CAEUG Computers Are Easy User Group

Abort, Retry, Ignore....

Founded 1984 ARI is the Official Newsletter of Computers Are Easy User Group

August 2019

Volume XXXVII Issue 8

Confirmed meeting dates
:: ::

August 24
Room A
:: ::
September
TBA
:: ::

Mailing address:
CAEUG
P.O. Box 3150
Glen Ellyn, IL
60138

:: ::
MEETING PLACE is the Glenside Public Library

:: ::
Visitors Welcome
HOPE TO SEE YOU THERE!!

****

August 24, 2019 4th Saturday

Our presenter:

Michael Goldberg will present the video,
Windows 7 Sunset by Greg Skalka
of APCUG VTC 5-4-19
in Room A (8/24/19 4th Saturday)

****

Lamp Post 216
August 2019
by John Spizzirri

The brown (grizzly) bears that feed at Brooks Falls are in Katmai National Park, Alaska (1). The feeding cameras are live. The salmon are jumping up the falls. The bears are catching as many as they can and the feeding frenzy is in full swing.

1) https://is.gd/5XSkeR

Con't pg 2

Table of Contents

According to Ars Technica (1) you can check if your personal information has been compromized (2) by the Equifax (3) data breach and if it has claim additional benefits from the settlement (4). The explanation of how to qualify for additional benefits or reimbursments for remedial expenditures is on the web site. How to file a claim on line is at the EquifaxSettlement site (5).

1) https://arstechnica.com/
2) https://is.gd/TvqvXG
3) https://www.equifax.com/
4) https://arstechnica.com/?p=1542257
5) https://is.gd/lld9sB

A Virtual Private Network (VPN (1)) is essentially a secure tunnel across the Internet that increases privacy through the use of software and or hardware. VPNs, in general, use encryption (2) and authentication to discourage snoopers and crackers. Authentication is often accomplished transparently via Transport Layer Security (TLS (3)) or Secure Sockets Layer (SSL (3)). VPNs cannot keep out a determined cracker, but it makes life very difficult. The snooper or cracker may look at the data being transmitted your PC / tablet / phone and some server on the Internet but will only see encrypted gibberish because when your device and the server began the communication the TLS/SSL set up a secret handshake that only the machines know and that lasts only for the duration of the one communication. All data between the devices are encrypted using that secret handshake. It is discarded when the communication is broken. That is the reason why you should ALWAYS logout / sign out / log off of any financial institution web site you communicate with. Those of you who have multiple devices in your home may opt to get pre-flashed VPN routers so that all devices are always covered by a VPN when on the Internet. The trade off there is that VPN routers are expensive and may not have warranty coverage because of the VPN software. The other problem lies in that devices that are portable like phones and tablets may leave your home and connect at places outside your control. They must have a VPN client installed to be covered. Your phone connecting to your bank while you are in the coffee shop or restaurant without a VPN opens you up to a Man in the Middle attack (MITM (4)). You can think of MITM attacks as eavesdropping. MITM attack is where someone with a device nearby you appears to you as your bank's server. The MITM then establishes a handshake with you. The MITM then contacts your bank's web site that you wanted to contact and creates another connection. All information like passwords, usernames, financial details, and other identifiers are passed through the MITM device in the clear (un-encrypted). Without a VPN you nor the bank are aware of the MITM. I used the bank web site as an illustration. It could be a wealth management account, credit card account, credit bureau account, brokerage account, Bitcoin, or other sensitive web site. Other practical advantages of a VPN are that it hides your Internet Protocol (IP (5)) address from prying eyes. Most VPNs encrypt your data so that snoops cannot read your user names, passwords, e-mails, photos, videos, audio files, bank / financial data and other sensitive information. Stream your favorite content without throttling (6) or location censorship (7). Some targeted advertising charges higher

Con't pg 3

or lower prices based on IP addresses. Some VPNs allow you to change your IP address on the fly during any on line session.

1) https://is.gd/tul6iI
2) https://is.gd/PsDQa8
3) https://is.gd/huFTKB
4) https://is.gd/kRP5d2
5) https://is.gd/lfGlL6
6) https://is.gd/ktGiSY
7) https://is.gd/VlbKDL

The VPN is a useful tool to protect yourself. Former chairman of Sun Microsystems, Scott McNealy (1), said a little over twenty years ago, "You have zero privacy anyway. Get over it." (2) McNealy's company Sun Microsystems was at the time part of the Online Privacy Alliance (3) and a government contractor. Computer industry and government regulators went apoplectic. According to the Wired magazine article (2), Intel disabled some features of the Pentium III chip. The Federal Bureau of Investigation (FBI (4)), Central Intelligence Agency (CIA (5)), National Security Agency (NSA (6)), Department of Defense (DOD (7)), and law enforcement, secret and quasi-secret agencies did not say a word. Jodie Bernstein, of the Federal Trade Commission (FTC (8)), said that McNealy was out of line. Why would Jodie say anything at all. The FTC had been charged with the tenuous task of enforcing fuzzy laws and guidelines about privacy produced and enacted during the twentieth century. Jodie may have privy to the 5 eyes, 9 eyes, 14 eyes ((9), (10)), and all that those designations imply or she may have been just ordered to protest the big mouth on a contractor that did not know how to read his contracts. The 5 eyes was established after World War II as a formal agreement between the U.S.A., Canada, U.K., Australia, and New Zealand to continue electronic spying activities that had begun during the war. As the cold war developed additional countries were recruited creating the 9 eyes adding Denmark, France, Netherlands, Norway. A few years later and more recruiting created the 14 eyes by adding Belgium, Germany, Italy, Spain, Sweden. Today there are unofficial members who may or may not cooperate every time they are called upon to do so. They are Japan, Israel, South Korea, Singapore, and other island territories. Island territories are important in that underwater telephone cables surface on these islands. The government spying on you may not concern you, but it should. Whether it is metadata ((11), (12)) or whole data, our government considers both actionable ((13), (14)). Why should government spying concern you? When the government spys on you, it can do so using metadata or actual data. Metadata can be VERY misleading. I will grant that the government tries to alleviate errors but they do creep in. As a 'for instance' of misleading metadata, lets take me. I have a number of isolated contact lists (address books). I try not to give my phone number as an identifier on e-mail accounts, if possible. I know a variety of people; some law enforcement, some petty criminals, some felons, and some federal criminals. As far as I know, I do not know any 'terrorists', but the definition of terrorist changes from time to time so that may change. I knew a man from Detroit with an Arab sir name, Salah. I would talk to him from time to time

Con't pg 4

before 2010. The last time we talked, the call lasted for a little over a half hour. We talked about business and home life. He told me about his new job as financial planner in Abu Dhabi (15). I asked when he was going. He told me that he was already there. I was flabbergasted. We had been talking for half an hour while we were 7,000 miles apart. I told him that the call must be costing him a bundle so we ended the call. Thinking about the call in light of the Snowden revelations, I know that everyone in my on line address book that was attached to my phone number was now being checked out because I had a call with a Middle Eastern country with a man that has an Arab sir name similar to a name of a man on the FBI top 20 wanted terrorists, Ramadan Abdullah Mohammad Shallah (16). By reading this article this far, you may be linked to the terrorist in the previous sentence by metadata. If you downloaded this document from the CAEUG.NET web site, you may be linked to that terrorist by metadata. The people in your contact list may also be linked because of your download. Still have nothing to hide? But then again I may be paranoid.

1) https://is.gd/p80OmO
2) https://is.gd/9cWtbC
3) https://is.gd/AA1qOj
4) https://www.fbi.gov/
5) https://www.cia.gov/
6) https://www.nsa.gov/
7) https://www.defense.gov/
8) https://www.ftc.gov/
9) https://restoreprivacy.com/?p=16818
10) https://makeawebsitehub.com/?p=6479
11) https://en.wikipedia.org/wiki/Metadata
12) https://is.gd/zEOI8Z
13) https://www.nybooks.com/?p=46276
14) https://youtu.be/UdQiz0Vavmc
15) https://is.gd/Zd4yNY
16) https://is.gd/Zd4yNY

There are other ways of protecting your privacy. Using virtual machines ((1), (2)) with different operating systems is very useful. Creating a new virtual machine each time you want to have better privacy (you cannot have perfect privacy). Using more secure operating systems such as Linux (3) or BSD (4). Use The Onion Router (TOR (5)) to encrypt your browsing so that trackers and ads cannot follow you. Crackers cannot see what you are doing. Snoopers cannot collect data about you. TOR is as easy as downloading and running a browser. The downside is that metadata still exists.

1) https://is.gd/eyjl2B
2) https://is.gd/wkMQg1
3) https://www.linux.org/
4) https://www.bsd.org/
5) https://www.torproject.org/

Con't pg 5

Do you own or know someone who owns a Microsoft (MS (1)) Surface Pro 6 or a Surface Book 2? These two PCs have major troubles with hardware overheating ((2), (3)). They are supposed to run at 1.9MHz but when the overheating occurs the safety circuits reduce the speed to 400 MHz. That is about one quarter of the advertised speed. MS is coming out with a fix in the coming month(s)? Let's hope so. Thanks Microsoft!

1) https://www.microsoft.com/
2) https://is.gd/FCj7u4
3) https://is.gd/e4wj4j

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

Password Managers

By Dave Gerber, Windows 10 Forum
Sarasota Technology Users Club, Florida
July 2019
www.thestug.org
davegerber1 (at) verizon.net

A question about Password Managers came up during the Windows 10 Forum at the July STUG Meeting so I thought I'd share some info common to all of the best known and reputable programs ... Dave Gerber

Password managers are the most recommended tool by security experts to protect your online credentials from hackers. But many people are still hesitant to use them. Here's why password managers are safe, secure, and your best defense against password-hungry cyber criminals.

What is a password manager?

Think of it like a safe for your passwords. When you need something inside the safe, you unlock it. Password managers work the same for your online credentials.

You create a single, super-strong password, which acts like a key. Install the password manager app on your phone, computer, browser, and other devices. Your passwords are securely stored inside it. Anytime you need to log in to an account, unlock your password manager and retrieve your login info.

With website vulnerabilities and security incidents on the rise, many people have grown to mistrust a tech tool to manage their passwords. What if the password manager gets hacked?

Reputable password managers take extra steps to lock down your info and keep it safe from cyber criminals.

Con't pg 6

A good password manager:

- Doesn’t know your master password (so hackers can never steal it)
- Encrypts all your data
- Does not store any of your data on their servers
- Can generate strong, secure password

No privacy tool can completely guarantee your online safety. Even the most elaborate lock can be broken into. Yet we still lock our doors to our houses and cars.

The alternative to using a password manager is to rely on your own memory to remember all your credentials. This inevitably leads to recycling passwords or using variations — a bad habit that hackers love.

Password managers can be such an effective security tool because they help us improve bad habits. With a password manager installed on your computer and phone, it’s a lot easier to take your logins everywhere so you can use unique, strong passwords on every account.

Password managers don’t store all your credentials together in one place. Any data you store in a password manager — passwords, logins, security questions, and other sensitive info — is securely encrypted. Even if the password manager gets hacked, cyber criminals would not be able to see your logins.

The only way to access your data is with a single master password that only you know. You use this password to unlock the manager on your computer, phone, or other devices. Once it’s unlocked, a password manager can fill in your logins to websites and apps.

Our memories sometimes fail us. Ever clicked a “forgot password?” link? It’s very common to use variations of the same password to make them easier to remember. With a password manager, you don’t need to remember any of your credentials. It can be installed on all your devices and will auto-fill your passwords for you. Once you get in the habit of using one, you’ll no longer have to worry about forgetting your credentials.

Sure, it takes time to log all your credentials in a password manager. But you don’t need to do it all at once. You can always start small and change just a few passwords at a time. Try installing a password manager and creating new, unique passwords for the websites you visit most frequently. Over time, as you log in to other sites, you can add others.

Some Fun: After 10 years a wife started to think their child looks kinda of strange so she did a DNA test and found out the child is not theirs, she told her husband what she found out, the husband replied, u don't remember do you?? When we were leaving the hospital the baby pooped and u told me go and change him so I went inside got a clean one and left the dirty one there. The wife fainted....

Using a Web Browser

By Jim Cerney, Forum Leader
The Sarasota Technology Users Group, FL
June 2019 issue, The STUG Monitor
www.thestug.org
jimcerny123 (at) gmail.com

Have you heard of Google Chrome, Microsoft Edge, Firefox, or Safari? Well, they are all Internet Browsers – apps (programs or software) that allow you to see web pages and cruise the internet. No computer should be without one! Windows computers come with Microsoft Edge included for free, but the others are free as well.

Do not confuse a web browser with a search engine. A search engine, such as Google, is a web page that you use to search the internet for something – and you can get to Google on any browser. All web browsers will do the same things, maybe in slightly different ways, and it is up to you to pick the ones you like to use. Here are some tips and information for using any browser:

1. You need internet access to use a browser. If you do not have internet access and try to use it you will get a message that you are not connected.

2. Use the “search/address bar” to enter either text you want to search the internet for OR a web page address (like www.thestug.org). The browser will determine if you are doing a search (not entering a valid web address) and will use the default search engine to do the search and display your results. Firefox, for example, will use Google by default as its search engine. Most browsers will allow you to change the default to another search engine in “settings.” If you enter a valid web page address you will “go to” and see that web page.

3. The “search/address bar” displays the web page address of the page you are looking at. You can highlight and copy this address to paste it in a document, email, etc.

4. As you browse the internet and click on different things, new web pages will be displayed – and you are creating a “chain” of web pages. Not every “click” will create a new web page in the chain, some may create a new “tab,” for example. Use the “left and right arrows” to go to previous web pages (left) or to web pages you have already viewed (right).

5. The little “house” or “home” icon will take you back to your starting web page.

6. The menu of options, including “settings,” “help,” and more is displayed by clicking on the three lines (called a “hamburger”) or three dots in a vertical line.

7. TABS – those things on the top row of your browser (or near the top), are used to create a new “window.” You may think of a tab as if you opened another session of

your browser. As you click on different links sometimes a new tab will be created for you. Tabs can be helpful if you learn how to use them. Create a new tab by clicking on the plus sign “+” at the right end of the tab row. It is easy to return to a web page by clicking on the tab. In your browser settings it is possible to have a set of tabs opened and ready for you when you open the browser.

8. SETTINGS – Can provide the many options, help, and defaults for your browser. Most browsers will have a video of how to use it and will describe what each setting option does.

9. By all means go to Google and ask, “How do I use Google Chrome” (or any browser you prefer) to see videos and help. Take a few minutes to learn more about your browser!

10. FAVORITES or BOOKMARKS will let you create a list of all your favorite web pages. You can organize this list any way you like, including creating “folders.” Clicking on a bookmark may or may not create a new “tab.”

11. History, cookies, and other records are created by all browsers. Look in settings and ask Google about the options for your browser to turn off these things or to delete them. Usually it is a good thing to delete your history upon exiting your browser session.

Learning is good for you. And learning how to use your browser opens up more ways to learn using the internet. Enjoy your potential.

WYSIWYG WEB WATCH (www) - June

by Paul Baecker, Editor
Sterling Heights Computer Club MI
June 2019 issue, WYSIWYG
www.shcc.org
webwatch (at) sterlingheightscomputerclub.org

This column attempts to locate sites containing valuable, amusing, and free content, with no overbearing pressure to purchase anything.

Why do some web site addresses start with WWW2?
https://www.maketecheasier.com/sites-with-www2

Find wood imperfections with mineral spirits (2-min. video).
https://www.todayshomeowner.com/video/find-wood-imperfections-with-mineral-spirits/

Raspberry Pi kits:10 options for beginners as well as experienced makers.
https://www.pcworld.com/article/3244253/best-raspberry-pi-kits.html

How to install and use Microsoft Office on Linux (with a license key, of course).

Con't pg 9

https://www.makeuseof.com/tag/install-use-microsoft-office-linux/

Still using your kid's birthday as your universal password? You're heading toward trouble. Here's a review of password manager software choices.
https://www.pcmag.com/roundup/300318/the-best-password-managers

Kodi was described in an April 2019 newsletter article. Here is a list of 10 legal Kodi add-ons for free movies.
https://www.makeuseof.com/tag/best-legal-kodi-add-ons-free-movies/

A list of 'best' WordPress hosting providers recommended by the author.
https://www.makeuseof.com/tag/best-wordpress-hosting-providers/

Backstabbing, disinformation, and bad journalism: The state of the VPN industry. In the Internet era, everyone needs a VPN — just be cautious with your choosing.
https://www.pcmag.com/commentary/368081/backstabbing-disinformation-and-bad-journalism-the-state

They don't always get away with it. Some spammers have been caught and punished. Here is a rundown of cybercriminals who have done (or are doing) hard time for their misdeeds.
https://askbobrankin.com/spammers_and_scammers_in_the_slammer.html

Don't erase, overwrite: How to avoid being that person who resells or recycles a drive with data still on it.
https://www.pcworld.com/article/3390742/dont-erase-overwrite-how-to-avoid-being-that-person-who-resells-a-drive-with-data-on-it.html

Rock Pi 4B : M.2 & USB 3.0 SBC — Unpacking and using a more powerful Raspberry Pi alternative. (22-min. video)
https://www.youtube.com/watch?v=C4p9EpjA0ZM&list=PL2m2YvnrOYxJQXzFWX5fC1tTfi7COIpAY

"The ultimate guide to your PC: Everything you wanted to know — and more." Near the top of this article is a link to download the entire guide to your PC as a .pdf file — go get it!!
https://www.makeuseof.com/tag/download_your_pc_inside_and_out_part_1/

20 awesome uses for a Raspberry Pi.
https://www.makeuseof.com/tag/different-uses-raspberry-pi/

Getting started with a Raspberry Pi 3 (hardware assembly and software installation and use). (15-min. video)
https://www.youtube.com/watch?v=juHoJYX86Dg

August 2019
DVD of the Month

AdwCleaner - Updated Adware remover
ARI - Monthly newsletter
AudioBook - Free audio book

BlackbirdPrivacy - Windows privacy tweaker

DVDOMlists - Contents of CDs and DVDs of the Month

IsMyHdOK - HD tester

MemberContributions - Things members send me

OldTimeRadio - Old radio audio files
OpenCloseDriveEject - Open/close DVD/CD drives
Ejects USB devices

PrivacyEraser - HD file shreader
PyScripter - Python script integrated development evironment

QuickMemoryTestOK - Memory tester

Shortcut - Video and image editor
SpybotSD - Spyware remover

UltWin - Windows manager

Upcoming Fond Farewell to Al Skwara

After many years in Wheaton as a member of CAEUG, I will be moving to Freeport Illinois to be closer to my son. his wife, and our grandson. I not sure when this will happen but we have targeted October 1 as a possible move date. It has been fun and I will miss the monthly meetings. As an aside we will be having a Garage Sale on August 29,30, and 31 at 2035 Cromwell Drive Wheaton from 8AM to 4PM. I will try to bring in my extra computer stuff to the next meetings, as give aways.
Thanks again for all the memories.
Al Skwara.

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
. 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 3150
Glen Ellyn, IL 60138

Members Helpline
Any member can volunteer to be on the Members Helpline.
Hardware problems, Win 7, Win 10, Linux and Virus Removal
- John Spizzirri

CAEUG OFFICERS

President	Mike Goldberg
	president(at)caeug.net
V.P. (Programs)	Roger Kinzie
Secretary	Al Skwara
Treasurer	John St. Clair
Newsletter	Kathy Groce
Board Member	Frank Braman
Webmaster	John Spizzirri
	webmaster(at)caeug.net