QBITS

Quad-Cities Computer Society

Newsletter for February 2014

Volume 32, number 1

563-265-1728

www.qcs.org

Data Privacy Day (DPD) January 28, 2014

Editor's note: Even though the observance of this day has passed by publication, it is an important issue for our members to consider and examine.

Data Privacy Day (DPD) is January 28, 2014. DPD encourages everyone to make protecting privacy and data a greater priority. It is an effort to empower and educate people to protect their privacy and control their digital footprint.

Data Privacy Day began in the United States and Canada in January 2008 as an extension of the DPD celebration in Europe. Data Protection Day commemorates the January 28, 1981, signing of Convention 108, the first legally binding international treaty dealing with privacy and data protection. DPD is now a celebration for everyone.

DPD is led by the National Cyber Security Alliance, a nonprofit, public-private partnership dedicated to cybersecurity education and awareness

Go to the **Privacy Day Observance** website: **goo.gl/ViGbdk**

On that page click:

Private Library → Get Resources

This link will direct to many useful websites. Why privacy control is important. What are cookies? How to manage your cell phone privacy.

Check Privacy → Check Settings

This link will redirect you to many popular webs sites and their privacy pages and options for everyone to customize and configure.

Do Not Fall Prey to the Vicious CryptoLocker Extortion

by Ira Wilsker

WEBSITES:

http://www.dhs.gov/national-cyber-securityawareness-month
http://www.fbi.gov/news/news_blog/nationalcyber-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-learnabout-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."

Views and opinions expressed by presenters do not necessarily reflect those of the Quad-Cities Computer Society. Monthly meetings are open to the general public.

The QCS is a member of apcug An International Association of Technology & Computer User Groups

Would You Like to receive your *QBITS* via email?
The *QBITS* can now be produced in Acrobat PDF format and sent to your email box. If you desire to have the newsletter sent to you electronically instead of by US Mail, notify:
Patty Lowry,
QBITS co-editor
(563) 332-8679
pattylowry@rocketmail.com

QBITS
Published monthly by the
Quad Cities Computer Society
c/o Dave Tanner
3449 - 52nd St
Moline, IL 61265
webpage: www.qcs.org
Co-editors
Joe Durham
joseph85_us@yahoo.com
Patty Lowry
pattylowry@rocketmail.com

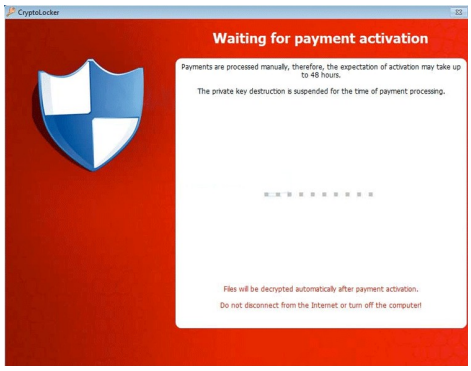
Around the country, at K-12 schools, colleges, universities, and private businesses, thousands of seminars and events took place during NCSAM in order to educate computer users at all levels on cyber security. I had the honor and privilege of presenting two citizen awareness sessions for the city of 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 email 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 email 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 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 email 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 emails, and I will admit that they do look like they are from a legitimate source, but I know not to open email 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 email 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 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

--continued on next page--

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 email 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 oj 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 Cyber Security Awareness Month, such as "don't click on and open email 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 alternative.

Monday, February 3rd
7:00 PM
"Practical Concepts for Protecting Your Computer: Its Hardware and Data" presented by Larry Stone

HOW DO I ENSURE THERE'S NO "NEXT TIME?"

Here are five "top tips" for keeping safe against malware in general, and cyberblackmailers in particular:

- **Keep regular backups of your important files**. If you can, store your backups offline, for example in a safe-deposit box, where they can't be affected in the event of an attack on your active files. Your backups will be rendered useless if they are scrambled by CryptoLocker along with the primary copies of the files.
- **Use an anti-virus, and keep it up to date.** As far as we can see, many of the current victims of CryptoLocker were already infected with malware that they could have removed some time ago, thus preventing not only the CryptoLocker attack, but also any of the damage done by that earlier malware.
- **Keep your operating system and software up to date with patches.** This lessens the chance of malware sneaking onto your computer unnoticed through security holes. The CryptoLocker authors didn't need to use fancy intrusion techniques in their malware because they used other malware, that had already broken in, to open the door for them.
- **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.
- **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.

Protect Your Laptop

Kathy Frey, Member, Computer Club of Green Valley, AZ
October Issue, *Green Bytes*
www.ccgvaz.org
Freyrbgv (at) gmail.com

Traveling to and from Green Valley or other parts of the world with a laptop in tow? Then here a few tips to keep it from being stolen.

1. Never leave it in your car. Keep it locked with a strong password and lock your case.
2. Do not put it on the floor of a restaurant, meeting room, airport, etc. If you do, then put your leg through the strap so you can feel its presence.
3. Do not keep your password in or around the case.
4. Do not leave it in the care of someone you just met so you can go to the restroom or talk to an airport agent.
5. Turn on alarms if you have them so you can hear if someone is tampering with your laptop or laptop case.
6. Check on the internet for other ways to secure your valuables

whether it be a laptop, iPad, iPhone or other device.

7. Treat your electronic gadgets like cash.

Filter Out Junk Email with Outlook 2010

By Lynn Page, Editor, Crystal River Users Group, Florida
November 2013 Issue,
CRUG Newsletter
www.crug.com
lpage46 (at) tampabay.rr.com

I have used Outlook for my email since my first version of Office (97). I keep my junk email protection level at high and have Outlook disable links in messages considered to be phishing and warn me about suspicious domain names.

Outlook's junk email filter is designed to keep spam and junk from getting to the inbox. It is on by default and will place the junk in its own folder. One of the default options is to have Outlook automatically delete suspected junk but it only takes a second to open the junk folder and glance to be sure something wanted didn't end up there. I changed the filtering protection from the default level to high.

Junk Email Options

To control Junk Email options while in Mail on Home tab in the Delete group click the down arrow by Junk. On the dialog box Options tab select the level of protection desired. Selecting No Automatic Filtering turns the junk email filter off but you can still block senders and that email goes into the Junk folder.

The Safe Senders tab lists email addressed that you trust and have noted so. Email addresses and/or domain names in this list are never considered junk, regardless of message content.

The Safe Recipients tab lets you add specify an email address you use for a mailing or distribution list. All email sent to that address is never considered junk. I use this for my Corel PaintShop Pro Groups.

All email from addresses or domain names on the Blocked Senders list are automatically considered junk.

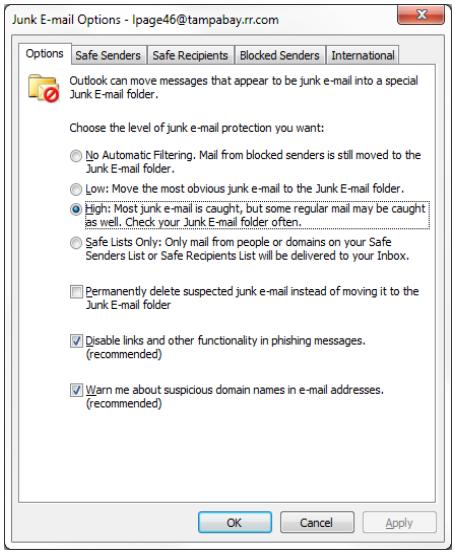
Add Senders to Safe Senders List

I mentioned that I keep the filter set to high so occasionally Outlook flags message I want as junk. That is not a problem. For an occasional email I simply drag it from the Junk to the Inbox. If the email is from someone I expect to continue to receive email from I add the address to the Safe Senders List.

Simply select the email in the Junk folder and in the Junk drop down menu (Home tab Delete group) select Not Junk and respond as required.

Block a Sender

Conversely a few times email slips through from someone I do not know and I don't want to continue receiving messages from them. In this case select the message and in the Junk drop down menu select Block Sender.



Interesting Internet Finds

By Steve Costello, President / Editor, Boca Raton Computer Society
October 2013 issue, *Boca Bits*
http://sefcug.com/
president (at) brcs.org

In the course of going through the more than 200 news feeds, I often run across things that I think might be of interest to other user group members.

The following are some items I found interesting during the month of October 2013.

How risky will it be to keep running Windows XP? **goo.gl/bM9iMi**

POP vs. IMAP: What Do They Mean and Which One Should You Use? **goo.gl/LMsSlm**

Talk to your Navigating Device: Android or iPhone **goo.gl/jA8VF7**

Can You Really Be Anonymous Online? **goo.gl/rKnVzJ**

Why You Don't Need an Outbound Firewall On Your Laptop or Desktop PC **goo.gl/uWA6jz**

How To Use the New Google+ Photo Editing Tools **goo.gl/LSErnW**

Where to Donate Your Used Tech **goo.gl/K24yZF**

How to Keep Your Internet Usage *Private [INFOGRAPHIC] **goo.gl/rW78WH**

How to View and Work on Google Drive Files When You're Offline **goo.gl/WRjkyX**

--continued on next page--

****

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

Goodbye XP

By Dick Maybach, Member, Brookdale Computer Users' Group, NJ

October 2013 issue, *BUG Bytes*
www.bcug.com
n2nd (@) att.net

On April 8, 2014 Microsoft will stop supporting Windows XP and Office 2003. After that date there will be no new security updates, non-security hot-fixes, free or paid assisted support options, or on-line technical content updates. However, all your software will continue to work just as well as it did on April 7, so you needn't panic, but it would be prudent to come up with a rational transition plan. There are three choices: (1) continue to use XP, but take some precautions, (2) keep your present hardware, but upgrade the software, and (3) purchase new hardware and software. The hardware and software vendors as well as the media in which they advertise prefer that you take the third approach, but let's consider all of them.

There are many advantages to staying with XP, which may not hold with the other two approaches.

* Your present hardware works with it.
* Your present applications run under it.
* It supports your present peripherals.
* You don't have to learn anything new.
* It costs less than the alternatives.

The main disadvantage is that as time goes on, you become increasingly more vulnerable to attack over the Internet and by malware. You can reduce this and its consequences by the following.

* Before April 8, 2014, use Microsoft Update to install the latest patches to all your Microsoft software.
* Update all your anti-malware software, and check that the vendor will continue to support it for XP after April 8. If not, change to a vendor that will.
* If you are connected to the Internet through a router, install the latest firmware in it. If your PC connects directly to your ISP's modem, purchase a hardware router, and update its firmware if necessary. For good measure, if you haven't already, install a software XP firewall.
* Be very careful about what you download, and avoid doing it if possible.
* Review you backup program; improve it if needed, and resolve to follow it rigorously.

The wording on the MS Website implies that old patches will remain available, but why take a chance? Update your software early, as the download rate may slow near the deadline. At the present time, about 35 per cent of the computers in the world use XP. This is a sizable market for anti-malware vendors, and I would expect them to continue supporting XP for some time. Your first line of defense against Internet aggression is your router and its firewall. Most likely, your ISP's modem also includes a firewall, but how careful is he about keeping it up-to-date? You don't know. With your own router, you have ability to keep it up to date, and as a result, having one is desirable even if you have only one PC. Despite all your precautions, as time goes on, and the bad guys find more XP vulnerabilities, your risk will increase. Be wary of any download, including e-mail attachments from friends. The best malware defense is to keep it off your PC. Your last defense is your backup program. Any information you haven't backed up on an external drive is one mouse click or one device failure away from trash. Although its most important to back up your data, you should in addition make an image backup of everything on your hard disk, because once XP becomes an orphan, applications and drivers for it will become increasingly difficult to find.

The second alternative is to keep your hardware, but change your operating system.

* Your vulnerability will be less than if you stay with XP.
* If your PC is old, it may not support some current operating systems.
* Your present applications may not run under the new OS.
* Drivers may not be available for some of your peripherals, requiring you to replace the devices.
* You will have to take care during the transition not to lose any data.
* You will have to learn new ways of working.

The hazard with this approach is that to install a new operating system, you generally must format your hard disk, but you must first inure that all your data is safe and readable by the applications in your new OS. For example, if all your financial records are stored in

Quicken files and there is no financial program available in your new operating system that can understand them, you essentially have lost all your financial records. A second problem is to insure that your current hardware supports the new operating system before you format your disk. If you are considering a newer version of Windows, run the Windows Upgrade Advisor (available at **windows.microsoft.-com/isis/windows/downloads/upgrade-advisor for Windows 7**). Don't forget to check your peripherals; I found that there was no Windows 7 driver for my scanner and had to buy a new one when I upgraded from XP. If your PC is compatible except for insufficient RAM, this is an inexpensive upgrade, even if done by a shop. (You should have at least one Gigabyte of RAM, even if you stay with XP.)

Consider Linux, especially for a secondary PC. I've converted two XP machines to Xubuntu (**xubuntu.org**), which is more responsive than XP on old hardware. It has the advantage that you can try it out with a "live-CD," which is bootable from a CD drive. It will be slow in this mode, but since it doesn't make any changes to the hard disk, you are just a reboot away from XP. While running Xubuntu, all the files on your hard disk are available, so you can check whether Linux applications can read them. (Instructions on how to create a live CD or DVD in Windows are available at **www.ubuntu.com/download/help/try-ubuntu-before-you-install**.) If you have room on your disk or can add a second one, consider a dual-boot system in which you can run either system. (All your Windows files will be accessible in Linux, and Windows applications are available that can read Linux disk partitions.) However, Linux is not Windows, which means there are many differences between the two systems. Try to find a sympathetic, experienced Linux user to help you get started, especially if you are less than comfortable in adventure mode.

The third alternative, buying new hardware and software is the easy and safe, but expensive. You are probably best off to purchase new components. XP-era processors, RAM, displays, and hard disks are woefully inadequate for any current OS. Keyboards and mice now cost just a few dollars, and your old ones may use obsolete connectors. You can keep your printer and scanner if drivers are available for the new OS; your old speakers will be fine.

* Your old PC with your data, applications, and peripherals remains available for use.

* You will probably have to purchase new applications for your new OS and probably some new peripherals, especially if the existing ones are several years old.

There will be a learning curve for the new system.

Spend some extra money; in particular, get more RAM and a larger disk than you think you can get by with.

I haven't considered a piecemeal hardware upgrade, because I don't think it's cost-effective. Most modern CPUs are incompatible with XP-era motherboards; new motherboards are usually incompatible with XP-era cases and expansion cards; and old RAM is incompatible with both modern CPUs and motherboards. My preference is to get a new PC up and running with all the essential software installed, and keep the old PC operating until you are comfortable with the new one and are sure that it has all the applications you need and that all your data has been successfully transferred to it.

Editor's Comment: Windows XP status on April 8, 2014

By Joe Durham, co-editor

As Larry Stone, our Windows SIG leader, observed at our last meeting,this closing of support for XP doesn't necessarily mean you have to change things. If you don't use the Internet on your XP machine and your programs and peripheral interfaces work fine, this transition is a non-issue. You can remain where you are.

If you do use the Internet, as the previous article mentioned always update your anti-virus software. Larry suggested that you use a browser that will continue to be updated in the XP domain such as Firefox or Google Chrome.

As with any computer, Larry Stone and Jim Kristan have always emphasized that you should back up your computer. Preferably in this case make an image of your hard drive as this will allow you to restore Windows XP back to square one if necessary. There are several programs that do this easily. Send Larry (**lstone521@mchsi.com**) or Jim (**jmkris@gmail.com**) an email and they will direct you.

Finally in my case I offer a different Linux solution than the previous article. I use Puppylinux Lupu 5.28. I have used Linux since 2005. If

--continued on next page--

you have Word documents, photos, music, these are all accessible from Puppylinux.

I use LibreOffice to do word processing, and spreadsheet work. It is Microsoft Compatible, even with the docx formats. Gimp is the Linux equivalent of Photoshop. And there are many audio players in Linux. Puppylinux has a firewall and Linux is impervious to virus attacks. It will support the older hardware you use in Windows XP as well. And as Jim Kristan has pointed out this software is free.

All it requires is that you burn the downloaded Puppylinux iso file to a CD. Place it in your CD and boot. You can download l**upu-528.005.iso** from my Dropbox directory **goo.gl/a5Nv5Y** along with a free Windows CD burner program **burncdcc.exe** in my Dropbox folder to accomplish this goal. If you have any questions email me and I will be glad to help or send you a burned CD. joseph85_us@yahoo.com

---

Get Plain Text

By Linda Gonse, Editor & Webmaster, Orange County PC Users' Group, CA
October 2013 issue, *Nibbles & Bits*
www.orcopug.org
editor (at) orcopug.org

It's probably safe to say that everyone has copied text from a webpage at some time and pasted it into an email or into a Word-like program. So, of course, you can relate to my dismay of pasting the type complete with its formatting riding piggyback on it.

I always have to stop what I'm doing and unformat and reformat the type, so it blends in with what I'm working on.

I can hear "old timers" yelling, "Notepad! Use Notepad!"

That's true. And, it's a good option. I'm using Windows XP (still), so I have a shortcut to Notepad on my Start menu. It's very easy to click on Start while I have my browser open and click to open Notepad to paste the web text, then recopy it from Notepad, and repaste the text into a document.

But, I found a simpler method.

Really. There is no learning curve.

I only have to click once after copying from a webpage and then I can immediately paste unformatted text into anything anywhere!

With our typical complicated programs to work with, this just doesn't seem possible. Or, maybe alchemy might be involved!

The short of it is that this is true, no hocus pocus. It is possible with a tiny program called Get Plain Text.

It's only 70Kb and it doesn't add an icon to your system tray or grab any memory when you use it.

It works in less than a second to remove text formatting, including fonts, sizes, colors, and embedded images. It just leaves plain text.

Download the program from the developer's webpage (**clipdiary.com**) at **bit.ly/1bzFuea** or a secondary download site at **www.softpedia.com/get/PORTABLE-SOFTWARE/Office/Clipboard/Portable-Get-Plain-Text.shtml**. Save it to your preferred disk location. Click on the program to run it.

Add the icon that launches Get Plain Text to your Quick Launch bar or favorite program launcher.

I keep it on my Quick Launch bar. As soon as I copy something to the clipboard, I click on the Get Plain Text icon. Then, I paste the text anywhere I desire. That's it.

When I use Get Plain Text, no window opens. There are no dialog boxes or preferences to select. There are no flags, bells, or whistles to tell me it is finished. It simply works fast, silently, and unobtrusively.

What else? Oh, yeah. It's free!

CryptoLocker: The Worst Malware/ Ransomware Ever?

This is malware that when it infects a computer, it starts encrypting every document, spreadsheet, PowerPoint, graphic and photo file it can find. Once everything is encrypted, the malware posts a ransom notice demanding money. Jim Evans and APCUG member group, the Greater Cleveland PC Users Group has created a special CryptoLocker page at http://gcpcug.org/CryptoLocker and updates it regularly with articles, software, tips and video links.

Share this information and link with every computer user you know. By paying the ransom, the cyber criminals are only encouraged to continue.

What I Would Change If I Were In Charge

By Jim Cerny, Director, Sarasota PC Users Group, FL
July 2013 issue, PC Monitor
www.spcug.org

jimcerny123 (at) gmail.com

Yes I am a big fan of technology. I enjoy it. To me, my computer devices (including my tablet and phone) and the things they can do for me are totally amazing. Computers are also very complex.

I believe the day has long past when one person can know everything about them. I certainly am not any-where close to that.

But having used computers for a number of years, I am still totally amazed at some of the design decisions that are made about these devices and the software (programs, apps) they use.

Do the designers sit around a table and say "Ok, let's do it that way, the users will figure it out."?

Does there ever seem a real reason why they do the things they do?

Do they ever trial their designs with real people like us?

Top Ten Change List

I don't mean to be rude -- maybe just a bit amusing. Here is my "top ten" list of the things I would change if I were in charge:

10. Computer buttons on a device would be a different color from the rest of the device.

I would like to be able to clearly see the buttons or switches, especially as the devices get smaller and smaller.

9. When I move or copy a file from one place to another, I would have a pop-up box appear that says "You have successfully moved (or copied) file X to folder Y."

That way I could catch a mistake if I dropped it into the wrong folder. If other users are so confident that they would never move something to the wrong place, they could turn off this feature.

8. When updating software, I would keep the most-used commands in the same place in the window.

For example, when updating an email program, I would not move the "write" command box from one side of the screen to the other, nor change its color from blue to red, nor change the word "write" to "compose" or "create."

7. I would have the "help" searches recognize the words most users would enter in the "help" search, not just the words the program designers decided to acknowledge.

Maybe the software uses the term "font color", but some people may search help for "letter color" or "text color.

6. Finding seldom used commands or options should be easier to find and not removed out of sight be-cause I haven't used them lately.

5. All companies that take my money should have a live person whom I can talk to on the phone in a reasonable time.

4. Companies which use an automatic answering system (a computer voice that answers the phone and asks you questions, also known as a "phone robot") MUST make their own management employees call their own number and go through the same "telephone tree" that their customers go through.

And they should all do it at least once every three months because they must "please listen carefully as our options have changed!"

3. If I give an answer to a telephone answering robot, I should not have to answer the same question again from a real person who finally gets on the line to help me.

2. *When writing a new version of software, I would initially make it look like the old version and grad*ually help the user transition and learn as they use the new version.

And now (drum roll please) my number 1 thing I would change:

1. Company employees who finally help me on the phone should be knowledgeable of their own company's web page and the information on it!

Yes, believe it or not, you can constantly negotiate totally different deals and prices in person, on the phone, and on the Internet – all with the same company.

Conclusion

Well, I guess no world is perfect. And I am sure you have your "top ten" list too. If any of you get a call from a company asking for your opinion on any of these things, please let me know.

For some reason no one calls and asks me. Maybe it's because of my "telephone tree" answering message they have to listen to first.

Nibblers

By Jeannine Sloan, Member, Twin Cities PC Users' Group, Minnesota
October 2013 issue, The Digital Viking
www.tcpc.com
sqwalbran (at) yahoo.com

Skydrive & Google Drive both perform OCR on photos of narrative. Google Drive can convert PDF to text.

--continued on next page--

A More Secure Web Browser
http://www.guidryconsulting.com/techtips/2013/09/how-to-secure-your-web-browser/

---

10 Free Learning Websites for Kids

Here's a list of some fun,educational, and safe websites for your child or grandchild to visit and explore.

SWITCHEROO ZOO
www.switcheroozoo.com
Watch and play game to learn all about amazing animals.

NAT GEO FOR KIDS
www.kids.nationalgeographic.com
Learn all about geography and fascinating animals.

INTO THE BOOK
www,reading.ecb.org
Go "into the book" to play games that practice reading strategies.

SEUSSVILLE
www.seussville.com
Read, Play games and hang our with Dr. Seuss and his friends.

ABC YA
www.abcya.com
Practice math and reading skills all while playing fun games.

FUN BRAIN
www.funbrains.com
Play games while practicing math and reading skills.

PBS KIDS
www.pbskids.org
Hang out with your favorite characters all while learning.

STAR FALL
www.starfall.com
Practice your phonics skills with these read-along stories.

STORYLINE ONLINE
www.storylingonline.net
Have some of your favorite stories read to you by movie stars.

HIGHLIGHTS KIDS
www.highlightkids.com
Read, play games and conduct cool science experments.

Officers 2013-2014

Elected Officers

President	Judi McDowell	(309) 314-1780	julee89@gmail.com
Vice President	Ralph Drexler	(309) 755-8138	drexlerrm@mchsi.com
Secretary	Maggie Gillespie	(563) 332-5661	m.gillespie@mchsi.com
Corresponding Secretary	Shari Peterson	(563) 468-1658	skp4joy@gmail.com
Treasurer	Dave Tanner	(309) 764-6455	dl.tanner@mcshi.com
Directors at Large	Jim Buche	(309) 755-4893	jhbuche@mchsi.com
	Marie Drexler	(309) 755-8138	drexlerrm@mchsi.com
	Tina Gean	(309) 373-1122	tina2121@yahoo.com
	Melinda Missman	(309) 235-7579	mamissman@gmail.com
	Susan Peterson	(309) 721-7048	felspaw@gmail.com
	Emily Smith	(309) 794-9320	ginghis18@mchsi.com
	Diana Wolf	(309) 797-5413	
Director Past President	Patty Lowry	(563) 332-8679	pattylowry@rocketmail.com

Director/SIG Leader

Beginners	Jim Kristan	(309) 755-8277	jmkris@gmail.com
Genealogy	Len Stevens	(563) 359-9672	judylenstevens@msn.com
Digital (coordinator)	Vicki Wassenhove	(309) 787-2239	wazz123@gmail.com
Internet	Ted Huberts	(309) 792-9470	slowhand54@sbcglobal.net
Investment SIG	Darlene Norton	(309) 798-1085	darn54@gmail.com
Office	Judi McDowell	(309) 314-1780	julee89@gmail.com
QBits	Joe Durham	(309) 764-5570	joseph85_us@yahoo.com
Windows	Larry Stone	(309) 787-5574	lstone521@mchsi.com

Appointed Officers

Membership Director	Susan Peterson	(309) 721-7048	felspaw@gmail.com
Program Director	Ralph Drexler	(309) 755-8138	drexlerrm@mchsi.com
Public Relations Dir.	Melinda Missman	(309) 235-7579	mamissman@gmail.com
Publicity	Joe Durham	(309) 764-5570	joseph85_us@yahoo.com
Financial Committee	Mel VanderHoek	(563) 505-9661	vanderhoek@netexpress.net
APCUG Representative	Patty Lowry	(563) 332-8679	plowryapcug@gmail.com
Membership Records	Susan Peterson	(309) 721-7048	felspaw@gmail.com
Web Master	Vicki Wassenhove	(309) 787-2239	wazz123@gmail.com
QBITS Newsletter	Joe Durham	(309) 764-5570	joseph85_us@yahoo.com
	Patty Lowry	(563) 332-8679	pattylowry@rocketmail.com
Mailing	Patty Lowry	(563) 332-8679	pattylowry@rocketmail.com
Resource Manager	Judi McDowell	(309) 314-1780	julee89@gmail.com

MEMBERSHIP CORNER

Membership dues are payable **July 1st** each year and expire the following **June 30th**.

Individuals	$30
Family	$40

Payments can be made in person at a meeting or mailed to the treasurer

David Tanner
3449 – 52nd Street
Moline, IL 61265

SIG and Event Calendar

February 2014

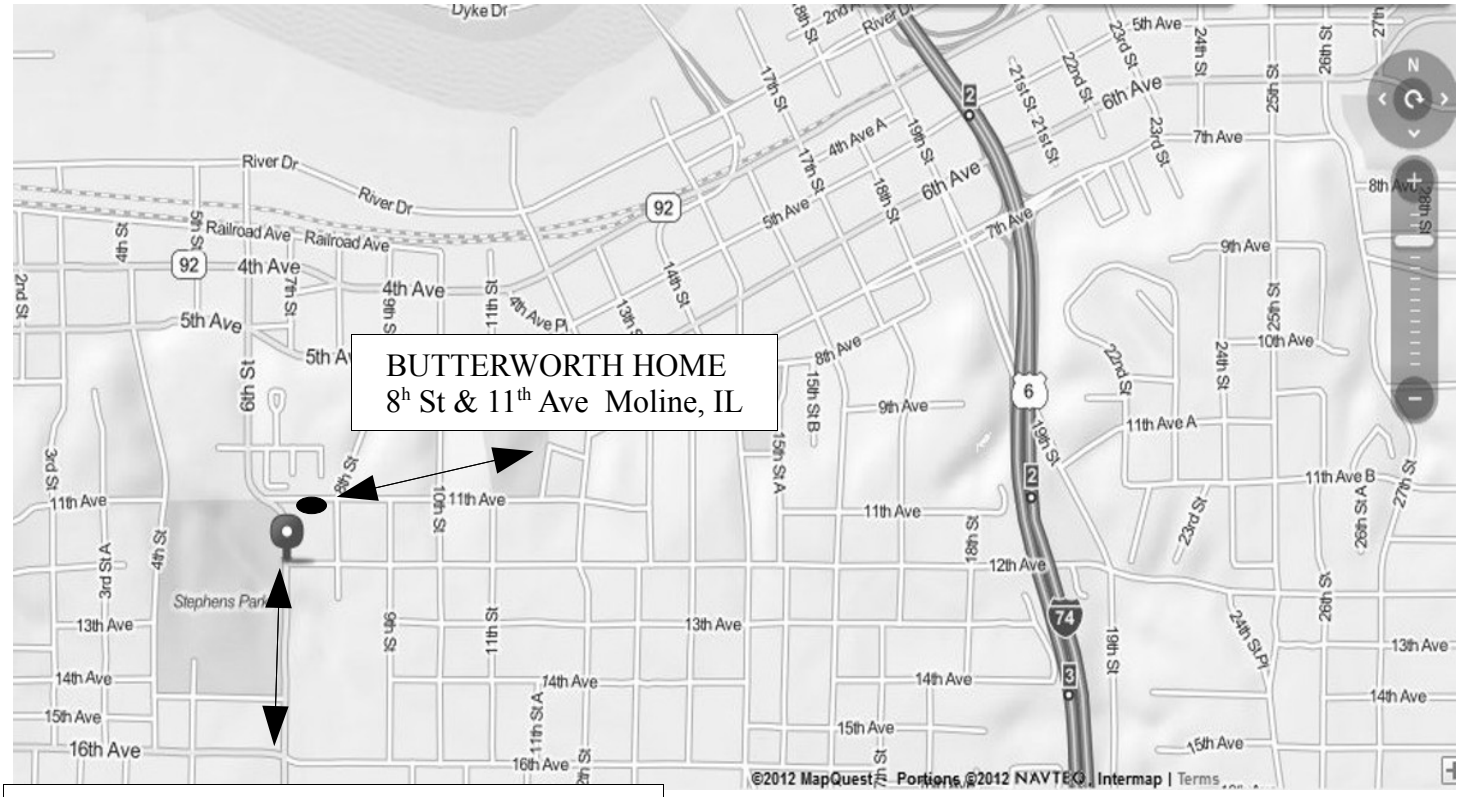
Feb 3th – Mon	5:30 PM	**Beginners SIG**	EDC	Jim Kristan	309-755-8277
	7:00 PM	**Pratical Concepts for Protecting Your Computer** presented by Larry Stone	EDC		
Feb 17th – Tue	5:30 PM	Genealogy SIG	EDC	Len Stevens	563-359-9672
	7:00 PM	Internet SIG	EDC	Ted Huberts	309-792-9470
Feb 24th – Mon		**NO** Digital Media SIG	EDC	Vicki Wassenhove	309-787-2239
	7:00 PM	Windows SIG	EDC	Larry Stone	309-787-5574

Location Key

BCL Library of Butterworth Home
CRA Craft Room of Butterworth Home
EDC Education Center of Butterworth

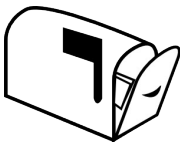
Location Key

MVC Moline Vikings Club
OAK Oak Room of Butterworth Home
ORC Orchid Room of Butterworth Home



EDUCATION CENTER OF BUTTERWORTH
7th St & 12th Ave Moline, IL

Quad Cities Computer Society
c/o Dave Tanner
3449 - 52nd St
Moline IL 61265



Moving? Send an address change to:
felspaw@sbcglobal.net

This Month in *QBITS* ....

Monday
February 3th
7:00 PM

"Practical Concepts for Protecting Your Computer: Its Hardware and Data"
presented by
Larry Stone

What I Would Change If I Were In Charge

By Jim Cerny, Director, Sarasota PC Users Group, FL July 2013 issue, PC Monitor
www.spcug.org jimcerny123 (at) gmail.com

Yes I am a big fan of technology. I enjoy it. To me, my computer devices (including my tablet and phone) and the things they can do for me are totally amazing. Computers are also very complex.

I believe the day has long past when one person can know everything about them. I certainly am not any-where close to that.

But having used computers for a number of years, I am still totally amazed at some of the design decisions that are made about these devices and the software (programs, apps) they use.

Do the designers sit around a table and say "Ok, let's do it that way, the users will figure it out."?

Does there ever seem a real reason why they do the things they do?

Do they ever trial their designs with real people like us?

Top Ten Change List

I don't mean to be rude -- maybe just a bit amusing. Here is my "top ten" list of the things I would change if I were in charge:

10. Computer buttons on a device would be a different color from the rest of the device.

I would like to be able to clearly see the buttons or switches, especially as the devices get smaller and smaller.

9. When I move or copy a file from one place to another, I would have a pop-up box appear that says "You have successfully moved (or copied) file X to folder Y."

That way I could catch a mistake if I dropped it into the wrong folder. If other users are so confident that they would never move something to the wrong place, they could turn off this feature.

8. When updating software, I would keep the most-used commands in the same place in the window.

For example, when updating an email program, I would not move the "write" command box from one side of the screen to the other, nor change its color from blue to red, nor change the word "write" to "compose" or "create."

7. I would have the "help" searches recognize the words most users would enter in the "help" search, not just the words the program designers decided to acknowledge.

Maybe the software uses the term "font color", but some people may search help for "letter color" or "text color.

6. Finding seldom used commands or options should be easier to find and not removed out of sight be-cause I haven't used them lately.

5. All companies that take my money should have a live person whom I can talk to on the phone in a reasonable time.

4. Companies which use an automatic answering system (a computer voice that answers the phone and asks you questions, also known as a "phone robot") MUST make their own management employees call their own number and go through the same "telephone tree" that their customers go through.

And they should all do it at least once every three months because they must "please listen carefully as our options have changed!"

3. If I give an answer to a telephone answering robot, I should not have to answer the same question again from a real person who finally gets on the line to help me.

2. *When writing a new version of software, I would initially make it look like the old version and grad*ually help the user transition and learn as they use the new version.

And now (drum roll please) my number 1 thing I would change:

1. Company employees who finally help me on the phone should be knowledgeable of their own company's web page and the information on it!

Yes, believe it or not, you can constantly negotiate totally different deals and prices in person, on the phone, and on the Internet – all with the same company.

Conclusion

Well, I guess no world is perfect. And I am sure you have your "top ten" list too. If any of you get a call from a company asking for your opinion on any of these things, please let me know.

For some reason no one calls and asks me. Maybe it's because of my "telephone tree" answering message they have to listen to first.

CryptoLocker: The Worst Malware / Ransomware Ever?

This is malware that when it infects a computer, it starts encrypting every document, spreadsheet, PowerPoint, graphic and photo file it can find. Once everything is encrypted, the malware posts a ransom notice demanding money. Jim Evans and APCUG member group, the Greater Cleveland PC Users Group has created a special CryptoLocker page at http://gcpcug.org/CryptoLocker and updates it regularly with articles, software, tips and video links.

Share this information and link with every computer user you know. By paying the ransom, the cyber criminals are only encouraged to continue.

Jim Evans, Greater Cleveland PCUG. User groups, are you educating your members about the CryptoLocker ransomware?

Well, 2013 is history and it's time to start thinking about collecting receipts and getting things in order for your income tax return. Of course it's a tendency for most of us to put this off till the last minute. You have to wonder what Warren Buffett's return looks like. I find it incomprehensible that Mr. Buffett made 37 million dollars a day last year. Yes, I said a day! The legendary billionaire and philanthropist finished 2013 with a net worth of $59.1 billion, up from $46.4 billion at the beginning of the year. Yes, the rich get richer! Get the low down from Market Watch. **goo.gl/lK8kyR**

Of course money doesn't create happiness. Most of us would love to win the lottery, but would we really? It's a fact that most lotto winners lost it all and are very unhappy people. Winning the lottery would create so much stress into our lives that it would be almost unbearable especially in those states that require your name to be released. Let me put in this paragraph what always appears at the bottom of the page in every Cyber News, and that's my motto. "Live with Passion, in a constant state of Joy, and with an Attitude of Gratitude"! Be grateful for what you have and your life will be happier!

Take a stroll down memory lane and look at events that influenced 2013. What was your biggest memory of last year? Was it the papal transition, the Zimmerman trial, the Royal baby birth, the Boston bombing, or maybe the Jodi Arias trial? Some of these events were negative, but perhaps you had a wonderful personal memory of the year. Yahoo has provided a site that will showcase highlights, and you could probably spend all day clicking on different stories! Take a look. **goo.gl/QeoeG5**

Curtain calls 2013: Remembering stars, old and young, who passed last year. Actress Bonnie Franklin, Annette Funicellow and comedian Jonathan Winters are just three. The story from NBC's Today. **goo.gl/pqrrJS**

Super Bowl 2014. Get ready everybody; this is going to be a Super Bowl of firsts. **goo.gl/GmYDus** Aside from being the first outdoor, cold weather Super Bowl, Super Bowl XLVIII is also the first to be hosted by two states. February 2nd is the big game and commercials on the Fox network have been sold out for some time. The rate? How about 4 million dollars for 30 seconds! Who bought the spots? Here's the scoop! **goo.gl/zsWur2**

Will Amazon and other companies be sending you Christmas presents via a drone next year? It's hard to imagine drones delivering packages. What kind of a mess will that make for our skies? But this is definitely in the planning stages. The story from Forbes. **goo.gl/Kb5iCu**

For years our computers came with a program called "Media Player." It would play all your music and videos, but what a lot of people didn't realize is it would also take you to the Internet for other options. You could listen to radio stations, preview movies, play games, and all kinds of fun stuff. With Windows 8 however, as with everything else, things changed and the button that took you to the Internet is no longer there. Kind of like the disappearing Start Button. After installing new computers for customers and being embarrassed as to where they were hiding this feature, I researched and found that now the fun is on a website. Check it out **goo.gl/SWtt7W** and bookmark it so you can go there often.

I should have put this site in Cyber News last month because it's a great place to find gadgets for your cell phone, along with other neat things. Would have been a good place to visit for Christmas gifts, but it's never too late for 2014. You'll have a blast checking out all the goodies! **goo.gl/O7j4ny**

Get a new computer or laptop for Christmas? If so, and if it's a PC, your operating system is Windows 8 and the best thing you can do to make your life not so frustrating is to install "Classic Shell." That's a third party Start button that will make you more at home with the new system and you can find it here. **goo.gl/Cxj5Yg**

Get a new iPad for Christmas? If you did, you must get the app "Flipboard." I sit on the couch every night, while watching TV, and flip through all my favorite news sources. It's the greatest app on my iPad and it's free! Also, here are some great tips **goo.gl/0syw8E** if you have an iPhone or an iPad!

Meet "Wisp," the wireless future of the Internet. The Internet connection we all rely on is about to change, now that WISP is coming to town. No more cable or telephone connections to get to the Internet. As if technology wasn't good enough today, tomorrow it's getting better! Read all about it from PC World. **goo.gl/C3j80q**

You undoubtedly heard about the theft of 40 million credit accounts from shopping at Target. If you

shopped there between November 27th and December 15th and used your credit card, you are at risk. The worst part of this scenario is that cards are being sold on the black market. Here's my take. If I were one of those persons I would cancel my card and have a new one issued. That is the only safe thing to do. Many stories have appeared on the Internet and here is one of them from CNET. **goo.gl/YvsGCV** Credit card hacks will continue happening because our credit card system in America is antiquated. That story from CNN.

Ever notice a spot on your body? If it looks a little out of the ordinary and doesn't want to go away, don't ignore this as it may be skin cancer. The first step is to find a good dermatologist and have it checked. If suspicious he or she may want to do a biopsy. Don't worry, this is not a big deal, cause I've recently gone through this. My spot was just below my left eye and was diagnosed as basal cell carcinoma and I went through a simple surgery to remove it. Read about it in my Blog. **goo.gl/eTNqFz**

I can remember television sets when they had black and white pictures and snowy at that! The TVs of today feature pictures that make you think you're in the scene. I recently saw an 80 inch model in a store that took my breath away. Now LG and Samsung have announced a 105 inch ultra HD TV. Wow! Details from NBC. **goo.gl/3nDDrO**

A lot of Internet sites require you to log-in with a user name and password. This is especially important when using banking sites, but the question is do you log-off when finished? Not doing so leaves your account open and that's not good. Here's a further explanation. **goo.gl/Ho906E** Remember also never to use the same password for all accounts. If a hacker guesses one, he has them all!

Imagine the year 2020: Augmented reality glasses like Google Glass are everywhere. Cars are connected and, in some cases, driverless. Your smart phone is less a phone than a command center uniting the various nodes of your technological self — watch, glasses, wallet and car alike. But what about your personal camera? What will it look like in 2020? The story from USA Today. **goo.gl/y8YyXp**

The year 2020 is a few years away, but 2014 is here now and so let's imagine what it will be like. Albert Einstein was quoted as saying "Imagination is everything. It is the preview of life's coming attractions." So let's imagine a Happy 2014!

Do Not Fall Prey to the Vicious CryptoLocker Extortion

by Ira Wilsker

WEBSITES:

http://www.dhs.gov/national-cyber-securityawareness-month
http://www.fbi.gov/news/news_blog/nationalcyber-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-learnabout-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 email 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 email 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 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 email 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 emails, and I will admit that they do look like they are from a legitimate source, but I know not to open email 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. Crypto-

Locker 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 email 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 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 email 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 Cyber Security Awareness Month, such as “don’t click on and open email 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.

HOW DO I ENSURE THERE'S NO "NEXT TIME?"

Here are five "top tips" for keeping safe against malware in general, and cyberblackmailers in particular:

- **Keep regular backups of your important files**. If you can, store your backups offline, for example in a safe-deposit box, where they can't be affected in the event of an attack on your active files. Your backups will be rendered useless if they are scrambled by CryptoLocker along with the primary copies of the files.
- **Use an anti-virus, and keep it up to date.** As far as we can see, many of the current victims of CryptoLocker were already infected with malware that they could have removed some time ago, thus preventing not only the CryptoLocker attack, but also any of the damage done by that earlier malware.
- **Keep your operating system and software up to date with patches.** This lessens the chance of malware sneaking onto your computer unnoticed through security holes. The CryptoLocker authors didn't need to use fancy intrusion techniques in their malware because they used other malware, that had already broken in, to open the door for them.
- **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.
- **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.