



# Computers Are Easy User Group

Abort,  
Retry,  
Ignore....

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

April 2024  
Volume XXXX Issue 4

\*\*\*\*\*

PER GLENSIDE Library (Masks are optional)

INFORMATION for Saturday April 27th 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 April presentation various short  
video presentations about remote control software

CAEUG, P.O. Box 3150,  
Glen Ellyn, IL 60138

\*\*\*\*\*

**Thank you! to all who paid the  
low \$20.00 dues for 2024!**

**Your support helps pay for our PO Box and  
APCUG membership and CAEUG website**

Confirmed  
meeting dates

**2024**

**April 27**

**May 25**

:: ::

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  
:: ::

## Table of Contents

	Page
2	Lamp 267 April 2024 By John Spizzirri
5	Two-Factor Fiasco By Greg Skalka
8	YouTube, an Online Video Sharing Service, Part 1 By Ron Sherwood
9	For those over 50 (Joke)

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 267 April 2024 by John Spizzirri

The bald eagles at Decorah, Iowa ( **1** ) eggs hatched at the North nest on March 24 and 25. The eaglets have shed their initial fuzz and grown in the beginning phase of their permanent feathers. As of this writing the birds weigh about two pounds. The adults are feeding them every two to three hours during the day.

The eaglets still cannot stand up for long, but they do get around. The South nest ( **2** ) has been taken over by a pair of Canadian geese (as I noted before). The clutch of six eggs was laid between March 9th and 18th. They will hatch any day now. The goslings will be nurtured for a day or two in the nest. When the goslings are prepared by the adults, they will jump from the nest to the ground. That is about a 55 foot drop to the forest floor. Most of the goslings survive as they fall on a bed of leaves with bodies that are very elastic.

- 1) <https://is.gd/0YqTVG>
- 2) <https://is.gd/YAuMFO>

The Northern Lights (Aurora Borealis) cam at Churchill, Manitoba, Canada ( **1** ) is pointed at the sky. When the weather is clear, you can see the lights at night. You can check the weather at the polar bear site ( **2** ). It is off season for polar bear watching. Churchill is in the Central Time zone. If you stay up really late or

get up early, try the Alaska Borealis cams ( **3** ) or Yellowknife cam in the Mountain Time zone ( **4** ). Two places to try offer various cams from around the world ( **5, 6** ). The brown bears are hibernating. The videos show highlights of the past. To check on the space weather (for aurora forecasts) try here ( **7** ) and NASA ( **8** ).

- 1) <https://is.gd/3RjcRQ>
- 2) <https://is.gd/7PDEvO>
- 3) <https://auroranotify.com/?p=63>
- 4) <https://auroramax.com/live>
- 5) <https://seetheaurora.com/webcams>
- 6) <https://lightsoverlapland.com/?p=79>
- 7) <https://www.spaceweather.com/>
- 8) <https://www.swpc.noaa.gov/>

Malwarebytes reported ( **1** ) something that I have been saying would happen for quite some time. The Federal Bureau of Investigation ( **FBI 2** ) requested all the information YouTube ( **3** ) had on any individuals that WATCHED certain videos this past January. If you can show a video on the Internet, i.e. not child porn or snuff video, why is the FBI interested in who is WATCHING any YouTube video??? The Surveillance Technology Oversight Project ( **STOP 4** ) chimed in, stating "No one should fear a knock at the door from police simply because of what the YouTube algorithm serves up. I'm horrified that the courts are allowing this." Forbes ( **5** ) indicated that it saw Justice Department documents stating that YouTube is not to tell anyone that they did this. There is no comment from YouTube at this time. This is one of the reason I do not give my name or an address to YouTube and I use a Virtual Private Network ( **VPN 6, 7, 8** ). Many people say that VPNs are a waste of money. If the FBI could not get the name and address of the person from YouTube, they wanted the ip address. A VPN hides the ip address with a different address. That address can be tracked back to you but it is time consuming and requires staffing. Any police agency must balance their resources against the "crime" of WATCHING a legal video. The costs might be too much. The FBI never has that problem.

- 1) <https://www.malwarebytes.com/?p=107322>
- 2) <https://www.fbi.gov/>
- 3) <https://www.youtube.com/>
- 4) <https://www.stopspying.org/>
- 5) <https://www.forbes.com/>
- 6) <https://is.gd/tul6il>
- 7) <https://is.gd/r57og8>
- 8) <https://www.wired.com/story/best-vpn/>

In early March, PetSmart Data Security Team notified their customers that they were seeing an unusual number of customers guessing their passwords. They sent out a letter ( **1** ) to warn customers that they should not use the same

password and username on different accounts. It is never a good idea to use the same credentials for more than one account. Crackers that buy or crack a data base with user credentials will try those credentials on other sites to see if they work. It is good for PetSmart to spot this and notify customers to change their passwords. Malwarebytes ( **2** ) reported this in their newsletter, reprinted the letter that was sent to PetSmart customers, and, of course, tried to sell Malwarebytes software.

- 1) <https://is.gd/iaVAhV>**
- 2) <https://www.malwarebytes.com/?p=106155>**

Andrew Cunningham did an article ( **1** ) for Arstechnica about the Raspberry Pi 5 ( **2** ). According to him the 5 is capable of doing desktop work provided an add-on cooling fan is used. The 5 is capable of using an add-on NVMe SSD or the SD card for the operating system. One of the things he does not point out is that with all the extra things that are needed to make a usable desktop will require about \$200 (monitor, keyboard, mouse, power supply, cooling fan, SD card, cables, & Raspberry Pi 5). You can get a Windows 11 PC for about the same amount of cash ( **3, 4, 5** ). Obviously, neither one of these PCs are speed demons, but they can both do the job.

- 1) <https://arstechnica.com/?p=1986894>**
- 2) <https://is.gd/xadXwl>**
- 3) <https://amzn.com/dp/B0CH81C4K3>**
- 4) <https://amzn.com/dp/B0BW8K69VP>**
- 5) <https://amzn.com/dp/B003NREDC8>**

TechCrunch has an article outlining the way AI companies are treating the term 'open source' ( **1** ). The article pointed out that these companies ignore the concept behind open source with the freedom to study and change code. These companies use the copyright laws and the hardware that wealth buys to prevent open source from being implemented all the while claiming that they are supporting it. Within the article are a list of other articles that support that premise. The article goes on to talk about a computer called Hala Point ( **2** ) delivered to Sandia National Laboratories ( **3** ). Hala Point can resemble functions of the human brain. The worry is will this device determine that the human race is detrimental to its existence and what will it do about that. Nice round up of AI.

- 1) <https://techcrunch.com/?p=2693989>**
- 2) <https://is.gd/CtcZiv>**
- 3) <https://www.sandia.gov/>**

TechCrunch reported on how to remove spyware on your Android phone ( **1** ). They have other associated articles about 'The Truth Spy' ( **2** ), 'KidsGuard' ( **3** ), and other 'stalkerware' ( **4** ). The article shows screen shots

of how to remove the spyware. The article references the Coalition Against Stalkerware ( 5 ) which also tells how to remove the software without the screen shots. The Coalition also has information about how to protect yourself from the person that is tracking you (they will know that you removed the software and may want to do something about it.)

- 1) <https://techcrunch.com/2024/04/19/remove-android-spyware/>
- 2) <https://techcrunch.com/2022/10/26/inside-thetruthspy-stalkerware/>
- 3) <https://techcrunch.com/2020/02/20/kidsguard-spyware-app-phones/>
- 4) <https://techcrunch.com/tag/stalkerware/>
- 5) <https://stopstalkerware.org/information-for-survivors/>

Bleeping Computer has a report ( 1 ) about recent instances of ransomware that should make you backup your hard drive before you finish reading it. Ransomware has decreased over the past year but recently has had an uptick.

- 1) <https://is.gd/PxWOjN>

Arstechnica reported that DARPA ( 1 ) has outfitted F-16D jet fighter to be flown exclusively by AI against a human piloted jet fighter ( 2, 3 ) in a dog fight. The F-16D is monitored by two human pilots in the event that they need to take control. This type of control is a big breakthrough. If foreign powers can manage this capability, the only winner will be the one with superior jet fighter hardware as the human factor will be gone.

- 1) <https://www.darpa.mil/>
- 2) <https://arstechnica.com/?p=2018649>
- 3) <https://www.darpa.mil/news-events/2024-04-17>

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

---

**Two-Factor Fiasco**  
**Greg Skalka, President**  
**Under the Computer Hood Users Group Home (uchug.org)**  
**UCHUG (Under the Computer Hood Users Group) SD | Meetup**  
**1editor101 (a) uchug.org**

If you are accessing a personal account or app on the web, you should be concerned about that account's security. Bad actors (and I don't mean those who can't get a job in Hollywood) constantly search for our login credentials, hoping to access our accounts and steal money or personal information. The best ways to protect online accounts include using strong passwords and protecting them, resisting attempts by others to gain access to those accounts through scams and phishing communications, and using two-factor authentication on those accounts.

Two-factor authentication, or 2FA, requires at least two identification items of

different types to log into an account. It is a subset of multi-factor authentication (MFA). This can be enabled for most online accounts; some account providers now require it. It typically requires providing two or more identifying items from three categories for account access. These categories are something you know (like a password, birthdate, or the answer to a security question), something you have (could be a specific phone, computer, or email account, or a security key, fob, or dongle), and something you are (a biometric like a fingerprint).

To get money from an ATM (assuming you are not trying the big truck with a chain approach), you must provide something you have (an ATM card) and something you know (a PIN). With a 2FA-enabled online account, to gain access, you would typically need something you know (a password) and something you have (either a smartphone or computer that can receive a security code through text message or email). Entering the correct code sent to the device that presumably only you have validates your identity in a second way (in addition to the password).

Your account provider may be using 2FA, and you don't even realize it. Even if you only enter a password for access, the provider may look at the IP address or other identifying information from your device's connection to validate that it is really you (something you have). If you usually log in from one device and then suddenly use another, the account provider may ask for additional verifying information, like the answer to a security question.

It should be evident that trying to make it more difficult for others to access your accounts could also make it more difficult for you. Going through additional steps, like entering a six-digit code you were sent through a text message, takes time and opens up the possibility of being denied access. If you lose your phone, have phone communication problems, have a malfunction in your fingerprint scanner, or lose control of your email account, you may not be able to get timely access to your accounts.

I was a little apprehensive about 2FA at first due to concerns about my being denied access due to some problem outside of my control. I don't remember if I started using 2FA because I enabled it or if some account I already had started requiring it. I have used 2FA for several years on most of my critical accounts. Whenever I am asked to enable it, I look to enable it on some accounts (I have found some that did not support it then; I'm starting to think less of those companies). I typically use my phone as the second form (something I have); I need to ensure I have my phone handy when I want account access on my computer. Receiving a code as a text on a phone is supposed to be more secure than receiving it in an email. It may be a little more work, but I have had a few problems with it denying me access when I needed it.

Recently, however, I have had a few instances of being denied access to accounts through 2FA. My first instance was about a week ago when I was trying to access my Scripps online medical account on my computer to perform an electronic check-in for a medical appointment. Of course, I was in a hurry, trying to do this late at night, just before bed for an appointment the next day, and I would not have time to do it later.

After successfully entering my username and password on the MyScripps web login page, a page was provided to select the method for sending a code: email or text. I have found that my phone usually receives the text in just a few seconds. This time, however, the text did not come right away as expected. I waited maybe 60 seconds (remember, I wanted to finish this and go to bed) and then clicked "Send code again."

Again, I waited, this time a little longer. I checked my phone to see that it was on and not in airplane mode or something else that would turn off reception.

After waiting longer than I wanted, I finally selected email to deliver the code. Then, I had to start Thunderbird (my email program) to access my Juno email on my computer. Fortunately, the email with the code was there, and I successfully logged into Scripps and completed my task. At the time, I thought it was strange, but I didn't consider the problems I had any further. The following day, I found that the texts had come in at night.

A few days later, I tried to log into my US Bank online banking account from my computer; I again needed to check my account balance with some urgency. The US Bank 2FA code enter screen comes up right after entering a valid username and password; I may enable only texts to my phone for this. Again, I was used to having the text with the code pop up on my phone immediately, but I waited several minutes without receiving the text message. I now remembered my Scripps incident. There was no email delivery selection on the 2FA code entry screen on the US Bank website, but there was a link to "verify another way." I had hoped it would lead to verification through an email, but instead, it asked me to enter my debit card PIN.

I don't use a debit card for any of my accounts; I may have been sent one by the bank years ago, but I never activated it and had no way to get its PIN. This lack of access to my account was beginning to make me angry.

I canceled out of that screen (the only option) and tried going into the login page to get another code sent, but no code text message came to my phone. Finally, the bank locked me out of online access for too many unsuccessful attempts. I would need to change my password to get access again, and the first step for that was to send me a code that I'd need to enter. Good grief! I searched their website and finally found a number to call for online access support (they don't make things like this very obvious on their site).

While still on their site, I called the number and started my way down their automated phone menu system. Suddenly, while listening to the next set of options, I heard the sound of text messages being received on my phone. I found a bunch of texts from US Bank with 2FA codes that had just come through on my phone. I hung up the call and returned to the web page, but after entering the code from the last text, it said the code had expired, and a new one would be sent. Again, no code text was received. I called the US Bank support number again and found that action again appeared to trigger the receiving of text messages on my phone. Again, I was too late to enter these codes, but I now saw a pattern.

I returned to the bank website and asked for a code to change my password. I then immediately called the US Bank support number, and after a few entries in their audio menu, a text arrived on my phone. I could enter this code in time, change my password, and regain access to my online accounts.

I finally got the information I needed off the website, but I was concerned about what I had to go through to get it. Why were my texts not coming through right away? It seemed like making the phone call (or pressing phone keys) triggered the reception of texts that appeared stuck somewhere.

This seemed like a problem, so I cycled power on my phone and then tried logging into my US Bank online account. This time, the text message with the 2FA code was

received right after my password was accepted, just as it had been.

Something in my phone went awry, and cycling the power fixed it. I try to remember to do that periodically; I need to be better at making that a part of my tech management routine.

I still understand that online security is essential, but I also know how it feels to be locked out due to some malfunction in the system. The lesson in resiliency to take away is not to decrease security to prevent being affected by such a failure. Still, instead, I plan so I'm not doing things at the last minute and making myself vulnerable to problems when something inevitably breaks down.

---

**YouTube, an Online Video Sharing Service, Part 1**  
**By Ron Sherwood, Member**  
**East-Central Ohio Technology Users Club**  
**<https://ecotu.club/>**  
**newsletter \*\* ecotu.club**

YouTube is an online video-sharing service currently owned by Google. According to the Wikipedia entry for YouTube, it is second only to Google Search as the most visited website. According to *wyzow*, YouTube Stats: Everything You Need to Know In 2023! "An average of 2,500 new videos are uploaded to YouTube every minute," so there is plenty to watch. Content covers the gamut from humor to science; my favorite is the how-to videos. Access is free; anyone with an account (any Google account will work) can have their own "channel" and upload content. As you might expect, this "anyone can upload" policy means the accuracy of the content varies from excellent to what I consider just plain junk. As you should with any Internet content, use caution and common sense when judging the accuracy of YouTube content.

To access YouTube, type YouTube.com into your browser's address box. The opening page shows a variety of videos available for viewing. Keep scrolling down for more and even more possibilities. To narrow the video choices, use the search box at the top of the page. I often search for "how to" videos. For example, I just replaced the weather strip around some doors. I've done this before, but I thought I'd see if I could find any "secrets" of the pros to simplify the job. I viewed several videos, and the creators generally agreed on what to do. Some said to start at the top; others started with the sides, but otherwise, there was agreement.

One tip I picked up was mitering the corners for a better seal. I also learned when and where to install foam wedges.

Want to learn how to cook a particular dish? Type the name into the search box, and you will likely get hundreds of videos to view.

A special tip: did you miss a presentation at an ECOTUC/LCCS meeting? Type LCCS Media into the search, and thanks to club member Everett McKee, you will find videos of presentations at meetings. Everett also posts videos of general meetings.

Some content creators post new videos as often as daily. Other channels change infrequently. If you find a channel you want to follow, click the "subscribe" button to begin a list of channels for easy access. This is similar to "favorites" in other applications. You will need to sign in with a Google address to create a subscription list.



## For Those Over 50

(Joke)

I thought about the 30 year business I ran with 1800 employees, all without a Blackberry that played music, took videos, pictures and communicated with Facebook and Twitter.

I signed up under duress for Twitter and Facebook, so my seven kids, their spouses, 13 grandkids and 2 great grand kids could communicate with me in the modern way. I figured I could handle something as simple as Twitter with only 140 characters of space.

That was before one of my grandkids hooked me up for Tweeter, Tweetree, Twhirl, Twitterfon, Tweetie and Twittererific Tweetdeck, Twitpix and something that sends every message to my cell phone and every other program within the texting world. My phone was beeping every three minutes with the details of everything except the bowel movements of the entire next generation. I am not ready to live like this. I keep my cell phone in the garage in my golf bag.

The kids bought me a GPS for my last birthday because they say I get lost every now and then going over to the grocery store or library. I keep that in a box under my tool bench with the Blue tooth [it's red] phone I am supposed to use when I drive. I wore it once and was standing in line at Barnes and Noble talking to my wife as everyone in the nearest 50 yards was glaring at me. Seems I have to take my hearing aid out to use it, and I got a little loud.

I mean the GPS looked pretty smart on my dash board, but the lady inside was the most annoying, rudest person I had run into in a long time. Every 10 minutes, she would sarcastically say, "Re-calc-ul-ating".

You would think that she could be nicer. It was like she could barely tolerate me. She would let go with a deep sigh and then tell me to make a U-turn at the next light. Then when I would make a right turn instead, it was not good.

When I get really lost now, I call my wife and tell her the name of the cross streets and while she is starting to develop the same tone as Gypsy, the GPS lady, at least she loves me.

To be perfectly frank, I am still trying to learn how to use the cordless phones in our house. We have had them for 4 years, but I still haven't figured out how I can lose three phones all at once and have run around digging under chair cushions and checking bathrooms and dirty laundry baskets when the phone rings.

The world is just getting too complex for me. They even mess me up every time I go to the grocery store. You would think they could settle on something themselves but this sudden "Paper or Plastic?" every time I check out just knocks me for a loop. I bought some of those cloth reusable bags to avoid looking confused, but I never remember to take them in with me.

Now I toss it back to them. When they ask me, "Paper or Plastic?" I just say, "Doesn't matter to me. I am bi-sacksual." Then it's their turn to stare at me with a blank look. I was recently asked if I tweet. I answered, No, but I do toot a lot.

---

**Remember -- April showers bring May flowers!**