Bits of Bytes

Newsletter of the Pikes Peak Computer Application Society, Colorado Springs, CO

Volume XXXIII | December 2013 | Issue 12

Next P*PCompAS meeting: Saturday, 7 December 2013
The Pikes Peak Library District will show us how to access their CyberShelf.
We will be meeting at the East Library. Doors open at 8:30 am; meeting at 9 am.

The Prez Sez

by John Pearce, President, P*PCompAS

The December meeting is at the East Library, 5550 N. Union Blvd., in Conference Rooms 1 & 2. The presentation by Shannon Miller and other members of the library staff is on the electronic library called CyberShelf.

The business meeting will start at 9 am and will include election of officers for 2014. Coffee and donuts will be available as usual and the presentation will start at 10 am.

Be sure to BYOD (bring your own device) with a fully charged battery, your library card, and your library PIN. ☺

Meeting Minutes

by Ilene Steinkruger, Guest Secretary, P*PCompAS

John Pearce called the November 2, 2013 meeting to order at 9 am and announced that Laura of Starbucks, 750 Citadel Drive East (Barnes & Noble) generously provided us with a large package of coffee for today's meeting. Guests receive refreshments free at their first visit and members are asked to voluntarily contribute $1 toward the doughnuts, which Pat Krieger graciously brought. Two sympathy cards were available for members to sign in memory of member Brad Logan and Chuck Blaney's wife, Fritzie.

The program entitled "Safe Browsing with Firefox" will be presented by Bob Blackledge in place of the previously scheduled program by Toni Logan. Because Bob has another commitment, today's meeting will be adjusted so Around-the-Room (Q&A) will be held following the program.

The minutes of the October 5th meeting were approved as published in the newsletter.

OFFICER REPORTS

Vice-President Bob Blackledge briefly described the December 7 "CyberShelf" program planned for the computer lab at the PPLD East Library, 5550 North Union Boulevard. Members are requested to bring their wireless devices, account log-in, chargers, and library card and pin number so they can perform techniques demonstrated by PPLD staff members. There is to be NO open coffee in the room. Detailed information and a map will be emailed to members prior to the meeting.

Dennis Conroy, Treasurer reported a $.49 dividend on the money market account bringing it to $5,810.64, $60 dues income for a total in checking of $903.49 and a financial total of $6,714.13.

Membership Chair Ann Titus thanked those who have paid their dues for 2014 and requested all members renew for the coming year.

Newsletter Editor Greg Lenihan said the deadline for submitting articles to the November newsletter is November 23, one week after the social breakfast.

Librarian Paul Major had nothing to report.

BOD President Gene Bagenstos had nothing to report.

APCUG Representative Joe Nuvolini announced that APCUG dues for 2014 have been paid. This month Joe included a new feature to our website http://ppcompas.apcug.org/ and demonstrated the audio recording that will be updated and included each month for members wanting to reference the meeting information for the current month only.

Media Rep Ilene Steinkruger said that Friday she forwarded the current newsletters from O'Reilly, Focal Press Creative Community, and Routledge to all PPC members and has a hardcopy of each at the meeting today for anyone wanting to read them. Please notify her if

Continued on page 2

In This Issue

Articles

P*PCompAS

Meeting Minutes (Continued from page 1)

you have books to suggest.

OLD BUSINESS

Frank Fraser, Nominating Committee, reported the following members have agreed to be officer candidates for 2014:

President: John Pearce
Vice President: Bob Blackledge
Treasurer: Dennis Conroy
Board of Directors: Warren Hill (reluctantly, so if another member is interested, notify Frank)
Secretary: Toni Logan (provided she can write abbreviated minutes of the business meeting)

Discussion followed because it is so difficult to find a candidate for the office and the responsibilities of the office are very time consuming. A number of members want access to information from the program or shared during around-the-room especially if they miss the meeting. The audio recording now available on the website will hopefully provide a solution to the dilemma. Another volunteer for the secretary position is still desirable.

NEW BUSINESS

The first Saturday of December our meeting room at the Springs Community will be unavailable thus we will have our meeting at the East Library. For December 2014 the room will probably not be available the first Saturday therefore our meeting will be scheduled for the second Saturday unless another satisfactory venue is available for the first Saturday of December 2014.

Greg Lenihan was presented a Certificate of Participation from the APCUG judges as a result of the Bits of Bytes Newsletter being submitted to the annual APCUG newsletter contest. John Pearce made the presentation and congratulated Greg for his dedication as Editor. Joe Nuvolini was also acknowledged for his maintenance of the P*PCompAS website and Pat Krieger for her past conscientious writing of user group meetings and proceedings.

John announced that Gene Bagenstos was managing the door prize drawings today and had also brought numerous electronic-related items for the drawing.

He also reminded members that the next meeting will be at the East Library where the program will be about the library's "Cybershelf."

PROGRAM

Bob Blackledge provided a very enlightening program entitled "Safe Browsing with Firefox," and began by discussing some of the Web browsing negatives characteristic of Internet Explorer, Google Chrome, and Safari as well as concerns such as Active X and 3rd party cookies. He then discussed and explored a variety of attributes and security features available for Mozilla Firefox. Mozilla is a non-profit organization that created Firefox, a free Web browser. It provides numerous free/open source

Continued on page 3

In Memory of Brad Logan

1928-2013

The club expresses its condolences to the Logan family. Brad was a member and former officer, and the husband of current secretary Toni Logan

Nybbles and Bits

by John Pearce, P*PCompAS

Bob Blackledge did a great job presenting the NoScript add-on for FireFox at the November meeting. I've been using it for several years. In addition to NoScript, you might consider using the BetterPrivacy add-on to manage Locally Shared Objects.

Adobe Flash Player creates Locally Shared Objects (LSO's) on your local hard drive. These are sometimes called super cookies or Flash cookies. LSO's are not cookies in the traditional sense of an HTTP cookie (browser cookie). What makes an LSO different? The LSO's never expire; they can store up to 100 KB of data as compared to 4 KB for a HTTP cookie; they are created and queried without the user's permission; they can be used to recreate HTTP cookies that have been deleted.

LSO's operate independently of a particular browser. An LSO created while using Internet Explorer can be read when that same website is viewed by FireFox. This happens because the LSO's are controlled by Flash and the website being visited rather than by the browser being used. Generally, HTTP cookies are not shared between browsers.

BetterPrivacy gives you the option to delete LSO's when you close FireFox. You can protect selected LSO's from deletion. The BetterPrivacy FAQ covers this issue. In addition, the default

LSO file named *settings.sol* is not deleted by BetterPrivacy.

If you want to see if there are any LSO's on your computer, open Windows Explorer and start at c:\Users\<your username>\AppData\Roaming\Macromedia\Flash Player\#SharedObjects and just keep opening the next folder until you get to the bottom level. You can see your Flash Player configuration settings at **http://www.macromedia.com/support/documentation/en/flashplayer/help**. ☺

Meeting Minutes (Continued from page 2)

Bob Blackledge presents Firefox browsing in November.

apps/plug-ins/add-ons to allow computer users to control their web experience. See http://www.mozilla.org.

Although there are many Web vulnerabilities, Bob concentrated on two specific add-ons that help provide privacy and security for computer users and then gave a detailed demonstration of how to access and use them. He entertained questions as they arose and encouraged members to access and experiment with the plug-ins.

NoScript - an add-on that "allows active content to run only from sites you trust and protects against XSS and Clickjacking attacks."

Request Policy - "an extension that improves the privacy and security of your browsing by giving you control over when cross-site requests are allowed by webpages you visit," and avoiding CSRF (Cross-sit Reference Forgery).

AROUND THE ROOM HIGHLIGHTS

Jeff Towne questioned how to back up a website.

Joe Nuvolini showed a short video in which John McAfee was interviewed and discussed security issues with the Obama Care website. People who access the site can easily be susceptible to hackers that steal personal information.

Deborah Jordan requested information regarding problems she encountered with her mouse use on her Vista operating system.

Continued on page 5

From Your Nominating Committee

By Frank Fraser, P*PCompAS

This is to advise you that the following members will be running for the positions indicated at the December meeting. President: John Pearce, Vice President and Program Chair: Bob Blackledge, Treasurer: Dennis Conroy, Secretary: Toni Logan, and BOD member: Warren Hill.

I would like to thank everyone for your support by volunteering for these important positions in our Club. Without your dedication to this great organization, we would be unable to function.

Also a reminder: Just because we have volunteers for the positions noted above, does not mean that you should not volunteer to run. Each position will be open one more time for nominations/volunteers, prior to the elections being held at the December meeting.

Nuggets from Nuvo

*by Joe Nuvolini, P*PCompAS*

Neil McAllister has an interesting article on the Windows 8.1 rollout in *The Register*. I'll try to summarize it. Windows 8.1 is being offered as a free upgrade for Windows 8 users. However, getting the upgrade is not that simple, especially if you have several Windows 8 computers. The upgrade can be downloaded from the Windows store, but there is no ISO file, so the download/upgrade must be done separately for each computer, unless you are an enterprise customer with Volume Licensing (VL). This can be a real headache for a small business with multiple computers. The 3.5 GB download and update must be performed on each machine. The installation media for (VL) versions of the new OS can do in-place updates over existing Windows 8 installs. Folks who installed Windows 8.1 Preview have additional issues. Only their user accounts and data will be saved. Applications will have to be reinstalled, including Windows Store apps. If you are upgrading from Windows 7, you can order Windows 8.1 media to accomplish the task. Not so for XP and Vista users. They must purchase Window 8 media, install it, and then download and install the Windows 8.1 update. Based on Neil's article, I wish you Good Luck! For the full text of his article visit: http://www.theregister.co.uk/2013/10/17/windows_81_update_what_to_know/.

Recently John McAfee appeared on the Fox Business Network's "Cavuto." He discussed the flaws in the Obamacare Website. He claimed that the site as designed "is a hacker's dream" that will cause "the loss of income for millions of Americans who are going to lose their identifies." He pointed out that there is no central exchange which lists all the legitimate brokers for all the states so you can pick or choose a valid one. Currently, any hacker can set up a site, make it look legitimate, and secure all sorts of very personal information which can most assuredly make you a victim of identity theft. He predicts that millions of Americans will have their assets wiped out in one day because they signed up for Obamacare. You can watch the video clip at: http://www.truthorfiction.com/rumors/m/john-mcafee-warning-101613.htm#.UnAZLXCPP-s.

I found this item concerning health problems arising from excessive use of high tech devices. Some iPhones and iPad users have reported migraines or nausea, prompting Apple to issue a fix. Next is phantom vibration syndrome. That's when you hear a phone buzzing and always think it's yours, when it probably isn't. How about "laptop thigh?" If your laptop runs hotter than 110 degrees, it can cause pockmarking and discoloration of your legs. I'm sure most of you have suffered neck and/or back issues from hunching over your monitor. Finally there's "Octus Rift." This occurs when you wear 3-D goggles that put you into a virtual world when playing certain video games. They make some sick and "off their feed" for the rest of the day. ☺

The digerati were preparing themselves for Thanksgiving at the November breakfast at the Country Buffet. They gave thanks for the good food and fellowship and started making their holiday plans.

Do Not Fall Prey to the Vicious Cryptolocker Extortion

Published with permission from Ira Wilsker, Golden Triangle PC Club, columnist for The Examiner, Beaumont, TX

WEBSITES:
http://www.dhs.gov/national-cyber-security-awareness-month
http://www.fbi.gov/news/news_blog/national-cyber-security-awareness-month-2013
https://en.wikipedia.org/wiki/Cryptolocker
http://blog.emsisoft.com/2013/09/10/cryptolocker-a-new-ransomware-variant/
http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information
http://nakedsecurity.sophos.com/2013/10/18/cryptolocker-ransomware-see-how-it-works-learn-about-prevention-cleanup-and-recovery/
https://en.wikipedia.org/wiki/Key_size

GRAPHICS:
http://blog.emsisoft.com/wp-content/uploads/2013/09/crilock.png
http://blog.hotspotshield.com/wp-content/uploads/2013/07/who-is-spying-on-you.png

October was the tenth anniversary of National Cyber Security Awareness Month (NCSAM). According to a statement on the FBI website, "(National Cyber Security Awareness Month) Established by presidential directive in 2004, the initiative—administered by the Department of Homeland Security—raises cyber security awareness across the nation by engaging and educating public and private sector partners through a variety of events and programs. The ultimate goal is to protect the country from cyber incidents and respond to them effectively if they do occur."

Around the country, at K-12 schools, colleges, universities, and private businesses, thousands of seminars and events took place during NCSAM in order to educate computer users at all levels on cyber security. I had the honor and privilege of presenting two citizen awareness sessions for the city of Port Arthur, Texas. I discussed several of the contemporary online threats and how users could effectively protect themselves from those threats. One of the warnings that I repeated several times was to never open e-mail attachments, as they are a common vector used to bypass much of the security software that we (should) have installed on our computers.

Now that the National Cyber Security Awareness Month is behind us, we should not forget the lessons learned about clicking on e-mail attachments. Unlike our new years' resolutions that many of us make, but quickly forget to implement, cyber security threats are continuing, and in many cases becoming more threatening. One recent example is a new version of an old Russian cybercriminal extortion scam; in the original versions, which took over countless millions of computers worldwide (and still showing up in large numbers), the purloined computer displayed a window after boot that had an official looking logo of the FBI or other law enforcement agency, along with an official looking criminal complaint

Continued on page 7

Meeting Minutes (Cont. from page 3)

She also suggested Hit Man Pro (available from CNET) to remove Anti-Virus Service Pro if mistakenly installed.

Harvey McMinn recently attended an AV expo in Denver and reported future features including 8 K and curved screens.

Greg Lenihan reminded members of the CryptoLocker malware/virus and its potential destructiveness. Cryptoprevent http://www.komando.com/downloads/category.aspx?id=15499&page=2 a free utility may be useful solving the problem as well as using a good back-up program such as Acronis True Image to prevent.

DRAWING

Pat Krieger—Adding Machine
Jeff Towne—Keyboard
Dennis Conroy—Speakers
Barbara McMinn—Zip Drive
Stanley Rapaport—Tickets to AFA game
Greg Lenihan—USB Headset.
☺

Stan "Pineapple Man" Rapaport played an early Santa by handing out the golden fruit at our November Membership Meeting.

Safe[r] Browsing with Firefox

by Bob Blackledge, P*PCompas

In November's P*PCompAS presentation, we covered the Firefox browser (Mozilla.org), and specifically two important Add-Ons/Extensions: NoScript and RequestPolicy.

In this article, we'll quickly review the material, and also mention several other add-on/extensions which might be of value (from a security perspective). For illustrative purposes, we'll use Weather.com as an example for now—it's only a harmless example of what you might encounter at a common website and should NOT be the basis of thinking poorly of Weather.com!

Add-ons for Firefox are usually obtained from the Firefox add-on/extensions website (**addons.mozilla.org/en-US/firefox/**), but the source URL and last release date for each is also provided below. Add-ons[/extensions] can be individually enabled, disabled, or removed starting from Firefox's menu-bar Tools > Add-ons> (about:addons).

As presented, NoScript (NoScript.net Oct'13 Ff) protects your browsing by disabling (by default) scripts at a visited site (such as Weather.com) and any sites it directly references for content—all of which can be the basis of much net-based security problems. NoScript adds a Snake ("S") icon to the Firefox toolbar that indicates the state of protection currently being provided. Right-clicking this icon produces a drop-down list of websites explicitly referenced from the current website, and their blocked status (7 accessed by Weather.com including itself). Individual sites here may be enabled permanently or temporarily (what I use). Once enabled, a website will be permitted to be accessed, including running scripts, for the remainder of this browser session (temporarily enabled) from ANY website or until explicitly disabled on a site-by-site basis. Additionally, ClickJacking (replacing an apparant target URL on the fly with another URL) is protected! Commonly, you will permanently enable websites you use all the time (your bank, your credit-card, Google, Amazon, etc), and only enable other sites when you actually need them; there are usually related websites you will need to enable to get the full functionality (such as Gstatic.com & GoogleUserContent.com from Google.com, and images-amazon.com & ssl-images-amazon.com from Amazon.com) which are often used for load-balancing.

Many times a website is fully functional without the additional references, but if the website doesn't work correctly you can enable other referenced sites one by one (or all at once temporarily).

RequestPolicy (RequestPolicy.com Aug'13 Ff) extends the scripting protection to sites referenced from the website you're visiting beyond just content, known as XSS (or Cross-Site Scripting) where scripts may be loaded directly from Weather.com, or embedded in script/graphic/flash/HTTP references. Similar to NoScript, RequestPolicy adds a 'flag' icon to Firefox which goes from red (some sites are blocked) to grey (nothing blocked), and right-clicking the icon produces a list of sites that can be enabled permanently or temporarily, specifically when referenced from the current website (Weather.com in our example) or globally. This means that if you've enabled, say GoogleAdServices.com from Weather.com, it will NOT be enabled when referenced from KKTV.com. With NoScript (alone) enabling, GoogleAdServices.com would enable access when visiting ANY website (not merely Weather.com). Weather.com references three other websites (depending upon where you go or click on while there (I enable imwx.com and fonts.googleapis.com, but not DoubleClick.net).

Beyond these two, there are many additional add-ons/extensions of some personal security interest that I use and you might want to consider:

* FlashBlock (flashblock.mozdev.org Apr'13 Ff)—replaces each HTML reference to a Macromedia Flash/Shockwave/Authorware file to a visible button, which may be individually clicked to enable just that file to download/run. Websites can be white-listed for being permanently enabled, or left disabled.

* BetterPrivacy (betterprivacy.en.softonic.com Jan'13 Ff)—protects against "Super Cookies" within Flash/... (officially LSOs or Local Shared Objects), which browsers don't control, and are much more powerful than normal cookies.

* DisconnectMe (Disconnect.me Oct'13 Ff; Collusion: C,S)—also blocks tracking websites it knows, and left-clicking the browser's "D" icon will show how many websites for Advertising, Analytics, Social and Content were blocked; and how much time/bandwidth was saved and how many requests were "secured."

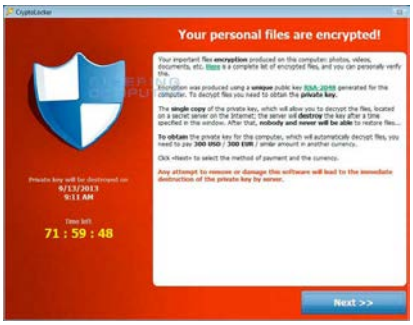
* DoNotTrackMe (abine.com Jul'13 Ff,iE,C,S)—a tracking web-

Continued on page 7

CryptoLocker (Cont. from page 5)

that child pornography (or other illicit content) was found on the computer. Nothing else could be done on the computer, as it was effectively locked by the "FBI." The computer user was told that if they did not pay the fine, typically $200, within 24 or 48 hours, he would be subject to arrest, charged with a felony, and face 10 years in federal prison, plus a $10,000 fine. Detailed instructions were provided on where to purchase a specific prepaid debit card, and then entering the cards 16 digit number into the payment box on the warning screen. After payment was received, the 'FBI" would drop the charges and (hopefully) release control of the computer.

The especially nasty new type of ransom ware, also likely from Russia, goes a step further than the other recent ransom ware; the new version contains a version of a vicious piece of malware called "CryptoLocker." Some variants contain a version of the well-know Zeus trojan, which is used to install and run CryptoLocker. Typically spread via an e-mail attachment, often apparently sent from a known acquaintance or company, the attachment appears to contain a ZIP file with a disguised file that looks like an innocent PDF file. I have personally received dozens of these e-mails, and I will admit that they do look like they are from a legitimate source, but I know not to open e-mail attachments that have any vestige of being suspicious. Once opened, the attachment executes, installing itself in the Documents and Settings folder with a random file name, adding a startup command key to the registry which causes CryptoLocker to load when the computer is booted. CryptoLocker then goes through a series of servers, making it difficult to trace, eventually connecting to a command and control server. This remote server generates a very sophisticated 2048-bit RSA encryption key pair using the public key to encrypt Microsoft Office and Open Document files, as well as some common graphics file formats. CryptoLocker will not just encrypt the computer of the user unfortunate enough to open



the e-mail attachment, but can also encrypt those file types on any mapped network drive, including USB drives, network file shares, and even cloud storage folders that are made to appear as a drive letter (like "G:\" drive), which may effectively shut down a business, school, hospital, or government agency that uses mapped network drives; it only takes one infected computer to possibly compromise the targeted files on an entire network.

Once the files are encrypted using the 2048-bit RSA public encryption key, a warning is displayed on the computer that critical data files have been encrypted, and that the ransom (extortion) payment must be made in a specified time, often 72 or 100 hours, or else private encryption key on the command and control server will be destroyed and "nobody and never [sic] will be able to restore files". The extortion demand is, " ... a payment of either 100 or 300 USD or Euro through an anonymous pre-paid cash voucher (i.e. MoneyPak or Ukash), or 2 Bitcoin in order to decrypt the files." Anecdotally, some published reports have claimed that some businesses have received cyber extortion demands of $10,000 or $20,000 dollars, or equivalent amounts in Euros or Bitcoins (private currency). In order to add a sense of urgency, a countdown timer is displayed

Continued on page 8

Safe[R] Browsing (Cont. from page 6)

site blocker/deleter; they also have newer add-ons named MaskMe and DeleteMe which I've not investigated.

* GooglePrivacy (code.google.com/p/gprivacy/wiki/README Nov'12 Ff)—enforces Ff's "Do Not Track" option at Google, YouTube, Yahoo!, Bing! and Faceboook with additional control. You enable this tracking option in your Ff browser in Tools> Options> Tracking.

* Adblock Plus (AdBlockPlus.org/en/ Oct'13 Ff,iE,C,O)—blocks banners, pop-ups/-unders and video, 'unacceptable' ads as well as social-media tracking-buttons, and adds an ABP clickable icon on the Ff toolbar. Note that most websites get revenue by displaying ads, so you're not helping them if you block all ads.

* CertificatePatrol (patrol.psyced.org Mar'13 Ff)—monitor/compare/report SSL certicate changes for HTTPS accesses. Interesting for me, but not for the casual user!

So have a safe[t] browsing experience with Ff plug-ins/extensions! ☺

CryptoLocker (Continued from page 7)

indicating the deadline to pay the ransom, or the files will forever become unrecoverable (Image: http://blog.emsisoft.com/wp-content/uploads/2013/09/crilock.png). The 2048-bit encryption keys used by CryptoLocker are considered in the security industry as extremely secure and virtually unbreakable, and can be expected to meet security requirements until the year 2030 (source: en.wikipedia.org/wiki/Key_size#Asymmetric_algorithm_key_lengths).

Almost all of the common security suites, including Kaspersky, Symantec, Sophos, Emsisoft, and others, can detect and remove the CryptoLocker malware and the Zeus trojan, but no one (yet) has been able to come up with a practical method to crack the encryption key and recover the encrypted files; effectively they are gone forever. Removing the infection is a moot point, as the encrypted files will remain unusable. While some experts claim that paying the extortion prior to the expiration, hoping that the cyber criminal will send the private key necessary to decrypt the files, many others, including most law enforcement agencies do not condone paying ransom under the theory that it will only encourage more criminal behavior. Cited by Wikipedia, “Symantec estimated that 3% of users infected by CryptoLocker chose to pay the ransom.” Do some simple arithmetic; if a million computers are hijacked by these criminals, and only 3% pay a $200 ransom, the crook receives a cool $6 million in illicit proceeds. Since multiple millions of computers have been held for ransom by CryptoLocker, the proceeds to the criminal enterprise may be staggering.

As is typical, prevention is the best method from being taken over by CryptoLocker or any of the other cyber threats. Sophos, a well respected multinational security company headquartered in the UK has published “Five “top tips” for keeping safe against malware in general, and cyberblackmailers in particular” (nakedsecurity.sophos.com/2013/10/18/). The first of the five tips is common sense, and a task incumbent on all computer users, “Keep regular backups of your important files.” After cleaning the CryptoLocker and any other malware that infected the computer, the encrypted files can be safely deleted and replaced by their backup copies. One strong warning about the backup copies and the devices that the backups are stored on; do not leave the backup devices, such as external hard drives, attached to the computer or the network, as they will likely have a drive letter that can be identified by CryptoLocker. If CryptoLocker can see it, it will also encrypt the files on those devices, making the backup copies as useless as the encrypted files on the primary hard drive. Good practice is to frequently rotate through multiple backup devices, creating redundant backup copies, and never allowing more than one device to be attached and running at any given time. The other backup devices should be stored securely, and only connected in rotation, never having more than one backup device connected at a time. While CryptoLocker may also encrypt the files on an attached backup device, it cannot attack any unattached devices.

The second tip from Sophos is the often stated, “Use an anti-virus, and keep it up to date.” I would add to that rule that it should also be required to do frequent and periodic security scans for malware using alternate third-party security software such as Emsisoft, SuperAntiSpyware, and MalwareBytes. My rationale for this secondary scanning by alternative scanning utilities is that prior infections may have either slipped through the primary security software, or rendered itself immune to detection by it. There are documented cases of CryptoLocker being downloaded and installed by Zeus or other malware that was already present on an infected computer, without a user opening an e-mail attachment.

“Keep your operating system and software up to date with patches” is Sophos’ third tip. Software publishers often release patches and updates to close newly detected security vulnerabilities. According to Sophos, “This lessens the chance of malware sneaking onto your computer unnoticed through security holes.”

Number four on the Sophos list of tips is, “Review the access control settings on any network shares you have, whether at home or at work. Don’t grant yourself or anyone else write access to files that you only need to read. Don’t grant yourself any access at all to files that you don’t need to see—that stops malware seeing and stealing them, too.”

Sophos concludes its list of five tips with, “Don’t give administrative privileges to your user accounts. Privileged accounts can “reach out” much further and more destructively both on your own hard disk and across the network. Malware that runs as administrator can do much more damage, and be much harder to get rid of, than malware running as a regular user.”

Using the lessons learned during National

Continued on page 9

What to Do if You Think Your E-mail Has Been Hacked

by John King, Contributing Editor, Golden Gate Computer Society, July 2013 Issue, GGCS Newsletter, editor (at) ggcs.org

The first thing to do if you worry about e-mail hacking is to change your e-mail account password to something more complex than 123456. For best security, use a password such as Q*93im#&qrR-57$. You'll never remember it and won't have any more e-mail problems [insert snicker].

My Hotmail account was hacked a while ago. A human hacker or automated bot was indeed sending spam from my account on Hotmail. My local computer wasn't involved. Everything was happening on the Hotmail computers.

Spammers like to use other people's e-mail accounts to send spam because it's free and makes the spam harder to block. After I changed my weak Hotmail password to a stronger one, the spammer/bot couldn't access my account; and the problem ended.

Alternatively, a spammer may be simply spoofing the return address of the spam using your e-mail address to make the message less likely to be blocked. There's nothing that you can do to stop that. You could stop using that e-mail address, but the spammer can keep using it as the return address anyway.

Fortunately, spam with your spoofed return address usually stops in a few days or weeks at the most. The spammer probably found your address without hacking your account, for example, from the address book of a friend, an intercepted email, etc. Nonetheless, changing your e-mail password is still a good idea.

If your e-mail is a POP account, as opposed to a Web mail account such as Hotmail or Gmail, the odds are higher that your computer has been hacked, which is a much larger problem. The best solution is to restore a backup system image made well before the hacking was suspected. The chance that you have a backup image to restore is as likely as the intruder putting money into your bank account, but this instance is when you want backups. Lacking a backup, you can thoroughly scan your system with several antimalware products in addition to your normal antivirus product.

Again, you should change the passwords for your Internet Service Provider, router, and e-mail, and be sure that your Wi-Fi network is protected with the highest level of security possible. People often hate passwords on computers; but if any computer on the network was hacked, all computers on the network should have logon passwords. Fortunately, protecting the network is enough in most cases.

Personally, I'd suggest you change your e-mail password, scan your computer with your up-to-date antivirus software, and wait to see what happens. If possible, do not do any online shopping or banking until some time has passed to confirm that only your e-mail was hacked. Also watch for any suspicious activity on credit card and bank accounts. ☺

Tip: Shortcut for Horizontal Scrolling in a Window

You might have heard that you can press the Ctrl key and use the mouse scroll wheel to make text larger and smaller. Another thing you can do with the mouse wheel is scroll across a page by pressing the Shift key.

You may not come across this problem often, but if you are on one of those annoying pages that don't quite fit in a window, and force you to scroll from left to right, then you may find this trick useful. ☺

CryptoLocker (Continued from page 8)

Cyber Security Awareness Month, such as "don't click on and open e-mail attachments," being aware of the tremendous threat and damage that the rapidly spreading CryptoLocker Ransomware can wreak, and following the five safety tips recommended by Sophos, our computing safety and security may be much improved. Remember that in computers, as well as in other aspects of life, prevention is far better than the alternatives.☺

P*PCompAS Newsletter
Greg Lenihan, Editor
4905 Ramblewood Drive
Colorado Springs, CO 80920
e-mail: glenihan@comcast.net

Coming Events:
Next Membership Meeting: 7 Dec, beginning at 9 am (at East Library)
Next Breakfast Meeting: 21 Dec@ 8 am, Country Buffet, 801 N. Academy Blvd.
Newsletter Deadline: 21 Dec.

Check out our Web page at: http://ppcompas.apcug.org