club members, our two SIGS, the WYSIWYG, and our Yahoo newsgroup.

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

If your dues are paid the month they are due, as shown on the invoice the club sends, you automatically get an extra month of membership. This policy has been in effect for many years but newer members may not be aware of this "free month" policy.

SHCC Post Office Box

After 9-11 some of the rules have been changed concerning post office boxes. These changes are intended to make it more difficult for persons using post office boxes to remain anonymous, at least to the post office. If you send anything to the club's PO box don't put a person's name on it. It's OK to use titles such as President, Treasurer, and such. If you use a person's name, your mail will sit at the post office until that person can get to the post office with ID and claim the mail. This just slows down your mail and inconveniences the addressee.

Member Classified Ads

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

SHCC Emergency Cancellation

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

WYSIWYG WEB WATCH (www)

by Paul Baecker webwatch@sterlingheightscomputerclub.org

This column attempts to locate sites containing valuable, amusing and free content, with no overbearing pressure to purchase anything. Send your favorite entertaining, helpful or just plain useless sites (a description is optional) to the e-address noted above, for inclusion in a future WYSIWYG.

Recent versions of Windows contain their "Snipping Tool" with basic features to capture a screen shot, or *snip*, of any object on your screen, and then annotate, save, or share the image.
http://windows.microsoft.com/en-us/windows/use-snipping-tool-capture-screen-shots#1TC=windows-7

25 maps that explain the English language.
http://www.vox.com/2015/3/3/8053521/25-maps-that-explain-english

The Domain Name Service automatically converts the names we type in our web browser address bar to the IP addresses of web servers hosting those sites. Here is a description of the process in a comics format.
https://howdns.works

Quick Start Guides for various Microsoft 2013 desktop products, including Office.
https://support.office.com/en-us/article/Office-2013-Quick-Start-Guides-4a8aa04a-f7f3-4a4d-823c-3dbc4b8672a1?CorrelationId=e714bd83-1714-4552-b606-f9d16408d03c&ui=en-US&rs=en-US&ad=US

Videos of American and European exotic automobile rallies.
https://www.youtube.com/user/Shmee150/

Use a sandbox tool to avoid malware infections while testing a software product on your PC. Guide to the free Sandboxie tool here.
http://www.techsupportalert.com/content/introduction-and-quick-guide-sandboxie.htm

A beginner's guide to using Skype on an Android device.
http://www.makeuseof.com/tag/use-skype-android-beginners/

How do you secure the hard drive when you take your computer to get it serviced? Consider more than just 'trust'.
https://askleo.com/how_do_i_secure_a_hard_drive_before_sending_it_in_for_repair/

Four things that you can do to reduce the spam quantity in your e-mail.
http://www.makeuseof.com/tag/still-getting-spam-4-email-mistakes-avoid-today/

If you consider saving files to the cloud as being secure, here is a comparison of cloud storage services.
http://www.ilovefreesoftware.com/03/webware/comparison-best-free-cloud-storage-services.html

Sharing your Wi-Fi internet access with a neighbor might seem friendly, but be aware of the dangers to your own computers.
https://askleo.com/if_i_let_my_neighbor_share_my_wifi_can_they_see_my_network_traffic/

Disposing an old laptop computer? Here's what to recycle and what to keep (unless you're donating it to *me*!).
http://www.makeuseof.com/tag/disposing-of-an-old-laptop-what-to-recycle-what-to-keep/

If you need to install or reinstall Windows 10, you can use the tools on this page to create your own installation media using either a USB flash drive or a DVD. Note: If you want to upgrade to Windows 10 for free, select "Upgrade this PC now" in the tool.
http://www.microsoft.com/en-us/software-download/windows10

A worthwhile 40-minute overview tour of Windows 10.
https://www.youtube.com/watch?v=FZqKyhfD7-E&feature=iv&src_vid=kGw9k-ImkG4&annotation_id=annotation_4060882225

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

World Wide Web Column on the Club Web Site

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