CAEUG Computers Are Easy User Group

Abort, Retry, Ignore....

Founded 1984 **ARI** is the Official Newsletter of **C**omputers **A**re **E**asy **U**ser **G**roup

October 2012
Volume XXIX Issue 10

Confirmed meeting dates for 2012
Room A

October 27
4th Saturday

Check www.caeug.net for Nov/Dec meeting date

MEETING PLACE will be the Glenside Public Library
** **
*** ***
Visitors Welcome

HOPE TO SEE YOU THERE!!

Our October 27th 2012 (4th Saturday) Presentation:

Frank Braman will give a presentation on
how to scan and merge documents using Office Suite
(address and print envelopes, if time allows)

October is National Cyber Security Awareness Month

by Ira Wilsker

1Ira is a member of the Golden Triangle PC Club, an Assoc. Professor at Lamar Institute of Technology, and hosts a weekly radio talk show on computer topics on KLVI News Talk AM560. He also writes a weekly technology column for the Examiner newspaper <www.theexaminer.com>. Ira is also a deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime and security.

WEBSITES:
http://www.dhs.gov/national-cyber-security-awareness-month
http://staysafeonline.org/ncsam
http://staysafeonline.org/ncec/ (Educational information K-12 and College)
http://msisac.cisecurity.org
http://www.stopthinkconnect.org
http://www.prnewswire.com/news-releases/new-national-cyber-security-awareness-month-web-portal-offers-wealth-of-resources-to-stay-safe-online-169306026.html
http://staysafeonline.org/ncsam/events
https://www.facebook.com/staysafeonline
http://www.prweb.com/releases/cybersecuritytraining/cybersecurityconference/prweb9920629.htm
http://www.microsoft.com/security/resources/cybersecurity.aspx

Con't pg 2

Table of Contents

October is National Cyber Security Awareness Month	by Ira Wilsker	1
Lamp Post 142 by John Spizzirri		5
A Clean up / Speed up Story by Larry Bothe		7
October DVD of the Month List		9
Social Networks StaySafeOnline.org		9

Regular readers of this column are well aware that one of the most frequent topics covered is cyber security. Most computer users are blissfully unaware of the degree of cyber crime that is currently taking place, and the current threats to our computing safety. Virtually all computing devices are at substantial risk, regardless of operating system; Mac computers have recently become the targets of a large number of types of malware; Android devices, smart phones and tablets, are now being attacked at alarming rates; iOS devices (iPhones and Apple tablets) are likewise falling prey to malware attacks; Windows powered devices continue to be widely targeted due to the prominence of Microsoft operating systems (XP, Vista, Windows 7, and now Windows 8). According to Troels Oerting, the new chief of the European Union's (EU) European Cybercrime Centre (as quoted on EUobserver.com, September 17, 2012), " There is no absolute security, it is a myth." Oerting went on to describe, " ... that more than 200 billion spam emails are being sent every day and that 46 new malicious codes aimed to steal online data are being created every second. Foreign intelligence services are among the long list of culprits who increasingly use the Internet to steal data to gain inside advantages on trade. Activists, hackers and organised crime are also becoming more active."

Cyber security is a concern and a necessity at all levels. While computers and networks operated by governments, businesses, academia, and other associations and agencies have been prime targets of cyber attack, the number and rate of attacks on privately owned personal computers and smart devices has become explosively endemic. While cyber security and safety is a responsibility of all computer and smart device users, the federal government along with a variety of private and public partners has promoted "National Cyber Security Awareness Month" (NCSAM) for many years. Traditionally, the President of the United States had inaugurated NCSAM with a presidential declaration calling on everyone to be aware of cyber security, and to take all appropriate precautions to secure their digital devices from attack. During October, 2012, there will again be a national effort to encourage and promote cyber security.

This year, the lead federal agency promoting Cyber Security Awareness Month will be the Department of Homeland Security (DHS), which will be coordinating events and activities with the National Cyber Security Alliance (NCSA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). According to the DHS, this joint operation, " ... encourages Americans to ACT – Achieve Cybersecurity Together – reflecting the interconnectedness of the modern world and the responsibility each of us in securing cyberspace."

One may ask himself, "So what can I really do to help the cyber security effort?" The various agencies working together have come up with a list of actions and activities all computer and smart device users should implement. One of several behaviors encouraged by the alliance is to "STOP, THINK, CONNECT" (**stopthinkconnect.org**). According to the alliance, all users should: "STOP: Before you use the Internet, take time to understand the risks and learn how to spot potential problems. THINK: Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's. CONNECT: Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer. Protect yourself and help keep the web a safer place for everyone."

There are several definitive steps that users can take to implement and improve the security of their digital devices. According to a Microsoft webpage devoted to the
National Cyber Security Awareness Month (**www.microsoft.com/security/resources/cybersecurity.aspx**), there are six major practices that we should all accomplish in order to improve our cyber safety and security. Microsoft's first recommendation is to defend your computer by strengthening your computer's defenses, and not to be tricked into downloading malicious software. While these first recommendations may seem to be common sense for most computer users, these recommendations are also some of the least implemented. In order to defend our computers and other devices from attack, we need to keep all software (especially web

Con't pg 3

browsers) up to date; install legitimate and comprehensive security software and keep it current with the latest updates (most security publishers now push hourly or continuous updates); use and never turn off the firewall; be sure to have a hard to guess password on your router (and my urging to implement the highest level of encryption available on your wireless access point or device); and to use USB and other flash memory devices cautiously, as they have become a major vector for passing malware between computers and other devices. Microsoft also warns, "Think before you open attachments or click links in an email message, an instant message (IM), or on a social network, even if you know the sender." Much of the spam and malware being disseminated appears to come from someone we know, as their computers, instant messaging account, address books, or email accounts have been hijacked, and used to spread malware and spam to others, under the guise that it is OK because it is from someone you know. Another component of this second recommendation is to never click on links or buttons that appear in pop-up windows.

Identity theft and related financial crimes has become a huge source of revenue for cyber crooks the world over, and Microsoft covers this in its second recommendation, "Protect Sensitive Information." Microsoft warns users that before they enter any sensitive data on a website or online form, look for indications that the webpage is secure, such as the web address beginning with "https" rather than "http", and some indication from the browser that the connection is secure. Most browsers use a padlock (clearly open or closed) or some similar indication of a secure connection. Another common trick to steal personal information, such as usernames, passwords, banking and credit card information, and other personal information is commonly referred to as "Phishing", where identity thieves attempt to trick the user into disclosing personal information. Much of this phishing is by way of emails informing the user that their email account will be locked unless they respond with their username and password; apparently legimate (but false) contacts from retailers, credit card companies, banks and other institutions asking for personal credit card or bank account information; offers of riches in exchange for helping some foreign official or widow to place investments in this country; foreign lottery winnings; and a variety of other scams. One of the latest common scams is known as "ransomware", where the user's computer is locked, and a warning from the FBI or other law enforcement agency appears on the screen informing the user that unless he pays a "fine", typically $200, his computer will remain locked, and he will be prosecuted for several felonies, including possessing child pornography.

Similar requests for personal information that can be abused often arrives in instant messages or social networking postings. Another common email scam is a post apparently from a friend or relative that claims they lost their wallet, checkbook, passport, return airline tickets, and credit cards while visiting a foreign country, and are stranded unable to return home. This recognizable friend or relative then asks you to make him a loan and wire a large sum of money to him such that he can get home; of course, "I will pay you back as soon as I get home." The problem is that this is a complete fraud, and that friend or relative overseas is a name stolen from a hijacked email account or address book! Also be aware of phone calls claiming to be from Microsoft (or a recognizable computer security company) telling you that your computer is infected with a virus, and that either for free or for a fee charged to your credit card, they will remotely access your computer and clean it for you, "so please give us remote access to your computer". Not just will they not clean your computer of malware, but they will likely plant malware on your computer as well as access and steal all of your personal data and information on your machine.

Third on Microsoft's list of recommendations is to create strong passwords, and keep them secret. Passwords should be complex long phrases, consisting of upper case (capital) and lower case letters, along with numbers and symbols. These passwords should not be easy for other to guess like permutations of your name, address, phone number, kids names and birthdays; pets' names; and other information that can be easily

Con't Page 4

obtained through public or online resources. It is also necessary to utilize different passwords on different websites, such that if one website is compromised, it will not adversely impact your passwords and accounts on other websites. Microsoft emphasizes that it is especially important to use different complex passwords on websites that contain your financial information, such as banking, credit card, and shopping websites.

Number four from Microsoft is "Take charge of your online safety and reputation. Discover what is on the Internet about you and periodically evaluate what you find." What others say about you online in social networking services, blogs, and even eBay user ratings can adversely impact your online reputation. It is important to both maintain a positive online reputation, and correct erroneous postings about you, but be careful not to fall into someone's trap and disclose too much personal information.

In its fifth security recommendation, Microsoft urges that users exercise care when using social networks, such as Facebook and Twitter. All of the legitimate social networking services offer "settings" or "options" where users can set and manage their privacy and security settings. Users should control who can access their private information, what private information is available, and how others can search for your information. It may often be very appropriate to block other people from viewing your information. In addition to Microsoft's suggestions, I would also add do not post information that you are out of town, on vacation, or even at a movie or at dinner, as burglars and other literal crooks read Facebook and Twitter looking for empty homes to burglarize. Turn off the GPS in your digital camera or Smartphone before taking pictures that you want to post on a social networking site, such as Facebook, or otherwise strip off the GPS information, as crooks and pedophiles have been well known to use the GPS information encoded in digital photographs posted online to locate homes, cars, valuables, and children for the purposes of victimization. An old cliché' says "Don't do anything that you would not want your grandmother to read in the newspaper," and that applies to social media postings as well.

Number six from Microsoft says, "Take extra steps to help keep kids safer online." Online safety and security must be a family effort, and incorporate some mix of guidance and monitoring. Microsoft suggests that, "(Parents) negotiate clear guidelines for web and online game use that fit your kids' maturity and your family's values. Pay attention to what kids do and who they meet online." Pedophiles and identity thieves troll chat rooms, social networking websites, blogs, and other online resources looking for potential victims. Parents and children need to be cognizant of the risks and educated in what to watch for that may indicate potential risks to children. Children must never disclose personal information to anyone, especially others who claim to be the same age and gender as the child (pedophiles often pretend to be a child in order to gain the confidence of the potential victim). Identity thieves try to gain the trust of children and trick them into disclosing private family information; residential burglars will do the same, asking the child about vacation or dinner plans; "We are going out for pizza and then a movie" tells the burglar that the house may be a good target. Children should never go to meet someone face to face that they met online, unless under the direct supervision and participation of a parent.

There are a number of National Cyber Security Awareness Month events posted online (staysafeonline.org/ncsam/events), several of which will be streamed free over the internet. There are also free materials available for parents, teachers, children, and businesses that can be used in a variety of environments for educating others (staysafeonline.org/ncsam). While October is officially National Cyber Security Awareness Month, every month should be a NCSAM. Stop, think, and connect properly, and stay safe online.

Lamp Post 142
October 2012
by John Spizzirri

I recently got an old PC from a client. The PC is a Compaq **(1)** Evo Desktop **(2)** model D510 computer it came with Windows 2000 . It has a Pentium 4 processor and had 256MB RAM. The last Evo was shipped in 2003 which makes this PC at least 9 years old. The Windows 2000 ran well, but many newer programs require Windows XP or newer to operate thus limiting the usefulness of this PC. Getting a valid copy of Windows XP is becoming difficult as well as costly **(3)**. This machine can run Windows XP but it would need at least 1GB RAM for acceptable performance. I added an additional stick of 256MB RAM bringing the machine to 512MB RAM. I blew away the Windows 2000 and replaced it with Peppermint Linux **(4)**. I selected Peppermint because it is lightweight **(5)**, yet easy to use. Some lightweight distributions like Lubuntu **(6)**, Puppy Linux **(7)**, and DSL **(8)** require tweaking by a knowledgable user. Peppermint works right away without tweaking. It took about 45 minutes to install. It has a fast boot time (about 90 seconds including the password entry). Peppermint is built to use Internet applications, but can use locally loaded applications. Peppermint uses very little drive space (about 512MB to 1 GB). I installed some of the more popular software titles that handle audio, video, CD burning, Internet, and office tasks. Each took about two minutes, except Libre Office **(9)** which took 10 minutes. The total installation used three megabytes of hard drive. The problems with the machine are few. It has two ethernet connections. This causes a little confusion because I loaded a network activity application. It shows both connectors and indicates (correctly) that one is not connected. It has four USB connectors, one of which is dead. It has only a CD player - no writer. Because it has only 512MB RAM, only two applications can be run at the same time. If more are run simultaneously, the CPU **(10)** will sometime peg at 100% causing all apps to pause until CPU time is available.

1) **http://www.hp.com/**
2) **https://en.wikipedia.org/wiki/Compaq_Evo**
3) **https://www.buycheapsoftware.com/search_text.asp**
4) **http://peppermintos.com/**
5) **https://en.wikipedia.org/wiki/Lightweight_Linux_distribution**
6) **http://lubuntu.net/**
7) **http://puppylinux.org/**
8) **http://www.damnsmalllinux.org/**
9) **https://www.libreoffice.org/**
10) **https://en.wikipedia.org/wiki/Central_processing_unit**

While searching for some information about Internet Relay Chat (IRC **(1)**), I came across a web site that has instructions on various computer and non-computer related subjects. It is called Instructables **(2)**. The front page has articles ranging from knot tying to cocktail mixing to worm farming to Raspberry Pi **(3)** projects.

1) **https://en.wikipedia.org/wiki/Internet_Relay_Chat**
2) **http://www.instructables.com/**
3) **http://www.raspberrypi.org/**

The Ohio Linux Fest **(1)** was held at the end of September. Here is an overview of the topics covered

Con't pg 6

with short descriptions **(2)**. This may pique your interest to go to a large Linux fest like the Northeast Linux Fest **(3)** that will be held at Harvard University next March 16th and 17th.

1) **http://ohiolinux.org/**
2) **http://ohiolinux.org/talks**
3) **http://northeastlinuxfest.org/**

October is National Cyber Security Awareness Month **(1)**. You may want to scan your Windows PC with Panda's free online scan **(2)**. Trend Micro also has a scan, but it requires that you download a small program to complete the scan **(3)**. Downloadable Microsoft (MS **(4)**) scanners are available **(5,6,7)**. Some advice on passwords can be found here **(8)**.

1) **http://www.staysafeonline.org/ncsam**
2) **http://www.pandasecurity.com/activescan/index/**
3) **http://housecall.trendmicro.com/**
4) **http://www.microsoft.com/**
5) **http://www.microsoft.com/security/scanner/en-us/default.aspx**
6) **http://www.microsoft.com/security/pc-security/malware-removal.aspx**
7) **http://windows.microsoft.com/en-US/windows/products/security-essentials**
8) **http://cybergeddon.yahoo.com/?blogid=182dbd7e-2318-3fa1-b6f3-e8525f5e0346#access**

The Register had an article this month that I found hard to believe. The article **(1)** reported that MS is offering a product that competes with JavaScript **(2)**. The part that I could not believe was that this MS product is supposedly open source!

1) **http://www.theregister.co.uk/2012/10/02/microsoft_releases_typescript/**
2) **https://en.wikipedia.org/wiki/JavaScript**

Smart Computing Magazine **(1)** is available for free at Staples. It can be read on line for free. You may also subscribe to the print edition for $29 per year. Read the July 2012 edition **(2)**, August 2012 **(3)**. and September 2012 **(4)**, October 2012 **(5)** editions.

1) **http://www.smartcomputing.com/**
2) **http://www.smartcomputing.com/digitalissues/smartcomputing/SC____2307__/**
3) **http://www.smartcomputing.com/digitalissues/smartcomputing/SC____2308__/**
4) **http://www.smartcomputing.com/DigitalReader/Default.aspx?IssueName=SC____2309__#1**
5) **http://www.smartcomputing.com/DigitalReader/Default.aspx?IssueName=SC____2310__#1**

Paul Allen, one of the founder of MS, seems to like Windows 8 and hypes it on his web site **(1)**. He is also selling his new book (like he needs more money).

1) **http://www.paulallen.com/TemplateGeneric.aspx?contentId=21**

There is a new search engine **(1)** that searches specifically .xxx sites. .xxx sites are reserved for sites providing sexually explicit content, such as pornography **(2)**. This top level domain makes it easy to

Con't pg 7

use parental control software to eliminate those sites from your computer. The search site has no explicit material on it until a search is done.

1) **http://search.xxx**
2) **https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains**

A free audioBook is available at Porctherapy **(1)**. A pdf version of the book is also available **(2)**. Amazon has a paper version of the book **(3)**. This book is less than one year old.

1) **http://www.porctherapy.com/audiobooks/mnc/**
2) **http://radgeek.com/gt/2011/10/Markets-Not-Capitalism-2011-Chartier-and-Johnson.pdf**
3) **http://cl.lk/25cyf81**

We will be returning to Standard Time **(1)** on November 4th this year **(2)**. This skeptical web site **(3)** sees no reason for this and does not think we should turn our clocks back or forward.

1) **https://en.wikipedia.org/wiki/Standard_time**
2) **http://geography.about.com/cs/daylightsavings/a/dst.htm**
3) **http://www.standardtime.com/**

Between you, me and the LampPost, that's all for now.

A Clean up / Speed up story

by Larry Bothe

A friend stopped me at the airport a couple days ago. He told me his desktop computer (a compact Dell running Vista Home Basic) had gotten very slow, and asked if I would work on it. I went by his house yesterday to have a look. I started by doing a little benchmark timing. Boot-up took 1:55, and getting into Control Panel with all the icons up took 1 minute even. Then I went to work.

The good news is that there wasn't a lot of junk, like toolbars, running on the machine. I always go after toolbars first, and remove them all. I took off only one program, some 3rd-party Smart Vista Tweaker. Then I looked in MSconfig to see what was starting up that wasn't necessary. Since I had worked on this machine in the past I had already been through that area; nothing more to be gained. I then looked in the Start-Up folder in All Programs and found Windows Live Mail (WLM) and Skype. The owner wanted Skype to start because he uses it a lot. OK for Skype.

It turned out that WLM was the principal culprit. I had put it on his machine over a year ago to handle his email, which he got using the phone company as his ISP, running over a DSL line. The problem was that he had recently changed how he got his mail. He got rid of his wired phone line altogether and instead now gets his mail using a mobile hotspot device for his Internet signal with a little USB receiver attached to the computer. His daughter set it up for him, creating a gmail account and accessing it through Chrome. The mail is web-based. The rub came in that the daughter didn't take WLM out of startup. So WLM was starting and hunting around for an Internet connection (he doesn't always have his hotspot turned on) and for mail from Frontier (the fired phone company), neither of which are available. To explain to the owner what was wrong I likened it to a dog running around in the back yard looking for a bone it couldn't remember where it was buried, thus using up lots of energy and getting nothing accomplished. I simply took WLM out of Start-Up, and that mostly cured the problem. (I know that WLM can be configured to pull gmail, but I chose not to go there, at least for now.)

Con't pg 8

After making the changes listed above I did a regular clean-up. I ran Disk Clean-Up and got rid of old restore points. Next I ran CCleaner to get rid of needless files and clean the registry. Then I put the Auslogics defragmenter on his machine and ran it in Optimize mode. That ran through in about 10 minutes. I'm impressed! I finished by cleaning up his desktop; removing unused icons and moving the remaining ones around to make them easier to to see with respect to his wallpaper picture (a Stearman biplane). I also noted that the little tray icon for Microsoft Security Essentials was amber. Upon opening the program I discovered that it had not scanned for a long time. I ran a Quick Scan to cure that and then looked at the scan schedule. Sure enough, it was on the default, 2 AM on Sundays, a time the computer is never turned on. After consulting with the owner I changed that to 8 PM Wednesdays, a more likely time.

When it was all done I did a cold shutdown and then started it back up. The boot time is now 58 seconds, about half what it was before. I tried Control Panel. It was fully up in 12 seconds, 1/5 the previous time. I called it a success. The owner is pleased. I charged him the "friend price" for my services; 2 beers.

One final note: I looked in System and learned that the machine has only 1 gig of RAM, and at idle it uses about 65% of that. I told the owner that doubling the RAM would markedly increase the overall speed. I didn't open the case to see the RAM configuration, but my guess is that there are probably 2 memory slots with 2 pieces of 512 megs, so in reality to get to 2 gigs he would have to buy 2 1-gig pieces for about 60 bucks. He's thinking about it.

The real lesson here is that when you add new hardware and/or procedures to a computer it is necessary to remove the old ones if you don't want the machine to get bogged down. My friend's daughter didn't do that.

Larry Bothe, FAA Designated Pilot Examiner
Sport - Private - IFR; vintage & taildraggers

Larry asked me about this PC via e-mail. Here is my kibitz.
by John Spizzirri

I would like to make a few suggestions. First, on the opening screen of cCleaner is a thumbnail of the the machine under the cCleaner name logo.

Second, MSconfig is clunky. It does not let you see the whole path for each item in startup without a good deal of difficulty. cCleaner to the rescue. Run cCleaner. Click on the tools icon. Click on the startup button. If cCleaner is full screen, you can see the items with the full path. On the right are 3 buttons; Enable, Disable, and Remove. Goto the free software page on my web site under Disk Cleaning for a link to cCleaner.

Third, Speccy can give you the number of memory slots in a machine, which ones are filled, and what they are filled with. It also give you the model number of the mother board (mobo) for an easy Internet lookup of the maximum amount of memory the mobo can take. Goto the free software page on my web site under System information tools for a link to Speccy.

October 2012
DVD of the Month

AdvancedRenamer - Renaming multiple files and folders at once
ARI - October newsletter
Autostreamer - A way to create a single bootable installation CD that will install the base OS with the latest service pack
cCleaner - Updated Hard drive cleaner
CD/DVDOMlists - Lists of past CD/DVDOMs
D7 - A fully portable tool for PC technicians
DiskInvestigator - Discover all that is hidden on your computers hard disk
DriverBackup - Fast and user-friendly free tool for driver backup, restoration and removal
DuplicateCleaner - Finds and deletes duplicate files
Feedreader - News aggregation solution
FormatFactory - Multi-functional media converter
GingerGrammer - Grammar and spell checker
Grammar-multi - Grammar checker for English, Lithuanian, & Russian
Hotspotshield - Access all of your favorite content privately
McGuffeyReadingProgram - The reader has been revamped for the modern era
MemberContributions - Things e-mailed to me from members
OldTimeRadio - Old time radio broadcasts
ProcessExplorer - Shows which handles and DLLs processes have opened or loaded
SumatraPDF - A free PDF & eBook reader
Sysinternals - Suite of tools for trouble shooting PC troubles
TweakUI - Win XP PowerToy that changes the default user interface
UbuntuOne4Windows - 5 GB of Storage - File sync across platforms - share files
WebFerret - Fast search utility
YoutubeDownloaderHD - Ffree tool to download videos from YouTube

---

Social Networks
StaySafeOnline.org

Facebook, Twitter, Google+, YouTube, Pinterest, LinkedIn and other social networks have become an integral part of online lives. Social networks are a great way to stay connected with others, but you should be wary about how much personal information you post.

Have your family follow these tips to safely enjoy social networking:
Privacy and security settings exist for a reason: Learn about and use the privacy and security settings on social networks. They are there to help you control who sees what you post and manage your online experience in a positive way.
Once posted, always posted: Protect your reputation on social networks. What you post online stays online. Think twice before posting pictures you wouldn't want your parents or future employers to see. Recent research (**http://www.microsoft.com/privacy/dpd/research.aspx**) found that 70% of job recruiters rejected candidates based on information they found online.
Your online reputation can be a good thing: Recent research **(http://www.microsoft.com/privacy/dpd/research.aspx)** also found that recruiters respond to a strong, positive personal brand online. So show your smarts, thoughtfulness, and mastery of the environment.

Con't pg 10

Keep personal info personal: Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data, or commit other crimes such as stalking.
Know and manage your friends: Social networks can be used for a variety of purposes. Some of the fun is creating a large pool of friends from many aspects of your life. That doesn't mean all friends are created equal. Use tools to manage the information you share with friends in different groups or even have multiple online pages. If you're trying to create a public persona as a blogger or expert, create an open profile or a "fan" page that encourages broad participation and limits personal information. Use your personal profile to keep your real friends (the ones you know trust) more synched up with your daily life.
Be honest if you're uncomfortable: If a friend posts something about you that makes you uncomfortable or you think is inappropriate, let them know. Likewise, stay open-minded if a friend approaches you because something you've posted makes him or her uncomfortable. People have different tolerances for how much the world knows about them respect those differences.
Know what action to take: If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator.

Protect Yourself with these STOP. THINK. CONNECT. Tips:
Keep a clean machine: Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.

Own your online presence: When applicable, set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit how you share information.

Make passwords long and strong: Combine capital and lowercase letters with numbers and symbols to create a more secure password.

Unique account, unique password: Separate passwords for every account helps to thwart cybercriminals.

When in doubt, throw it out: Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.
Post only about others as you have them post about you.

Meeting Location and Special Accommodations

The Glenside Public Library address is at 25 E Fullerton Avenue, Glendale Heights, Illinois. Please park away from the building. Thank you. The meeting(s) are not library sponsored and all inquiries should be directed to Mike Goldberg at MikeGold60137(at)yahoo.com. Individuals with disabilities who plan to attend this program and who require certain accommodations in order to observe and / or participate in the program are requested to contact CAEUG president, Mike Goldberg at MikeGold60137(at)yahoo.com, at least five (5) days prior to the program, so that reasonable accommodation can be made.

Members Helpline
Any member with a specific expertise can volunteer to be on the Members Helpline.

Beginner Helpline
- Billy Douglas

Beginner hardware problems
- Dick Fergus

Hardware problems, XP, Win 7 & Linux
- John Spizzirri

CAEUG OFFICERS

President	Mike Goldberg
V.P. (Programs)	Roger Kinzie
Secretary	Al Skwara
Treasurer	John St. Clair
Newsletter Ed	Kathy Groce
Board Member	Billy Douglas
Webmaster	John Spizzirri