The Rochester Computer Society, Inc.
Founded 1982

MONITOR

Vol. 32, No. 2 February 2015

Next Meeting
Tuesday, February 10

The Briarwood at St. John's Meadows, Brighton

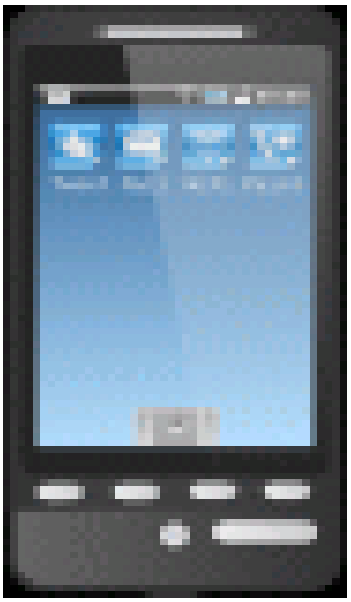
Contents

Federal Agencies Post Security Warnings and Recommendations for Mobile Phones

by Ira Wilsker

Now that the spring semester is starting, it is quite obvious that almost all of my college students have and are using smart phones and other digital communications devices for much more than the traditional calling function. One of my daughters is teaching high school, and almost all of her students have a smart phone. Going to a nice restaurant for dinner shows that almost all of the patrons check their smart phones to some degree. We are seeing frequent TV commercials about using the "Near Field Communications" (NFC) feature now built into most newer smart phones as a method of secure retail payment instead of swiping a plastic credit card or writing a check. With the near universal use of smart phones and related devices in our daily lives, it is inevitable that crooks and other dishonest people will find a way to illicitly capitalize on the popularity of these devices. The security risks prevalent on the use of these devices has caught the attention of several federal agencies,

including the Federal Communications Commission (FCC), Department of Homeland Security (DHS), and other federal agencies, all of whom have posted "security checkers" and other tips on properly securing our smart devices.



The Federal Communications Commission (FCC) has posted online an operating system specific "Smartphone Security Checker" at fcc.gov/smartphone-security. This security checker offers explicit infor-mation and recommendations for devices running Android, Apple iOS, BlackBerry, and Windows Phone. Selecting one of the operating systems, and then clicking on the "Generate Your Checker" icon will display appropriate instructions for your device. Since I have both an Android phone and an Android tablet, and Android has over 75% of the smart device market, I selected the Android option. The recommen-dations displayed for the other operating systems was very similar to that displayed for Android.

The security checker displayed for Android devices was headed, "Ten Steps to Smartphone Security for Android," and explains how these security guidelines could reduce the exposure and risk of mobile cybersecurity threats if they are imple-mented. The 10 steps recommended by the FCC for Android devices (and very similar to those for the other smart device operating systems), are:

1. Set PINs and passwords. To prevent unauthorized access to your phone, set a password or Personal Identification Number (PIN) on your phone's home screen as a first line of defense in case your phone is lost or stolen. Configure your phone to automatically lock after five minutes or less when your phone is idle, as well as use the SIM password capability.

2. Do not modify your smartphone's security settings. Tampering with your phone's factory settings, jailbreaking, or rooting your phone undermines the built-in security features offered by your wireless service and smartphone.

3. Backup and secure your data. You should backup all of the data stored on your phone – such as your contacts, documents, and photos. These files can be stored on your computer, on a removable storage card, or in the cloud.

4. Only install apps from trusted sources. Many apps from untrusted sources contain malware that once installed can steal information, install viruses, and cause harm to your phone's contents.

5. Understand app permissions before accepting them. You should be cautious about granting applications access to personal information on your phone or otherwise letting the application have access to perform functions on your phone. Make sure to also check the privacy settings for each app before installing.

6. Install security apps that enable remote location and wiping.

An important security feature widely available ... is the ability to remotely locate and erase all of the data stored on your phone, even if the phone's GPS is off. In the case that you misplace your phone, some applications can activate a loud alarm, even if your phone is on silent.

7. Accept updates and patches to your smartphone's software.

8. Be smart on open Wi-Fi networks. When you access a Wi-Fi network that is open to the public, your phone can be an easy target of cybercriminals. You should limit your use of public hotspots and instead use protected Wi-Fi from a network operator you trust or mobile wireless connection to reduce your risk of exposure, especially when accessing personal or

sensitive information.

9. Wipe data on your old phone before you donate, resell, or recycle it. Your smartphone contains personal data you want to keep private when you dispose your old phone.

10. Report a stolen smartphone. The major wireless service providers, in coordination with the FCC, have established a stolen phone database. If your phone is stolen, you should report the theft to your local law enforcement authorities and then register the stolen phone with your wireless provider. This will provide notice to all the major wireless service providers that the phone has been stolen and will allow for remote "bricking" of the phone so that it cannot be activated on any wireless network without your permission.

As more of us are using the Near Field Communications (NFC) feature available on most of our smart phones as a secure method of payment at retail stores, restaurants, gas stations, and at other sellers of goods and services, we must also be cognizant of the security threats and safety precautions necessary when using these "mobile wallets." Some of the widely used mobile wallets include Google Wallet, Apple's Apple Pay, eBay's PayPal, CurrentC (a joint effort of Sears, Target, and WalMart, CVS, and others), GoSoftCard (joint effort of American Express, Chase, and Wells Fargo), and several others. Supposedly these mobile payment services provide greater security and benefits than using a plastic credit or debit card, and award appropriate "points" on the credit card backing several of the services. The method of using the NFC features on many of our phones is quick and simple; the appropriate app (probably connected to an existing credit or debit card account) is opened, and the phone is held near the point of sale (POS) terminal to complete the transaction. As an added level of security, most of the payment apps also require the user to enter a PIN, fingerprint, or other method of verification on the phone prior to completing the transaction. The seller only has verification that a payment to them has been processed, but does not have access to credit card numbers and other personal information. Since the seller does not have this information from the payment process, cyber hacks such as what happened at Target, Home Depot, and other retailers would not capture our private, financial, and personal information.

Being aware of the rapidly increasing use of these alternative digital payment systems, the FCC published "Mobile Wallet Services Protection" online at fcc.gov/guides/mobile-wallet-services-protec-tion. While the actual point of sale transactions are reasonably secure when these digital wallets are used, the primary risk is the loss or theft of a smartphone containing the electronic wallet apps. The use of a PIN, fingerprint, or other verification at the time of the transaction provides good security, they are not perfect, and may be vulnerable to a miscreant in possession of a lost or stolen smart phone. Since many consumers are inherently complacent, and use the same or other easy to guess PIN numbers to access multiple resources (such as an ATM), PIN numbers are the most vulnerable of the primary verification methods.

In the "How to Safeguard Your Mobile Wallet Smartphone" guidelines are several "common sense" tips to protect our mobile digital wallets. We need to be aware of our surroundings, and protect our PIN and other verification modes from prying eyes, as well as very short range electronic interception (sometimes an innocuous looking device adjacent to the POS terminal), often within about four inches or 10 centimeters. If using an electronic wallet for paying for online purchases or other remote financial transactions, do not use an insecure, open, Wi-Fi network, as the information can be readily intercepted at distances of up to several hundred feet. Smartphones are popular items to steal, and can also be innocently lost. The FCC says, "Never leave your smartphone unattended in a public place. Don't leave it visible in an unattended car; lock it up in the glove compartment or trunk." If you have not already done so, write down the identifiers of your device, and store them in a secure but accessible location; these identifiers can often be found on the device in the battery

compartment, or under Settings - About Phone, as well as on the box the phone came in. This information may be needed in a police report, which should be filed if the phone is stolen. All phones have a unique serial number called an International Mobile Equipment Identifier (IMEI), sometimes also called a Mobile Equipment Identifier (MEID). This unique IMEI or MEID can also be displayed on most phones by dialing *#06# (asterisk - pound - zero-six-pound), which should be recorded, and used to definitively identify a phone. Provide this information to your carrier when reporting the loss of the device to them.

In terms of financial liability for the illicit use of a digital wallet on a lost or stolen phone, the terms of service for that app should be reviewed, but in general the limitations on financial loss are similar to those for the use of the plastic credit or debit card behind the app. As with any other debit or credit instrument, check the online and monthly statements for questionable or unauthorized charges, and follow the issuer's instructions for resolving the discrepancies.

The FCC also recommends that smart device users install and maintain security software and appropriate apps that can be used to locate a missing device (even if the GPS is turned off); remotely lock the device (even if only "temporarily" lost); wipe sensitive information off of the device after sending a remote command; and even sound a loud alarm or other sound (some apps call it a "scream"), which will be sounded even if the device is on "silent" or "vibrate," which can be used to locate a device, especially if "lost" at home, work, or in the car. Users may also want to display limited contact information on the "lock screen," which may allow an honest person to return a found phone. The FCC also warns about the personal information stored by social networking sites and internal apps that may allow unauthorized access to personal information. Also, in the event of a theft or loss, go online using another device and change all of your critical and wallet passwords and security questions.

Our smart phones and other intelligent devices have (arguably) done much to enhance our daily lives, as we make more use of them and find new and innovative ways to benefit from them. As important as these devices have become to us personally, we must also do what we can to secure them and their data, and protect the devices from loss.

Websites:

http://www.fcc.gov/smartphone-security
http://www.fcc.gov/sites/default/files/12.14%20Mobile%20Security%20Tips%20%28Android%20-%20Links%29_0.pdf
http://www.fcc.gov/blog/fcc-and-public-private-partners-launch-smartphone-security-checker-help-consumers-protect-mobil
http://www.fcc.gov/sites/default/files/smartphone_master_document.pdf
http://www.dhs.gov/stopthinkconnect
http://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device
http://www.fcc.gov/guides/mobile-wallet-services-protection
http://transition.fcc.gov/cgb/consumerfacts/Mobile-Wallet-Services-Protection.pdf
http://www.fcc.gov/guides/stolen-and-lost-wireless-devices
https://en.wikipedia.org/wiki/Near_field_communication

Courtesy of Mr. Wilsker.

Watch Out for Gray Market Goods

by Bob Rankin
askbobrankin.com

Between Walmart's everyday low prices and the sketchy fellow in Walmart's parking lot who's selling brand-new, boxed iPads for $50 lies a vast gray area appropriately called the "gray market." Here you'll find prices lower than those of any mainstream merchant but not quite low enough to scream "stolen" or "counterfeit." How do gray markets work, and are they legal?

What is the Gray Market?

Many gray market sellers represent themselves as "direct importers" or "independent dealers," terms that consumers tend to interpret as more economical than "regular" importers or dealers. Gray market sellers often tout themselves as small, "family owned" businesses who are more honest and trustworthy than corporate America. Many are even perfectly up-front about how they beat the big boys' prices.

Gray marketers buy goods outside of manufacturers" authorized distribution channels, evading the contractual obligations of authorized resellers that manufacturers impose in order to maintain the quality of their brands. Gray marketers don't provide warranty service or tech support. They don't participate in the manufacturer's product training or co-op advertising programs.

They may not provide user manuals in English or power supplies compatible with American A/C outlets, because they "directly import" goods from overseas. Some don't even answer their phones. The comments I found posted on one gray marketer's profile are typical:

- *I ordered a Black Canon M and received an open box SILVER Canon M. Both the flash and extra lens were missing. Major fail. I certainly won't order from this company again.*
- *They took my money and sent the wrong item. They did not want to take any blame and shipped a totally different item and did not contact me to see if it was ok. STAY AWAY FROM THIS SELLER THEY WILL NOT GIVE YOU WHAT YOU ORDER.*
- *Missing parts and no response from customer service. The camera battery charger cable that it came with was the international plug, but missing USA cable. Emailed them, but no one replied.*

Is It Legal?

It's not a crime to buy gray market goods, but it is unlawful to sell them. Trademark law, specifically the Lanham Act, gives manu-facturers the right to control how their trademarked goods are sold and supported. OEMs can require resellers to spend money on training, advertising, providing tech support and warranty services, etc., as conditions of being permitted to resell the goods. The costs of meeting these conditions are added to the authorized resellers' prices. Gray marketers avoid all of that expense and pass (some of) the savings on to buyers.

If you buy a product through a gray marketer, don't expect the manufacturer to provide any free support or warranty. Some OEMs will repair gray market units for a (usually steep) fee. Most will not sell you parts for a gray market unit. If the product breaks down, you're on your own to find parts and someone who is able and willing to fix it. Saving money on the initial purchase can be very expensive when you need service.

How can you tell if an online seller is offering gray market goods? An unusually low price would be the first tip-off. Some brands, notably Apple, almost never allow their products to be sold at a significant discount. If you see an iPad or MacBook at half price, put down the

mouse and back away slowly. You don't want to take a chance on buying on the black market. I'm not a legal expert, but I can imagine a prosecutor saying "You should have known better" while charging you with possession of stolen or counterfeit goods.

Other tipoffs may come from reviews of the seller. Check for complaints about "open box" shipments, missing plugs or cables, power adapters designed for European or Asian countries, manuals printed only in a foreign language, or missing warranty cards.

Is It Ever Worth It?

That said, there are times when it makes sense to buy gray market goods. If the product is extremely reliable you may not need service during the time you expect to use it. Hard drives, for instance, generally have MTBFs (mean time between failures) of 50,000 hours or more; that's 5 years and 8.5 months of constant disk activity, on average. And they don't plug into a wall socket, so you don't have to worry about plug compatibilty. If you're handy with a soldering iron or familiar with circuit boards, you may be able to make any necessary repairs yourself, if you can find parts. If the purchase price is low enough and you"re not going to keep any critical data on a device, it may be worthwhile to buy it and just throw it away when it breaks. You may also have to find and purchase missing parts or accessories, or replace power adapters that are not compatible.

The Bottom Line: It's the Bottom Line of Course

Gray market goods do save you money when you buy them. What they cost you is convenience when you need help and the peace-of-mind that comes with knowing you're covered if something breaks. You also have to swallow hard, trust that the seller won't take your money and run, and accept the fact that they are violating the law.

In my opinion, it's a trade-off that should be attempted only if you're a risk-taking power user, familiar with electronic components, handy with a soldering iron, and familiar with sources for any parts that may be needed. You should also have a credit card with excellent fraud protection. *Courtesy of Bob Rankin.*

Linux Magazines

by Cal Esneault
Cajun Clickers Computer Club, LA

Since Linux is not as commonly used as some other computer operating systems, users frequently resort to online sources for instructional information. Although easy to find, typical research often ends with information having a question and answer format focusing on isolated issues. A magazine format can give a broader view without being long or technically complicated. Two suggestions for free, online magazines for users are *PCLinuxOS Magazine* and *Full Circle Magazine*.

PCLinuxOS is a PC operating system with a KDE 4 desktop environment that was started by Bill Reynolds ("Texstar") in Houston, TX. It has an open-source "community" operation that publishes its own magazine. There is a lot of emphasis for new users transitioning from other operating systems. Many technical articles stick to a moderate length, and there is a lot of "fun" content (such as food recipes, screen shots of customized desktops, reader feedback, etc.).

Below are a few of the article topics covered in the last three issues of *PCLinuxOS Magazine*:

Xfce User Tips and Tweaks (Parts 1,2, & 3)

Password Security Revisited

OpenVPN: Other VPN Services

LibreOffice Tips & Tricks (Parts 1,2, & 3)
Inkscape: Holiday Tree; Torn Paper Effect
Undo Gmail's Latest "Enhancements"
Backup Your Gmail Account With getmail
GIMP Tutorial: Masks Explained
Game Zone: Sacred Citadel
Linux vs. Windows
Testimonials from veteran PCLinuxOS users
Gramps genealogy program
Screenshot Showcase

Full Circle Magazine covers Ubuntu and its derivatives (Xubuntu, Lubuntu, Edubuntu, etc.), but it is not associated with Canonical Ltd, the commercial sponsors of Ubuntu. It has many recurring feature topics (news, ask the new guy, software reviews, command line skills, etc.) and usually has more than 50 pages of content. For the most part, it relies on volunteer writers, There is also an associated podcast available. Note: the title Full Circle is in reference to the Ubuntu logo.

This magazine also carries well detailed multi-part articles about a few of the more popular software titles. Examples include LibreOffice, Inkscape, Blender, Python, and GIMP. There are sometimes special editions of concentrated compilations of these articles.

Examples of special issues are three special issues for LibreOffice, two special issues for Inkscape, and 6 special issues for Python (see the September 2013 main magazine issue for details). Since most of the software with multi-article coverage is cross-platform and can run on most operating systems (Linux, Mac OS, Windows OS), these articles should be of interest to almost any computer user.

Both magazines are published monthly. *PCLinuxOS Magazine* started in September of 2006 and is now at issue 80. *Full Circle Magazine* started in May of 2007 and is now at issue 77. Both can keep you up to date on news, software, and hardware related to Linux. In addition, you can get any of the past issues in PDF format from their archives without cost. These archives provide a huge resource of detailed information written in a style friendly to the average user.

These magazines are excellent examples of the way the open-source community works to share the knowledge about free computer software. Even if you do not currently use a Linux OS, browsing these magazines will give you a quick view of what open source software is all about.

From the November 2013 issue, *Cajun Clickers Computer News. Courtesy of APCUG.*

Print Folder Index

Q. Is there is any way to print the contents of a folder so I can obtain a list of the filenames, sizes and dates modified?

A. Yes, you can print a list of the files and subfolders contained in any Windows folder, and while this can be accomplished within Windows itself, using a third-party program makes the task a lot easier. One such program is PrintFolder at http://no-nonsense-software .com/free-

ware. PrintFolder can print files, subfolders or both, and it includes several other customizable options.

If you're a purist and prefer to print your directory of files and folders from within Windows itself, using My Computer or Windows Explorer, display the list of the folders or files you want to print, then press ALT + PRINT SCREEN (PrtScr) to copy an image of the active window to the Windows Clipboard.

Next, click Start > Programs > Accessories > Paint. On the Edit menu, click Paste (or right-click and select Paste). Click Yes to display the captured image then click File > Print.

Q. Is there a way that the photos in the body of email I receive can be made smaller in size? Thanks in advance for help, Mr. M.

A. The problem with super-large photos usually lies with the senders of those photos. Pictures to be sent by email should be low-resolution photos. Most digital cameras have a setting for that, but instead, many people send higher resolution (called "high-rez" photos) that are great for making prints, but often result in huge files. It then becomes the recipient's responsibility to correct the problem.

You can resize the photos yourself, though you might want to politely suggest that the sender actually open the manual that came with the camera and learn how to take low-resolution photos, or determine what relevant settings might exist for that specific purpose.

As the recipient of a super-large photo, ShrinkPictures.com is a Web-based service that enables you to reduce the size of digital photos. No software is required and the service is free. As an alternative, Resize2mail.com is also free. Senders of photos would be well advised to use either of these sites before sending photos.

My suggestion for anybody who wants to share photos is to simply use one of the online photo albums such as Snapfish.com, Shutterfly.com, PhotoBucket.com, or Picasa.google.com, then send the URL of their uploaded photos to others who can view the pictures online.

Q. I have Windows 7. Can I download the Windows 8.1 upgrade for free?

A. Unfortunately, no. The Windows 8.1 upgrade is only free for those who already have Windows 8 installed. It functions in the way a Service Pack would for previous of versions of Windows. If you purchase a download of Windows 8 now, it will most likely be Version 8.1. If you do, however, purchase Windows 8, the upgrades to Windows 8.1 will be free. The best way to obtain Windows 8, however, remains via the purchase of a new computer with the operating system installed.

Q. I'm not planning to use Internet Explorer anymore because of all the security problems associated with it, but is it safe to use it long enough to download the Google Chrome browser?

A. The fact that IE remains vulnerable is of no additional consequence in this instance, if you have been using it all along. And realistically, how else are you going to obtain another browser other than by using Internet Explorer, if that's the only other browser you have installed? You should be fine using your currently installed Internet Explorer to download Chrome.

Mr. Modem's DME (Don't Miss 'Em) Sites of the Month

MonkeySee

Free access to a large collection of professionally produced and user-generated how-to videos. Categories of videos range from Auto & Mechanical to Sports & Leisure. In the Beauty & Fashion section, I learned how to style my hair for the prom. Just my luck: Almost 50 years and 250,000 follicles too late.

www.monkeysee.com

Ruined Photos

A collection of photos that took an unfortunate turn just as the shutter was released. Sometimes it's the result of the positioning of the subject(s), sometimes it's somebody or something that wandered into frame at the last second, or a less-than-civil gesture on the part of some inebriated guest. While some of the photos are hilarious, sensitive or easily-offended individuals would be well advised to avoid this site as some of the photos are a bit coarse, racy and thus potentially offensive.

http://ruinedphotos.paulherron.com

Secrets Explained

Have you ever wondered how famous magicians and illusionists like David Copperfield, Criss Angel, and David Blaine accomplish their magic tricks? If so, this site is for you! At the top of the page you will find categories for each magician. Mouse over the magician whose tricks you want to explore, then select an illusion or trick. You can also navigate by the type of tricks or techniques like Basic Techniques, Card Tricks, Coin Tricks, and Rope Tricks.

www.secrets-explained.com

Honey, A Robot Shrunk my Job!

by Greg Skalka

Under the Computer Hood User Group, CA

I recently took a day trip alone with my 23-year-old daughter, which gave me the opportunity to find out more about her thoughts on the future. For the last five years she has lived about two hours away, so these opportunities for me to gain insight into her life and attitudes are rare. I was a little surprised to find one of her concerns was that robots would eventually occupy all jobs. She said she and her boyfriend had discussed this and wondered if one day everyone would be unemployed except for those that made robots (and she with a business marketing degree, of course).

I could write off some of her apprehension to the nine months so far spent looking for employment in her field of study, but this concern over technology eliminating jobs is a real issue. Modernization and mechanization have changed the career landscape in the past, but today's changes due to computer and communications technology, combined with increased globalization, may be coming faster than our society can cope with.

Since ancient times, mankind has sought to improve living conditions and decrease the labor required for a fulfilling existence. With the majority of early humans involved in agriculture, innovations were sought to reduce the labor in growing crops. The use of hand tools and plows and of animals in place of human labor allowed fewer people to grow more food. This allowed some who would otherwise be farmers the opportunity to pursue other professions and develop other innovations.

My daughter is only two generations away from an agrarian life. My father was raised on a farm with no electricity or indoor plumbing. As a young boy, he mostly ate only what his parents obtained from their land and their animals. Over the last 70 years, with tractors and implements, better agricultural science and improved transportation, farm production has improved such that a fraction of the farmers can now provide many times the previous agricultural output. Today GPS-guided tractors optimize the land for planting and farmers can use drones to monitor their crops and livestock. These changes have greatly reduced the labor required to feed the world, providing inexpensive food to a global market. With agricultural

labor requirements reduced, the rural towns and cities of the Midwest shrank as young people were forced to find work elsewhere.

The Industrial Revolution began 200 years ago, transforming manufacturing and industrial activities. Through most of the last century, the improvements brought by technology reduced the manual labor required to produce products. Though fewer workers were required to produce the same products, new industries were created that provided new jobs. As some classes of occupations became obsolete (like the ice delivery men that stocked the residential ice boxes), others came into being (like refrigerator repairmen). Though the changes to society were great, they came over a number of generations, allowing society to adapt.

The electronics and computer revolutions that started at the end of the last century have continued the increases to our productivity, but at a much greater pace. In addition to saving manual labor, computers reduce the mental efforts required in design and production, displacing workers with greater skills. New computer, telecommunications and consumer electronics industries were created as a result of this technology, creating new occupations as others were made obsolete. These profound changes to society now occur in a much shorter time, in a generation or two, or less.

When I was growing up, I could not consider a career as a Blockbuster Video sales clerk, as consumer videocassettes had not yet been invented. My daughter watched videos we rented for her as a child; now as a young adult, the video rental stores are gone, and she watches DVDs from the Redbox machine in front of the grocery store or views streaming videos on her iPad. The video rental clerk is an occupation that came and went in my lifetime; Netflix, Hulu, and that big red robot dispensing DVDs caused all those jobs to go away.

The video store clerk is the classic example of workers displaced by modern technology (and not replaced elsewhere in a successor industry in the same numbers), but there are plenty of others. Bank employment has been reduced, thanks to automated teller machines (ATMs), online banking, and even Internet banks. I don't know if there were ever 400,000 bank tellers employed in the U.S., but today there are that many ATMs here. Now with the ability to deposit a check by taking a picture of it with your smart phone, the need for physical banks, and their branch employees, is reduced further.

Postal and parcel deliveries have been greatly improved by computerization and automation. FedEx, UPS, and the other parcel delivery companies have used technology to improve service, open new markets and keep costs down while getting more out of fewer employees. They have taken a lot of business away from the U.S. Postal Service, which has had to automate extensively to compete. I love the "postal robot," the automated mailing kiosk in my local post office. It is available to me at all hours of the day to weigh and mail my letters and packages and sell me postage. It does not require overtime pay or a pension, so I'm sure it reduces the USPS's labor costs.

The state Department of Motor Vehicles is another place where computers should have cut the number of employees required (but considering it is a government activity that might not be the case). Since most simple DMV activities like car registration renewals and address changes can be performed online, most people can avoid for years the unpleasant prospect of visiting the a DMV office in person. Even when you do, you can make an appointment online.

San Diego Gas and Electric used to employ legions of meter readers; now with the new smart meters they have installed over the last few years, all your energy usage is transmitted back to them electronically. Most grocery and general merchandise stores have installed at least a few self-checkout registers, reducing the number of employees needed. A Cupertino, CA hotel is introducing a robotic butler to make deliveries to guests; it motors around like R2-D2.

Even NASA has installed a Robonaut on the International Space Station to help humans work and explore in space.

These days it is hard to think of a job that does not require the use of computers and related technologies. Computers and microcontrollers are being built into everything; these smart, networked devices improve our lives and save us labor. They also may be eliminating a lot of lower-paid jobs. If a robotic vacuum can clean your floors, you may not need to hire a maid. Some restaurants are introducing tablet-like devices customers can use to order food and pay their bills, reducing the wait staff required.

I think the next big technology innovation will be the autonomous vehicle. The military already has unmanned aerial vehicles for surveillance and munitions delivery; some are remotely piloted, but others are truly autonomous. Once the private sector can legally use drones for business, mass production will make them less expensive and more capable, opening up more possibilities for their use. Small surveillance UAVs may one day replace many police helicopter, patrol car and foot patrols. If Amazon has its way, all your packages will be delivered not by people but by quadcopters.

The self-driving cars being developed by Google and others will really provide benefits to mankind but will also cost jobs. A fully autonomous car would be a great help to those too disabled (or too impaired) to drive, and could have the potential to greatly reduce traffic accidents. Though the technology may already be here, once again the legal and social systems will need time to catch up. Meanwhile, we are getting bits and pieces of the self-driving car now, in the self-parking car and the car that automatically brakes to avoid a collision. Once the fully self-driving car is legal, look for taxi, bus, and truck drivers to be in the unemployment lines.

Then the self-driving trucks will transport the raw materials to the robotic factories, so that more robots and self-driving vehicles can be manufactured.

From the September 2014 issue of Drive Light, newsletter of the Under the Computer Hood User Group, CA. Courtesy of APCUG.

Uninterruptible Power Supplies

by Dick Maybach
Brookdale Computer Users' Group, NJ

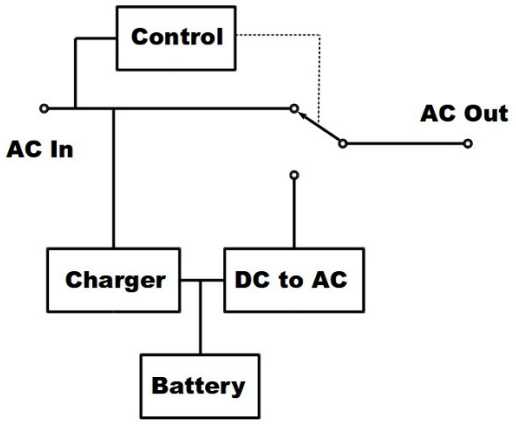
An Uninterruptible Power Supply (UPS) is a box that plugs into a power outlet on a wall and into which you plug in your computer and its key peripherals. You connect it the same way you connect a power strip. Inside the box is circuitry that monitors the ac voltage, a lead-acid storage battery, a charger, a power supply that converts the battery voltage to 60-Hz ac line power, and a switch that selects whether your computer is powered from the wall or from the battery. Most units also include a surge suppressor. Normally, your computer and its peripherals are powered from the wall and the UPS battery is being charged, but if the ac voltage becomes too high or too low, the battery powers your devices.

Power companies in the U.S. provide reliable service, but sometimes this is difficult. For example, they use the earth as part of their circuit, partly for safety reasons (to avoid high voltages building up on their wires). Service is difficult to maintain if the resistance of the earth is high as is the case in the Freehold, New Jersey area, where I once was responsible for a lab. We routinely ran tests lasting 24 hours or more, jointly with other companies from England, France, and Japan. Our schedules were tight, and if we experienced a power hit, a test was ruined. As a result, we had UPS cabinets the size of home freezers powering the entire lab. Partly as a result of this experience, I always used a UPS with my work computer. More than once I saw the lights blink, followed by streams of profanity from nearby offices where

computers had crashed because they weren't UPS equipped. Although there may be no economic impact resulting from a power glitch while working on a home computer, it is most frustrating to have an editing or photo-retouching session ruined. Modern UPS units are cheap and life is short, which often makes investing in one well worth its cost.

A surge protector has a device that is connected across the power line. If the voltage rises above a certain value, the resistance of the device becomes low. The hope is that the device will survive long enough to keep the voltage low until the surge is over. Most such devices will protect against one surge, but in doing so they burn out, which is why many surge protectors have an indicator that is illuminated if the device is good. Of course, since most of us locate our surge suppressors on the floor with the dust bunnies, we can't see their indicators.

By the way, neither surge protectors nor UPS units provide any defense at all against a direct lightning strike, which will vaporize the wiring in your house as well as equipment connected to it. The voltages are high enough for lightning to arc hundreds of feet from a cloud to the ground, and the currents can be a million Amperes or more. Fortunately, direct strikes are rare. However, when there is a lightning strike to the power grid, it can cause a momentary rise in the voltage, which is what a surge protector tries to prevent.



Most consumer UPS devices have the architecture shown in the block diagram.

In normal operation, the AC-Out socket is connected to the AC-In cord that is inserted in a wall outlet. At the same time, the input power is applied to a battery charger that keeps a lead-acid battery (which uses the same chemistry that starts your car) fully charged. Finally, control circuitry monitors the AC-In voltage, and if it departs from what is acceptable, a relay switches AC-Out to a DC to AC converter that generates a 125 volt, 60 Hz waveform from the DC voltage on the battery. This does mean that the AC-Out voltage is zero during the time it takes for the relay to complete its operation, but this time is short compared to the 1/60 second period of our power system, and it doesn't affect a computer's operation. Although not shown in the block diagram, most UPS devices have additional outputs that are connected to the AC-In port through a surge protector.

Some iMacs are incompatible with some popular UPS units. They work fine when the ac power is good, but the UPS will refuse to switch to battery when it fails. If you have an iMac, do your homework.

Try to buy your UPS from a supplier that offers a “No questions asked” return policy on UPS purchases; not all do (in particular, Amazon). As soon as you have everything connected and the battery is fully charged, pull the ac power plug to see if the unit switches to battery power. If it doesn’t you should trade it for a compatible one.

A UPS is designed to provide power when that from your power company fails. In particular, it assumes that commercial power is available when it's first turned on, and it may not start if this isn't true. This means you may not be able to use a UPS to provide power on a camping trip. You also may not be able to turn it on after the power fails.

Most UPS manufacturers specify the maximum output of their units in both Watts and Volt-Amperes, with the latter being larger. You should buy one with a maximum Wattage equal to or larger than the rating of your computer power supply. (We're discussing here only the total power supplied by the battery backup connectors; we can ignore the power supplied

by the surge protected connectors.) I'm assuming that you purchased your computer system, and that the manufacturer properly sized its power supply. Make appropriate adjustments if you know you have a larger than necessary supply, which is usually the case if you built your own system. The average power consumed by your computer will be significantly less than its maximum power supply rating. We have to be concerned about the maximum, because the UPS will shut down if you try to draw more than its rated power from its battery backup connectors.

To estimate how long you can run on battery power, you have to know the average power consumption of your computer. My desktop uses about 100 Watts, which is probably a good starting point, although I would double this for a game machine with a high-power display driver. If you're still using a CRT monitor, you should probably add 25 to 50 Watts for that. Some manufacturers, including APC, have graphs on their Websites that show run time vs. load, although these are valid only for new batteries. Lacking this, estimate five minutes of battery run time at maximum load. For example, my UPS is rated at 600 Watts; at 100 Watts it should last six times as long as it would if supplying maximum load, or 30 minutes. In fact, APC's chart shows 60 minutes at 100 Watts, so the rough estimate is comfortably conservative and allows for battery aging.

Decide what you want to keep running when the power fails. Your goal is to keep your computer running long enough so that you can save your work and power down normally. You may be able to work for a little while, but once the battery is exhausted, you're done. At minimum you need to back up your system unit and display. If you are visually impaired, you should also include your powered speakers. Everything else should have just surge protection; this includes your printer, scanner, and network equipment. It is especially important that you not try to back up a laser printer, as they draw so much current that your UPS may not turn on, even when your house power is normal.

Some UPS units have a master outlet; if the current supplied by it falls below a threshold, it will shut off the power to all the outputs labeled “switched” (or something equivalent.) If your UPS is so equipped, I recommend you connect your equipment as follows: the computer system unit to the master outlet, the display to switched backup, the speakers and scanner to switched surge protected, and the printer to unswitched surge protected. The last is because many printers should be powered down only with their own control switches. After everything is connected, be sure to test the operation to be sure that the desired devices remain powered when the power fails and (if your UPS has a master feature) that the desired devices turn off when the computer does.

Many UPS units have associated software that allows you to configure them and monitor their operation. It may also include a provision to shut down your computer if the battery becomes depleted during a power outage. However, UPS manufacturers are Microsoft-centric; their software may be Windows only, and if it does have Mac or Linux software, it probably has fewer features than the Windows version. Some higher-end units include front panels that provide much of the monitoring that the software does, which makes them less reliant on your operating system.

From the October 2014 issue of BUG Bytes*, newsletter of the Brookdale Computer Users” Group, NJ. Courtesy of PCUG.*

The Tip Corner

by Bill Sheff
Lehigh Valley Computer Group, PA

Deleting .EXE files

There is no problem with deleting any .exe files that you have in your download folder. Most of these files are setup files for programs. With unlimited storage, keeping them is not that big a problem, in case you ever want to reinstall a program that might be misbehaving. However, let me offer a word of caution. While some setup programs have the name of the program, many don't and just say "setup file.exe," so you have no way to know one from the other. What I do is set up a folder (within my download folder) with the name of the program. I then save the setup file in that folder. This is also a good idea since some setup files come in .zip format. Remember once the program has been installed the setup file is not really needed unless you plan to reinstall the program. If you end up with a lot of them, including some large downloaded files, you might consider saving them to a CD or DVD, possibly by year.

SD Card Class – What Does It Mean?

We all know that SD cards come in various capacities, these cards, no larger than a finger nail go from a meager 32MB up to a whooping 128GB and maybe more. Most tablets today limit the capacity of an SD to a max of 32GB. But not all SDs are created equal, and that is where class comes in.

Basically it all comes down to transfer speed. Manufacturers use different types of flash memory to make the card. The class rating is designed to indicate the minimum writing performance to ensure smooth transfer of streaming content like videos. There are basically two kinds of speed designation. Speed class is a number surrounded by a large C and Ultra High Speed Class is a number enclosed by a large U. The defined classes are 2, 4, 6, and 10 and apply to regular mini and micro cards.

Ultra high speed class only works on specific devices designed to record video at this level. They are not interchangeable with other cards. The USH Speed Classes are U1 and U2.

All speeds can transfer photos and documents. Class 2 is good enough for recording in standard definition but class 4 and 6 would be needed for full HD video recording. Class 10 would enable you to record full HD video and also grab HD-quality stills from that video.

If the tablet manufacturer states a specific or minimum class requirement you cannot use a card with a lower class. For example, a class speed requirement of 4 will work with 4, 6 or 10 but not 2.

As a point of information the higher the class the less fragmentation and would have an increase in speed.

It wasn't too many years ago that a hard disk in our computer didn"t even come up to the 128 GB size, and think of the weight savings in cameras.

Finally, if you aren"t sure what type of card your device works with, make sure you check the documentation or the manufacturer"s website before you purchase a memory card.
XP and Banking

I usually don't profess to follow some of the paranoid warnings of some people, however, I have to suggest that the very last thing you should be doing with a Windows XP computer is banking on line. Security support for Windows XP ended last April, and it's even worse if you happen to be using Internet Explorer. The highest version of IE supported in XP is 8 and that browser is also without any security support. You're slightly safer using Firefox or Chrome, but with XP receiving no security support from Microsoft, your system could be a prime target.

You should definitely stop banking online until you have another operating system.

Printing Coupons from Tablet

We know that using Drop Box or some other cloud storage makes it a snap to get things from one device to another, but what if you do not have a desktop computer?

Well, you do have to have a wireless printer. It doesn"t have to be yours, but you would have to be signed in to the network. For some of the newer printers there might even be an app available. Check out the Google Play store or the Android store and search for printing. You"ll find a lot of apps.

Google Cloud Print allows you to print from any printer that you've connected to the Google Cloud. You can even use a printer with a USB connection to a computer is many cases.

While browsing the store check for coupon apps as well. You may not need to print them at all. An App like RetailMeNot give you access to thousands of coupons that you can redeem straight from your tablet or smartphone just by showing at the checkout. Many retailers also offer their own apps that give you coupons that can be redeemed straight from your device. So shop around and you might find ways to have your tablet save you money at the checkout counter.

Will This Cord Fit My iPhone?

Most Android and Windows tablets and phones these days use what's called a micro-USB connection. You'll also find the micro-USB port on some cameras and MP3 players. The most common cord you"ll see is one with a USB to micro-USB connection. The same applies to the newer mini USB on some newer tablets.

This would allow you to plug you device into a computer to transfer files and charge. You can also plug this cord into a USB wall charger or even a car charger. Today the car chargers are starting to appear with both mini and micro USB ports.

Apple devices use a proprietary connector that only works with Apple devices, but can also be attached to wall and car chargers as long as you have the correct cable. The current Apple cable is called Lightning which used to be a 30-pin dock connector. Certified Apple connectors will generally cost significantly more than the low-priced cables and chargers available for the Android and Windows devices.

When Apple introduced iOS 7, many people found that cheaper non-Apple certified cables would no longer work with their devices and it's widely believed that Apple purposely prevents these cheaper cables from working with their devices.

All In the Family – Apple & Amazon To Allow Sharing

Apple and Amazon have both announced plans to allow members of the same family to share digital media content. Amazon"s plan is called the Family Library while Apple"s is named Family Sharing.

With Kindle's Family Library two adults and up to four children can share e-books. Adults can control which books children can access. Families will also be able to share apps, audiobooks and programming from Amazon Prime Instant Video. Family Library became available in October.

Apple's Family Sharing is part of iOS 8 and allows families to share music, videos, books and apps and to also share photo albums in the iCloud as well as a family calendar.

Malicious Advertising Targets Popular Websites

Visitors to several popular websites found their computers under attack thanks to malware distributed by two of the largest providers of ads on the Internet.

Among the sites affected were *The Jerusalem Post*, and music streaming site last.fm. But many more sites may also be inadvertently distributing the malware.

This malware has hitched a ride in ads distributed by doubleclick.net (which is a part of google) and ad agency Zedo. These companies place ads on websites and the sites are paid by the number of people who click. The individual sites don"t select the ads, the ads are provided by the ad placement companies. Websites trust that legitimate companies like doubleclick.net will screen the advertisers appropriately. But sometimes ads containing malware can get through. According to the folks at Malwarebytes, they "rarely see attacks on a large scale like this."

In this case, the actual websites don't have malware infections. These bad ads send people who click on them to sites that infect their computer with an exploit kit that searches the computer for vulnerabilities and then installs a bot that will then begin to download other malware to the infected computer. So, this is pretty bad news if you get infected.

This particular toolkit is called Zemot and Microsoft updated their Malicious Software Removal Tool to detect it recently.

So be diligent. Do your best to avoid those little ads that pop up on web pages, but how many times have you accidentally clicked on one? The best thing is to make sure you have adequate anti-malware protection such as Malware Bytes in place.

Beware eBook Malware

Security experts are warning eBook users to beware of malware attacks attached to eBooks. Bad code contained in the e-book data could infect your computer or tablet and even steal your credit card information from your Amazon, Nook or other account.

Most of this bad data would most likely come attached to pirated books or books side-loaded from stores besides official Kindle, Nook, or Google stores.

Pirated books are especially vulnerable to these kinds of attacks (It's not like you"d expect someone who sells stolen books to be honest in other areas of life, is it?) So if you see an eBook that"s selling for $10 everywhere else for $1 somewhere, beware. You"re probably much safer getting your books from the official store of your eReader or through legitimate library apps like OverDrive.

Also be cautious of site promising you free eBooks. Many of these pirate sites contain malware that could compromise your PC.

Hundreds of Art Books You Can Download for Free

Speaking of books here is an interesting site. The Getty Museum in Los Angeles houses a vast collection of amazing art and has also published an extensive library of books about art. Now they are making 250 of those publications available for you to download absolutely free at home.

To get a look see and get started, go to the Getty Publications Virtual Library. You can search for publications by Title, Author or Keyword. Or you can narrow the search by the Getty program, publication type, category or series.

You can also choose to browse the available publications from the J. Paul Getty Museum, Getty Conservation Institute and Getty Research Institute.

You can choose to read it online or download it as a PDF. If you choose to read online, Google Books will open it for you to read in a browser. If you download it any PDF reader will open and you can then click the icon to download and save the file. Some of these files are quite large because of the amount of images, so they could take a while downloading. If you have a PDF reader, you should be able to read these books on a PC, tablet or even a smartphone.

These books feature the works of many artists, many of which you may be familiar with.

This site is a great place to explore art and you can't beat the price!

From the November 2014 issue of the The LVCG Journal*, newsletter of the Lehigh Valley Computer Group, PA. Courtesy of APCUG.*

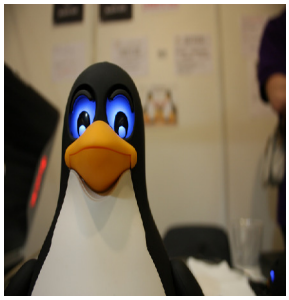
Society News

Help's Half Hour Notes
by Jan Rothfuss

Q: Who uses Windows 7?
A: Today is the last day that Microsoft supports it. They will continue to offer security fixes and they offer support for business at a price.
Q: How is Windows 10 coming?
A: It was shown at the electronics exhibition. Those who like touch screen will find it similar to Windows 8. Those who prefer mouse/keyboard it has been improved.

The Lighter Side

Linux SIG



The next workshop is the third Saturday in Feb., the 21st, at Interlock Rochester, 1115 E Main St. Enter through Door #7 on the end of the building near Goodman. Go up stairs to suite #200.

Come to get your questions about Linux answered. We have experts on hand to fix problems and answer questions about Linux and FOSS. Bring your system in so we can help you get the most out of it.

Enter through Door #7 near Main Street end of building. Find Interlock on the intercom directory to get buzzed in.

Hope to see you there!

RCSi Officers

Pres: Steve Staub 429-9877
srstaub1@rochester.rr.com
VP: Dan Rothfuss 347-6020
dr123498@hotmail.com
Sec'y: Arpad Kovacs 467-9270
podman@rochester.rr.com
Treas: Dennis P. MacMahon 235-1260
taxaccuracyinc@live.com

Board Members at Large:
Term ends 9/17:
Tony Dellelo 734-6149
tonydel@techie.com
Term ends: 9/16
Bob Avery 385-4491
bobajr@sprynet.com

Term Ends 9/15:

Sally Springett 442-3776
sspringe@rochester.rr.com

Standing Committees

Programs: . . . . . Tony Dellelo
Membership: . . . . . Steve Staub
Monitor: . . . . . Sally Springett
Webmaster: (webmaster@rcsi.org) . . . . . Bob Avery
Linux SIG: (unixgeek@faultline.com) . . . . . Carl Schmidtann