CAEUG Computers Are Easy User Group

**A**bort,
**R**etry,
**I**gnore....

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

October
2014
Volume XXXI Issue 10

**Confirmed meeting dates**

October 25
4th Saturday

:: :: :: ::

Check
www.caeug.net
for confirmed
meeting dates
MEETING
PLACE
is the
Glenside Public
Library

:: :: :: ::

Visitors
Welcome
HOPE TO SEE
YOU THERE!!
:: :: :: ::
**Copy & paste the urls in your browser to visit the websites in this issue**

**4th Saturday October 25, 2014 presenter:**

**Michael Goldberg will demo Windows Technical Evaluation Copy Build 9841 (Win 10) running in Virtual Box VM on Windows 7 Pro computer**

**National Cyber Security Awareness Month** is designed to engage and educate public and private sector partners through events and initiatives with the goal of raising awareness about cybersecurity and increasing the resiliency of the nation in the event of a cyber incident. October 2014 marks the 11th Annual National Cyber Security Awareness Month sponsored by the Department of Homeland Security in cooperation with the National Cyber Security Alliance and the Multi-State Information Sharing and Analysis Center. **http://www.dhs.gov/national-cyber-security-awareness-month-2014**

**How Safe Are Wi-Fi Hotspots?**

By Larry McJunkin

The Retired Geek Technical Tips for the Non-Technical "Over 50" Crowd

http://retiredgeek.net/ http://retiredgeek.net/contact-me/

Many of us travel a lot, whether in business or just to visit our families and friends. We use our computers, smartphones and tablets in hotels, restaurants, and other places, but are these Wi-Fi "Hot Spots safe?

We all assume it's safe to connect to the Wi-Fi network at our local Starbucks, airport, waiting area where we have our cars serviced, hospital, or even at a relative's home. But it is a really bad idea…a very bad idea! There are many

Table of Contents

reasons you wouldn't want to do this. Let's look at the various types of Wi-Fi network.

**Ad-hoc Networks & Access Point Networks**
Basically, there are two types of Wi-Fi networks accessible by your computer: ad-hoc networks and traditional access point networks. Ad-hoc networks are getting a little outdated, but they still exist. They connect devices directly to each other, while access point networks connect devices to a central router. For example, you could connect two laptops or your laptop and your phone together without the need for a router or any other networking hardware. This would create an ad-hoc network. This is different from a traditional access point network where each device connects to a router, like you most likely have in your house.

**Unsecured Network**
A network is deemed unsecured just by virtue of the fact there is no password required to access it. If you're able to click on a network in your smartphone or tablet and connect to it without a password, you are connecting to an unsecured network, and that makes the device you're using susceptible to hacking…plain and simple.

So, that "free public Wi-Fi" network you encounter at the airport is nothing more than an ad-hoc network that was probably started long ago as a service to travelers, but still persists to this day. Basically, when you connect to this type of network, you are most likely connecting to another computer. And when you connect to that other computer, your computer "could" also be set up to broadcast the "free public Wi-Fi" network to other devices around you, essentially allowing access to all your private data to anyone within range. This is not good!

**Why You Shouldn't Connect to Unsecured Networks**
Let's say you're sitting in a coffee shop and decide you want to check your email to kill some time. You scan the available networks and find one that's open and doesn't require a password. You connect and start surfing. Coffee and free Wi-Fi, how good does it get…right? Wrong! A hacker who is also fond of coffee shops and could be located within range of the router you connected to. He's waiting for someone just like you to connect to the network so he can start a middleman attack. Within a few minutes, he could easily gain access to all your passwords, including bank accounts, email, and anything else he wants. You may not think this is possible…but with today's software and technology, it is!

**How to Stop Wi-Fi Crime**
So how can you help prevent all this from happening? For starters, you can use *only* a secured network that encrypts all of your data. This will ensure your data is safe and scrambled as it travels between you and its destination". Now, if a hacker were to intercept your message, they would see nothing but a bunch of scrambled garbage. Of course, no security measure is 100% safe, but at least good encryption will help a lot.
Tips for connecting to unfamiliar wireless networks…if you must do so:

1. Save the really important tasks, such as online banking and other finances, for home.

2. Try not to connect to any "public" or "unsecured" networks. If you absolutely need access to the internet, pay a few bucks for the secure option...

Con't pg 3

3. When on a Wi-Fi network, look for websites that begin with “https” in the address bar, then try to use only these secure sites.

4. If you really want maximum security, use a VPN.

Lastly, tell all your friends and family to follow these Wi-Fi safety tips. You just may save someone from a major financial or identity theft disaster.

---

## Lamp Post 163

October 2014

It had to happen. Drone **(1)** racing has started in France **(2)**. It resembles the Ewok speeder bike chase scene **(3)** in Star Wars Episode VI: Return of the Jedi **(4)**.

1) **http://bit.ly/1ogXUvk**
2) **http://bit.ly/1wcDgw0**
3) **http://bit.ly/ZA0f8B**
4) **http://www.imdb.com/title/tt0086190/**

Federal Bureau of Investigation (FBI **(1)**) Director, James Comey **(2)**, blasted Apple **(3)** and Google **(4)** for locking police out of phones using strong encryption. The speech (**(5), (6), (7)**) was given to the Brookings Institute **(8)**, a liberal think tank **(9)**. Interestingly, the National Security Agency (NSA **(10)**) was not mentioned. Comey did not disagree with encryption but wanted a backdoor password to open any device 'with a court order'. The FBI has been looking for the same thing for years **(11)**. The Snowden **(12)** revelations have shown that many companies have caved in to government pressure and provided these backdoors. Comey referred only to bad guys but the backdoors have much wider implications to everyone using the Internet. Foreign Intelligence Surveillance Act (FISA **(13)**) court orders are essentially rubber stamps **(14)**. Anyone the government (FBI or otherwise) wants to investigate will be investigated. These court orders are done in secret with no recourse for those who are targeted.

1) **http://www.fbi.gov/**
2) **http://bit.ly/1vtraQh**
3) **https://www.apple.com/**
4) **https://www.google.com/**
5) **http://1.usa.gov/1wphJRT**
6) **http://bit.ly/1wcDnYs**
7) **http://wapo.st/1wgj3EM**
8) **http://www.brookings.edu/**
9) **http://bit.ly/1vLkhLl**
10) **https://www.nsa.gov/**
11) **http://wrd.cm/1DmRtd3**
12) **http://on.mash.to/1poO6dr item 6**
13) **http://bit.ly/1vLkAFY**

Con't Page 4

**14) http://bit.ly/1qQvsvA**

Because I live in Milton Township **(1)** of DuPage County **(2)**, I get a township publication a few times a year called S.A.L.T. (Seniors And Law Enforcement Together). These publications are usually timed to precede the various elections by a few weeks. They prominently feature elected officials (some of whom may be running in the upcoming election). Regardless of the obvious use of taxpayer money to promote incumbent candidates, there is sometimes useful information included. In the most recent edition, curently NOT available on the website, it talks of scams that are directed at anyone who stays in a hotel or motel. Pizza fliers in the room (usually slipped under the door) can be from scammers who require a credit card before delivery. Never give anyone you don't know a credit card number over the phone. If the hotel/motel offers free Wi-Fi, check with the desk clerk as to the exact name of the network and if a password is required. A scammer may have a router named similar to the hotel/motel and route your traffic through their router collecting your user names, passwords, and other critical information for identiy theft **(3)**. If you do not have a document shredder or have too many documents to shred, DuPage County is offering free (you paid your taxes, didn't you?) shredding in Lombard on November 1st from 9 AM to Noon at the commuter parking lot at 101 South Main Street. The restrictions are that only five bags or boxes can be accepted. No binder clips, binders, media disks, plastic bags, pens or pencils are allowed. Paper clips and staples are OK. Another on line safety tips include do not use a public computer (library, computer cafe, etc.) to do banking or other sensitive transactions. Do not put anything on social media that you do not want everyone (in the world) to see. Facebook **(4)** privacy has been simplified since it lost a lawsuit about privacy concerns **(5)**. Another privacy lawsuit has been filed that may cause some real financial trouble for Facebook **(6)**. The Illinois State Toll Highway Authority **(7)** warns that the E-Z Pass Collection Agency (**(8), (9)**) is passing itself off as the E-ZPass Group **(10)** in e-mail. The e-mail claims that the recipient has not paid a toll and thus owes a fine that can be paid by credit card. Do not reveal your credit card information in any e-mail for any reason. E-mail is like a post card, just about anyone can read it. If you have a question about an unpaid toll or e-mail requesting money call 800-824-7277. To file a complaint about an Internet crime go to the FBI Internet crime reporting site **(11)**.

**1) http://miltontownship.net/**
**2) http://www.dupageco.org/**
**3) http://1.usa.gov/1rP1Hul**
**4) https://www.facebook.com/**
**5) http://bit.ly/11MnSfJ**
**6) http://bit.ly/1qQvN1f**
**7) http://www.illinoistollway.com/homepage**
**8) http://bit.ly/1sZ9B9Y**
**9) http://bit.ly/11Mocv1**
**10) http://www.e-zpassiag.com/**
**11) www.ic3.gov**

Yahoo! **(1)** recent article called '10 ways to protect yourself from hackers' **(2)** had no secrets in it. In a nutshell, there were 11 common sense security issues.
1. Change the default password on your router **(3)** and turn on the WPA2 encryption **(4)**.
2. Install and keep up to date anti virus software **(5)**.

Con't pg 5

3. Use the latest version of your OS and update it as often as updates are released.
4. Keep all software updated as soon as updates are released **(6)**.
5. Don't use software that the publisher has stopped supporting.
6. Use passwords and change them periodically. Use a password manager like 1Password **(7)**, Dashlane **(8)**, LastPass **(9)**, Keepass **(10)**, or MaskMe **(11)**.
7. Do not use single password sign on for sensitive (financial) data. If your bank or financial institution does not have two factor validation **(12)**, do not use it.
8. Wipe old hardware **(13)**. Leave nothing for thieves to scavenge.
9. Do not use social media or, if you do, use it sparingly not revealing intimate details of your life such as nude photos of yourself **(14)**.
10. Make sure everyone that uses your computer, laptop, tablet, or smart phone understands and obeys the rules of usage which includes security. Children generally do not understand these rules as they live in a different culture than adults. I think that sometime in the future as these children become adults privacy will become an antiquated idea **(15)** unless things change radically.

1) **https://www.yahoo.com/**
2) **http://yhoo.it/1tBWkGm**
3) **http://www.routerpasswords.com/**
4) **http://bit.ly/ZA0JLY**
5) **http://bit.ly/1vLltyq**
6) **http://bit.ly/1qQwkjV**
7) **https://agilebits.com/onepassword**
8) **https://www.dashlane.com/**
9) **https://lastpass.com/**
10) **http://keepass.info/**
11) **https://www.abine.com/maskme/**
12) **http://bit.ly/1wcDOCc**
13) **http://zd.net/1tBWr4P**
14) **http://bit.ly/1nuALEY Page 5**
15) **http://bit.ly/107RML4**

The Electronic Frontier Foundation **(1)** reported that New York state does not like Bitcoin new law called BitLicense **(2)** prevents anonymity of developers of Bitcoin and other virtual currencies who will be required to provide detailed information about their lives. Information about people using virtual currencies in every transaction must also be recorded and kept for ten years. Why?

1) **https://www.eff.org/**
2) **http://bit.ly/1wcDVhe**

The New Republic Magazine **(1)**, a liberal, political publication **(2)**, recently had an article **(3)** about Amazon **(4)**. The article points out some interesting facts about the book selling giant. Amazon sells 41% of all new books. That translates to an immense power in the cultural life of America. Jeff Bezos **(5)**, CEO of Amazon, can affect the way many Americans think. Do you want him in charge?

Con't pg 6

1) **http://www.newrepublic.com/**
2) **http://bit.ly/1t1i6lR**
3) **http://bit.ly/1sVBAao**
4) **http://www.amazon.com/**
5) **http://bit.ly/1zgiLDi**

The speed cams **(1)** in Chicago **(2)** are not generating the income that the mayor thought they would **(3)**. Seems the mayor will just raise fees and other taxes to cover the 'shortfall' **(4)**. If you are looking to avoid these cams, PhotoEnforced has a map **(5)**.

1) **http://bit.ly/1wgjJKn**
2) **http://bit.ly/1poPkWd**
3) **http://cbsloc.al/1wgjM8Y**
4) **http://dnain.fo/1vLml0p**
5) **http://bit.ly/ZA1cO5**

Kim Komando **(1)** reports that medical records are more important than credit card numbers. The credit card numbers are only worth one dollar on the black market while medical information is worth ten dollars **(2)**. With the Medicare supplemental insurance enrollment time is upon us, it is imperative that you know who you are dealing with and the encryption is intact (look for the padlock **(3)**). One thing that you will want to remember is that your Medicare number is a letter followed by your Social Security **(4)** number.

1) **http://www.komando.com/**
2) **http://bit.ly/1wgjS0n**
3) **http://bit.ly/1poPAEJ**
4) **http://www.ssa.gov/**

Microsoft (MS **(1)**) announces the next iteration of Windows **(2)**. The name, Windows 10, shows emphatically that MS does not know how to count or they want to end the superstition about the 'every other' Windows versions. The 'every other' has been recounted to me by a number of Information Technology (IT) professionals. I do not think it holds up. Some Windows versions have failed miserably because they were not well designed and rushed to market in order to generate revenue. Version 8, Vista (v.6), and Windows ME (v.4) were and are bad. Version 7, XP (v.5), 98 (v.3) were and are good. Windows 95, NT4, and 2K were also good. The skipping of a version number may just be to show that Ballmer is not in charge any more. Whatever the case, I hope that version 10 lives up to the quality and stability of XP and 7. David Pogue reports that 10 corrects the flaws in version 8 and 8.1 **(3)**. Daniel Howley reports that six items that v.8 took away or overlooked are in v.10 **(4)**. Kim Komando thinks that there are only three things to know about this version **(5)**. Reuters's, Bill Rigby, reported that MS has "an uphill struggle in reigniting excitement about Windows" **(6)**. The Windows Club has a comparison of all the 'features' of each Windows version since Vista **(7)**. They also have an install tip list **(8)**. There is an unsubstantiated rumor that Windows 10 will be free to Windows 8 purchasers (**(9), (10)**).

1) **https://www.microsoft.com/**
2) **http://bit.ly/1rkA2l5**


Con't pg 7

3) **http://yhoo.it/1wpICq9**
4) **http://yhoo.it/ZJQPaY**
5) **http://bit.ly/1vtv8bs**
6) **http://trib.in/1rkA3W2**
7) **http://bit.ly/1tBWZHF**
8) **http://bit.ly/1wgk93k**
9) **http://bit.ly/ZJQVzf**
10) **http://bit.ly/ZJQYuU**

MS Office **(1)** has a new app called Sway **(2)**. It is described as a method to display your ideas. I am not sure what that means. Doesn't PowerPoint or Word allow you to do that? The Register's Tim Anderson does not understand it either **(3)**. He had a preview copy to review. The product is not completed. There is no undo or document history function. Maybe they will be added before a formal release. Of course, there is no way to tell what MS may do.

1) **http://bit.ly/1sZe2BR**
2) **http://bit.ly/1Dn1DKV**
3) **http://bit.ly/1CCW5K5**

If you have an iPad or iPhone, live in Glen Ellyn **(1)**, or have a library card in adjacent suburbs, you qualify for a 'free' adult class **(2)** on Wednesday November 5th at 7 PM.

1) **http://gepl.org/**
2) **http://bit.ly/1CCJnuR**

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

---

**10 Tips for Online Shopping Safety**

By Sandy Berger, CompuKISS

www.compukiss.com sandy (at) compukiss.com

Amazingly, in today's topsy-turvy world, because of vulnerabilities in the processing of credit and debit cards used at retail stores and the hackers who are focusing on those vulnerabilities, right now shopping online can actually be safer than swiping your card at a local store. For safety sake, however, there are a few online shopping rules that you should follow.

1. The first of these is to always have a good antivirus program installed on your computer and to update your antivirus program and other software like the operating system whenever an update is available. When in doubt, don't click on links. This is especially true of email where phishing schemes are prevalent, but you should also be careful when you are surfing the Web or visiting social media websites.

2. Shop at trusted, established websites. Don't use any sites that you've never heard of. If you want to try a new website, check to see if any friends or acquaintances have used it successfully.

3. Pay only through secure sites. Typically the address in your browser will change from "http:" to "https:" during a secure connection.

Con't pg 8

4. Never email your credit card number, social security number, or personal information to anyone. No reputable seller will request it by email since email is not secure.

5. Do your banking and shopping from home where you are on your own secure network. Wi-Fi hotspots at local coffee shops and other establishments usually do not offer enough protection unless the user takes some added precautions, which can be cumbersome for the average user.

6. Create strong passwords consisting of numbers, letters, and symbols. Do not use words or names. Make the password for each banking and shopping site unique. Keep your passwords private.

7. Credit cards are generally the safest option for shopping online. When using a credit card, you have limited liability and the ability to have the credit card company intervene if something goes awry. Debit cards can also be a good choice as long as you have investigated their liability limits, which may be higher than those of credit cards.

8. Keep a paper trail. Let's face it, none of us have perfect memories. Print and save records of your online transactions, including the name of the seller, product description, price, and date of purchase. Most reputable merchants allow you to print a receipt after the transaction is complete. You can use these printed receipts to compare to your bank and credit card statements.

9. Monitor your bank accounts and credit card purchases regularly. Report any discrepancies or unusual charges to your financial institution immediately.

10. Your social security number is the key to your identity. Be miserly about sharing it with anyone, especially online. No reputable merchant will ever ask for your social security number to make a purchase.

Credit card theft is pretty easy to get through. Usually you notify your financial institution and they issue you a new card. Identity theft is much more difficult to handle because a thief can open lines of credit in your name, buy a car, and obtain new credit cards. In order to steal your identity, the thieve needs personal information like social security number, address, phone number and financial information. So be careful when giving out any such information.

Many financial experts say that having your bills sent to you electronically and paying them electronically is safer than sending and receiving them by mail. They also recommend shredding paper documents with personal information. So whether you use a credit card at a physical store, you shop and pay bills online, or you pay bills by mail, the key word is "caution." Our mothers taught us to watch our wallets and keep the doors closed. Now we have a lot more convenience, and also a lot more to watch out for.

---

## Interesting Internet Finds

Steve Costello, Boca Raton Computer Society
editor@brcs.org http://ctublog.sefcug.com/

In the course of going through the more than 300 RSS 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 June 2014.

Con't pg 9

**How can I manage a lot of scanned documents?**
http://askleo.com/how-can-i-manage-a-lot-of-scanned-documents/
Leo Notenboom explains how he manages a lot of scanned documents. Check this post out to get an idea of how to handle your own collection of scanned documents.

**How to Record Screencast Videos on Android**
http://www.labnol.org/software/record-android-screencast/4929/
Have an Android and thinking about recording screencasts with it? If so, you should read this post first.
**How to Make a YouTube Video Easily**
http://www.aha-now.com/how-to-make-a-youtube-video/
Another interesting post, this time about how to easily make a YouTube video. This post explains how you can create your own YouTube video without a lot of specialized equipment and lighting.

**Is Your PC Updating Correctly? Are You Sure?**
http://www.techsupportalert.com/content/your-pc-updating-correctly-are-you-sure.htm
You're updating your Windows PC all the time. Are you sure the updates are actually being done? Gizmo's Freeware tells you how to check in this post. I think this is something you should do periodically. In fact, the post reminded me to check my Windows machines. They all checked out, giving me some peace of mind.

**Going Paperless Quick Tip: Clipping Email with the Evernote Web Clipper**
http://www.jamierubin.net/2014/06/17/going-paperless-quick-tip-clipping-email-with-the-evernote-web-clipper/
In this Going Paperless tip, Jamie shows how to clip your email into Evernote using the Web Clipper. I found the tip useful, and thought you might also if you use Evernote and email.

**6 Tips to Help You Go Paperless On Android**
http://www.makeuseof.com/tag/6-tips-go-paperless-android/
This MakeUseOf post explains ways to be paperless on your Android, by scanning receipts and documents, using a notekeeping app, printing to PDF, and more.
**********
Most Fridays, more interesting finds will be posted on the Computers, Technology, and User Groups Blog:
http://ctublog.sefcug.com/tag/interesting-internet-finds/
The posts are under Creative Commons licensing.

---

## October 2014 DVD of the Month

**360TotalSecurity** - Mobile security app
**ARI** - Monthly newsletter
**Autoruns** - Shows what runs at startup
**cCleaner** - Updated hard drive cleaner
**CdBurnerXP** - Updated cd/dvd burner
**CDOMlists** - Contents of CDs and DVDs of the Month
**Chrome** - Updated web browser
**Chromium** - Updated web browser
**Cyberfox** - Web browser
**epCheck** - Track and view TV series data
**continued on pg 10**

**continued from pg 9**

**FBackup** - Updated backup software
**File2Folder** - Creates folder based on file name
**Firefox** - Updated web browser
**FoxitReader** - Updated pdf reader
**FreeFileSync** - File comparison and sync
**GizmoDrive** - Mount ISO files as virtual drive
**ImgBurn** - Updated cd/dvd burner
**IperiusBackup** - Free backup software
**Jing** - Screen & partial screen capture
**JRT** - Updated Junkware Removal Tool
**KarensListPrint** - Print file/folder list w/ details
**LibreOffice** - Updated Office suite software
**LightBox** - Photograph adjusting software
**Listary** - Search utility
**LMMS** - Sound generation system, synthesizer, beat/baseline editor and MIDI control system
**MacriumReflectFREEEdition** - Free disk clone / image software
**MemberContributions** - Things members send me
**MiniToolPartitionWizard** - Partition Management Software
**MozillaLightningProject** - Calendar software for Thunderbird
**OldTimeRadio** - Old radio audio files
**Opera** - Updated web browser
**PDF-XChange** - PDF reader / editor
**PDFill** - PDF editor
**Privatefirewall** - Detects and blocks activity characteristic of known malware
**RemoteDesktopManager** - Holds remote credentials in one place
**SeaMonkey** - Updated web browser
**SSuiteOffice** - Updated Office suite software
**StartMenuReviver** - Win 8 menu replacement
**SyncFolders** - File comparison and sync
**TightVNC** - Updated remote control software
**TORbrowser** - Updated web browser
**UltraDefrag** - Disk defragger
**UltraVNC** - Updated remote control software
**Unetbootin** - Updated flash drive OS creator
**UnityPDF** - Merge, split, divide, rotate, protect PDF files
**USBImageTool** - Create / restore USB flash drive images
**WindowsRepair** - Updated Windows repair tool
**WinToolkit** - Aids in Windows installation
**WPS** - Free office suite
**YTD** - Youtube downloader

## 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 . 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

at least five (5) days prior to the program, so that reasonable accommodation can be made.

**Mailing address:**
CAEUG
P.O. Box 2727
Glen Ellyn, IL 60138

**Members Helpline**
**Any member with a specific expertise can volunteer to be on the Members Helpline.**
Hardware problems, XP, Win 7, Linux and Virus Removal
- John Spizzirri

**CAEUG OFFICERS**

| | |
|---|---|
| President | Mike Goldberg<br>president(at)caeug.net |
| V.P. (Programs) | Roger Kinzie |
| Secretary | Al Skwara |
| Treasurer | John St. Clair |
| Newsletter Ed | Kathy Groce |
| Board Member | Billy Douglas |
| Webmaster | John Spizzirri<br>webmaster(at)caeug.net |