CAEUG Computers Are Easy User Group

Abort,
Retry,
Ignore....

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

Nov/Dec 2023
Volume XXXIX   Issue 11

Confirmed
meeting dates

2023
Nov/Dec
Dec 9

2024
January TBA
Check Website

:: ::

Hybrid
Board Room
in person
OR Zoom

:: ::

Check
website for
dates and
meeting info

:: ::

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

****

PER GLENSIDE Library (Masks are optional)

INFORMATION for Saturday **Nov/Dec 9th** start time in person at Library Board Room is 9:30am or at home Zoom is 10:00am. This will be a hybrid meeting.

There will be a meeting invitation e-mail Thursday evening before the Saturday meeting.

Our **Nov/Dec** presentation will have various short video presentations about Computer Security

Make sure your software is up to date. Stay safe.

Dues for 2024 are due.
Mail dues to CAEUG, P.O. Box 3150,
Glen Ellyn, IL 60138

****

Thank you to all who have paid 2023 dues!

Table of Contents

Page

Join CAEUG meeting in Library or from Home,
Stay Safe! Update information on our website at

https://www.CAEUG.net

CAEUG OFFICERS
President Carl Wallin

V.P. (Programs) Roger Kinzie
Secretary Position OPEN
Treasurer Kathy Groce
Newsletter Kathy Groce

Board Member
Frank Braman
Joanne Beauregard
Webmaster John Spizzirri
webmaster(at)caeug.net

The Glenside Public Library address is at 25 E Fullerton Avenue, Glendale Heights, Illinois. The meeting(s) are not library sponsored 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, at least five (5) days prior to the program, so that reasonable accommodation can be made.

Members Helpline

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

- John Spizzirri

About DVD of the Month
Unfortunately, the DVD of the Month is no longer creating an income center for the club. August 2022 will be the last issue of the DVD. Starting in September, I will feature a review of a freeware program in the ARI... Some of these programs may be elaborate and complicated others may be very simple. I may include screen shots if that can be accommodated.

Lamp Post 263
November / December 2023
by John Spizzirri

Eagle **(1)** and bear **(2)** watching is over for the year, we can now concentrate on the sky. There is a camera at Churchill, Manitoba, Canada **(3)** pointed at the sky. At night, when the weather is clear, you can check for Northern Lights (Aurora Borealis). Churchill is in the Central Time zone. If you stay up really late or get up early, try the Alaska Borealis cams **(4)** or Yellowknife cam in the Mountain Time zone **(5)**. Another place to try offers various cams from around the world **(6).** Keep in mind that the eagles may return to the nest at any time, but will not start rebuilding in earnest until mid to late January. The bears are hibernating. The videos show highlights of the past.

1) https://is.gd/YAuMF0
2) https://is.gd/5XSkeR
3) https://is.gd/3RjcRQ
4) https://auroranotify.com/aurora-links/
5) https://auroramax.com/live
6) https://seetheaurora.com/webcams

Malwarebytes reported **(1)** that Sundar Pichai **(2)**, CEO of Alphabet **(3)**, parent corporation of Google, Inc. **(4)** said, “Privacy is at the heart of

Con't pg 3

everything we do.” On Alphabet's own web site, they self report on a Federal law suit **(5)** that they won stating that they deserve to collect the data on individuals because of the investment in search technology they make. In other announcements, Google stated that it will let users 'hide their IP address while using Chrome', change data retention practices making auto-delete the default, and strengthen Google Workplace suite protection. This sounds all well and good but let's face reality. Google, Amazon **(6),** and Facebook **(7)** make billions of dollars by collecting information about each and every person that uses any of their services even if they are not plainly marked Google, Amazon, and Facebook. For instance, Meta (**8)** not only sells products but owns Facebook, Instagram **(9)**, WhatsApp **(10)**, Beluga **(11)**, Onavo **(12)**, Messenger **(13)** and the Like button **(14)**. The companies owned by Alphbet are Google, Mandiant **(15)**, Fitbit **(16)**, Looker (**17)**, Nest **(18)**, Waze **(19)**, DoubleClick **(20)**, and YouTube **(21)**. The companies owned by Amazon are Whole Foods Market **(22)**, Zappos **(23)**, Kiva Systems **(24)**, PillPack **(25)**, Twitch Interactive **(26)**, and MGM Holdings Inc. **(27)**. According to Proton **(28)**, a company that provides encrypted email, online storage, and Virtual Private Network (VPN) services, Alphabet and its subsidiaries have spent $125 millions in lobbying and campaign contributions to get elected officials to let them collect as much information (about you) as they want. Let me show what this might mean to you. Say one day you log into your computer via Microsoft **(MS 29)** on Windows 10 or 11 using a MS account. You are now being tracked by MS. Instead of opening Edge browser you open Google Chrome and open your GMail account. You find a friend sent you a link to a web site about her vacation at Steamboat Springs, Colorado. On that web site is a link to a YouTube video about 'The Mountain'. You click it and watch the video. You click the like button and close the tab. You click about accommodations for skiers to see what the pricing is. The pricing is far too expensive for your budget so you close the tab. You decide to get in some exercise. You have heard good reports about new trail in the forest preserve across town. You put on your walking shoes and you Fitbit watch. Get the car warmed up and set the Waze map service on you cell phone to direct you to the forest preserve (avoiding the traffic jams). You get to the preserve, walk your prescribed number of steps, and set the Waze for a Home Depot near your home. On the way, Waze tells you that there is a Lowes that is more convenient. Before we go on, Alphabet, Meta, Amazon, and MS have incorporated what you did in about two hours into your already expansive dossier. Soon, you will start seeing ads for cold weather clothing, skiing sporting goods, travel and accommodations in various skiing destinations, not to mention home improvement ads and walking shoes and clothing. In that short time all the companies collected data abuot you and are guessing what you may want to buy in the next few days. You are getting ads in the most unusual times and places, perhaps even on your phone.

1) https://www.malwarebytes.com/?p=97612
2) https://is.gd/1RsvWT

Con't pg 4

3) **https://abc.xyz/**
4) **https://www.google.com/**
5) **https://is.gd/ZvUU4W**
6) **https://www.amazon.com/**
7) **https://www.facebook.com/**
8) **https://www.meta.com/**
9) **https://www.instagram.com/**
10) **https://www.whatsapp.com/**
11) **https://www.gobeluga.com/**
12) **https://www.onavo.com/**
13) **https://is.gd/ddqWjw**
14) **https://is.gd/V52MOK**
15) **https://www.mandiant.com/**
16) **https://is.gd/0XiSB7**
17) **https://cloud.google.com/looker/**
18) **https://is.gd/Hxj4Wl**
19) **https://www.waze.com/live-map/**
20) **https://admanager.google.com/home/**
21) **https://www.youtube.com/**
22) **https://www.wholefoodsmarket.com/**
23) **https://www.zappos.com/**
24) **https://is.gd/ZkCWpU**
25) **https://www.pillpack.com/**
26) **https://www.twitch.tv/**
27) **https://mgm.com/**
28) **https://is.gd/VjEPqY**
29) **https://www.microsoft.com/**

In a related story Malwarebytes reported that Meta is being sued by noyb **(1)**, European Union privacy watchdog group similar to Electronic Privacy Information Center **(EPIC 2)** and Electronic Frontier Foundation **(EFF 3)** here in the United States. The suit **(4)** is essentially a class action against Facebook. Facebook wants users to pay 251.88 Euros ($275 US) per year to not be tracked and sent ads or use Facebook for free and be tracked and sent ads. They have not made that offer in the U.S. yet.

1) **https://noyb.eu/en**
2) **https://epic.org/**
3) **https://www.eff.org/**
4) **https://bityl.co/MkcJ**

Georgia Tech **(1)** just released a study at the Conference on Computer and Communications Security in Copenhagen, Denmark **(2)**. The study **(3)** reveals that major web sites that require a password have very lax requirement for those passwords. "12% of websites completely lacked password length requirements." "30% did not support spaces or special characters." 75% did

Con't pg 5

not require password of at least eight characters in length.

1) https://www.gatech.edu/
2) https://is.gd/KAhao0
3) https://is.gd/AM7WkY

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

Modern-Day Bonnie and Clydes Are Trying To Steal Your Identity and Your Money

By Kurt Jefferson, Editor
Central Kentucky Computer Society
https://ckcs.org/
lextown2 ** gmail.com

I've written in the past that if Bonnie and Clyde were alive today, they definitely wouldn't waste time robbing banks. If you're not familiar with the couple, they were ruthless gangsters who robbed banks, stores, and other places of business and killed lawmen, shopkeepers, and owners of cars they were stealing in at least four states.

They were, perhaps, best known for robbing more than a dozen banks– some of the same banks twice–over a four-year period, primarily in Missouri, Oklahoma, New Mexico, and Texas. Back in their heyday, they also targeted stores in small towns and funeral homes located in rural areas. Make no mistake about it. They were dangerous lawbreakers. That was how it was in the Depression-era 1930s.

Fast forward to today. Modern Bonnie and Clydes don't rob banks. It's too much work. Instead, they steal personal data from computers, phones, and tablets. They're called hackers. One of their main goals in this life is to steal, rob, and gain access to your hard-earned dollars. Their goal is to grab your money and run; your goal is to keep that from happening. So, whether you're tech-savvy or not, how in the world are you supposed to keep this from happening? There are simple steps you can take.

1. When someone calls you on the phone from an unknown number, DO NOT answer the phone; wait for a voicemail message. Microsoft, Apple, etc., will not call you. These thugs want to get their hands inside your computer or other device to steal your passwords or personal information. If you answer the phone, your number may be sold for more money.

2. Don't open emails from unknown sources. Don't open attachments from unknown senders. Don't respond to schemes alerting you that a friend has been hurt in London, Paris, Sydney, or some other location. Could you send

Con't pg 6

money to help them? Your friend is in the hospital and needs your financial help. Their wallet's been stolen. Their purse has been snatched. And I'm the king of Spain.

Please don't fall for it. Don't click on links in an email from someone you don't usually hear from, urging you to view these great photos. There are no photos. Once you click on the link, malware infects your Windows PC and sends emails to everyone in your address book with the same message, urging them to click on a link to view photos. Phishing is the most successful cybercrime in America.

There were nearly 324,000 victims last year alone. (Phishing refers to an email that appears to be from a legitimate company or organization. There's often a threat – your account will be closed, or the sheriff will come to your house unless you respond. It's all bogus. But plenty of Americans fall for it.) Ever gotten an email that you owe $500 for Norton 360 (virus and malware protection software) that you never even purchased? You'd be surprised by how many folks respond to the email and even pay for the software they don't own. The thugs sending the email are not from Norton. Most junk email trying to get into your wallet originates in Russia, Germany, the U.S., and China.

3. Yes, it's a pain. But what tech folks call two-factor authentication can save your bacon. Turn it on. You'll be blocked if you decide to change your Gmail password, Facebook log-in, iCloud username or password, or some other account, you'll be blocked. You must enter a code you receive in a text message, an email, or even using the Gmail app on your smartphone to get permission to change your password. Yes, as I said, it's a pain. But it's preventing crooks from gaining access to your account. So instead of just changing your passwords, you must first receive a code and enter it into a website or Gmail app. That proves you are who you say you are.

4. Run antivirus software.

For Windows PCs:
Safety Detectives: The Best Windows Antivirus
https://www.safetydetectives.com/

PC Mag: The Best Antivirus Software for 2023
https://www.pcmag.com/picks/the-best-antivirus-protection

For Macs:
Safety Detectives: Ten Best Antiviruses for Mac in 2023
https://www.safetydetectives.com/best-antivirus/mac/

Macworld: Best Mac Antivirus Software 2023
https://www.macworld.com/article/668850/best-mac-antivirus-software.html

For Linux:
Safety Detectives: Five Best Antiviruses for Linux in 2023
https://www.safetydetectives.com/best-antivirus/linux/

Ubuntu Pit: Top 15 Best Linux Antivirus Programs in 2023
https://www.ubuntupit.com/best-linux-antivirus-top-reviewed-compared/

5. Don't go on a fishing expedition on the Web. The World Wide Web is remarkable. It's the best library in the world. There are an estimated 1.6 to 1.9 BILLION websites currently accessible. Less than 400 million are currently active. More than 51% of all people in the world are online. Asia accounts for half the Internet traffic worldwide. Talk about diversity. Websites appear in more than 200 languages. But watch your step. Don't put your foot into horse dung. Make sure the website you visit starts with https. No, this is not always possible.

Some websites refuse to use the "https:" system. The "s" stands for secure. You're accessing a secure website. Don't randomly visit online gambling websites, sites with outdated addresses, websites with shortened addresses, sites ending in .onion, torrent websites (file sharing sites), porn sites and others.

Google constantly scans websites, looking for legitimate websites that have been compromised, unsafe sites, or other questionable pages. If you wonder whether a website is safe or not, visit the web address below and paste your website into Google's Safe Browsing website:
https://transparencyreport.google.com/safe-browsing/search

It will tell you whether it's safe to proceed or not.

5. Use a well-regarded virtual private network (VPN).

This tool sends your Internet signal through a tunnel so that hackers and other thieves cannot access the web pages you visit, your email, your passwords, or additional private information. Do your homework. Find a good VPN you can afford.

Steer away from free VPNs because many sell your data online, bombard you with ads, and some even use your computer's processing power.

For Windows PCs:
Privacy Savvy: Five Best VPNs for Privacy
https://privacysavvy.com/vpn/best/windows/

VPN Reports: Best of the Best VPNs

Con't pg 8

https://www.vpnreports.com/best-vpn/windows/

For Macs:
VPN Reports: Best VPNs for Mac in 2023
https://www.vpnreports.com/best-vpn/mac/

Safety Detectives: Ten Best VPNs For Mac
https://www.safetydetectives.com/best-vpns/mac/

For Linux PCs:
Safety Detectives: Five Best Linux VPNs
https://www.safetydetectives.com/blog/best-linux-vpns/

Pro Privacy: Ten Best VPNs for Linux
https://proprivacy.com/vpn/comparison/best-linux-vpn

6. Use a password manager to track your passwords and log in to many websites requiring a username and password automatically. Experts say this is smarter than allowing your browser to remember your passwords. Unfortunately, web browsers are not really safe to keep that sort of information. As Tom's Guide writes, "That's because desktop web browsers, despite their best efforts, tend to do a lousy job of safeguarding your passwords, credit card numbers, and personal details, such as your name and address. As a result, web browsers are fairly easy to break into, and lots of malware, browser extensions, and even honest software can extract sensitive information from them."

Here are websites where you can read about the best password managers and pick one that works for you:

PC Mag: **https://www.pcmag.com/picks/the-best-password-managers**

Tom's Guide: **https://www.tomsguide.com/us/best-password-managers,review-3785.html**

How To Geek: **https://www.howtogeek.com/780233/best-password-manager/**

happy
holidays

HAPPY NEW YEAR
2024