CAEUG Computers Are Easy User Group

Abort, Retry, Ignore....

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

Feb 2025
Volume XLI Issue 2

****

PER GLENSIDE Library (Masks are optional)

INFORMATION for Saturday February 22 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 February presentation
We will have various videos about the DeepSeek program and China's involvement.

NEW!!! CAEUG, P.O. Box 153 NEW!!!
South Elgin, IL 60177

****

Thank you! to all who paid the low $20.00 dues for 2025!

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

Confirmed meeting dates

2025

February 22

March 22

:: ::

Hybrid Board Room in person OR Zoom

:: ::

Check website for dates and meeting info

:: ::

!!!! NEW !!! Mailing address:

CAEUG
P.O. Box 153
South Elgin, IL 60177

:: ::

Table of Contents

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

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 276
February 2025
by John Spizzirri

The Decorah bald eagles have rebuilt their nest **(1)** and started a new family. The first egg was layed on 2/10 and the second came on Valentines Day (2/14). The hatching is expected in about 35 days. With longer night time hours, now is the time to keep the Aurora cam sites in your favorites. The Northern Lights (Aurora Borealis) cam at Churchill, Manitoba, Canada **(2)** is in the Central Time zone as is the polar bear site **(3)**. If you stay up really late or get up early, try the Alaska Borealis cams (**4)**. Two places to try offer various cams from around the world (**5, 6)**. To check on the space weather (for aurora forecasts) try here **(7)** and NASA (**8)**.

1) **https://is.gd/0YqTVG**
2) **https://is.gd/3RjcRQ**
3) **https://is.gd/7PDEvO**
4) **https://auroranotify.com/aurora-links/**
5) **https://seetheaurora.com/webcams**
6) **https://lightsoverlapland.com/?p=79**
7) **https://www.spaceweather.com/**
8) **https://www.swpc.noaa.gov/**

Con't pg 3

Our newsletter editor, Kathy Groce, received a text allegedly from the Illinois Tollway Authority **(1)** claiming that she had an unpaid toll invoice. "To avoid excessive fines when your bill is past due, please cooperate and pay on time by (date). Have a great trip. Please confirm (bit.ly url)." She has never used any Illinois Tollway with any car with her current license number. She does not like driving on tollways. She wanted to know if the bit.ly **(2)** url actually was going to the Illinois Tollway. Tollway fines can be excessive and it is best to avoid any misunderstandings before things get out of hand. She wanted to check where the short URL went without going there in case it was a pirate site. I found three sites that would reveal the actual URL of any short URL. They are; Wheregoes **(3)**, Expandurl **(4)**, and Checkshorturl **(5).**

1) **https://illinoistollway.com/**
2) **https://bitly.com/**
3) **https://wheregoes.com/**
4) **https://www.expandurl.net/**
5) **https://checkshorturl.com/**

Chinese government has given DeepSeek, an artificial intelligence (AI) startup, considerable investment. It gets preferential tax treatment as a national high-tech enterprise. China's State Council released its Artificial Intelligence Development Plan in 2017 **(1)**. This plan wants local sections of the Chinese State to hunt down bright individuals for high tech industries such as AI. Cybersecurity experts have discovered that DeepSeek's code contains hidden programming with the capability to send user data directly to the Chinese government **(2)**. Ivan Tsarynny, CEO of Feroot Security, found direct links in DeepSeek's code to servers and companies in China under government control. The code appears to have the capability to send user data to CMPassport dot com, the online registry for China Mobile, a telecommunications company owned and operated by the Chinese government. China Mobile has been banned from operating in the U.S. since 2019 due to national security concerns **(3)**. There are risks to you if you choose to use DeepSeek;

1. Data Transfer: Users who register or log in to DeepSeek may unknowingly be creating accounts in China, making their identities, search queries, and online behavior visible to Chinese state systems.
2. Personal Information Collection: DeepSeek's privacy policy states that it collects information including users' device model, operating system, keystroke patterns, IP address, and system language. This data is held on servers located in the People's Republic of China.
3. Surveillance Concerns: John Cohen, former acting Undersecretary for Intelligence and Analysis for the Department of Homeland Security **(4)**, described DeepSeek as a blatant example of suspected surveillance by the Chinese government.
4. Behavior Manipulation: Ross Burley, co-founder of the Centre for

Con't pg 4

Information Resilience **(5)**, warned that the collected data could be used for behavior change campaigns, disinformation campaigns, and targeted messaging to Western audiences.
The National Security Council (NSC) is examining the potential national security implications of DeepSeek's launch **(6)**. President Trump called DeepSeek a "wake up call" for American industries (**7)**. China did something better and cheaper than we (American industry) did and our industries better catch up. American consumers have shown a willingness to risk it all to get the latest Chinese technology. DeepSeek has become the most downloaded free application in the U.S. on Apple's app store since its introduction **(8)**. This trend suggests that consumers may be dumber than they look. The use of DeepSeek is something that I, for one, will not try. Too many American and western companies are already tracking me no matter how much I try to keep them out of my life. I do not need the Chinese communists, too. Use DeepSeek at your own peril.

1) **https://bitl.to/3z0n**
2) **https://is.gd/myyd5n**
3) **https://www.fcc.gov/node/230418**
4) **https://bitl.to/3z0m**
5) **https://www.info-res.org/faqs/**
6) **https://is.gd/q4Vfbj**
7) **https://is.gd/sUvV4w**
8) **https://is.gd/3GLl3P**

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

Thunderbird Problem Solved
by Larry Bothe and
John Spizzirri

Larry Bothe, our former president and treasurer, had a problem with email phishing scams that were clogging his inbox everyday. He uses Thunderbird (1) as an email aggragator and client. He wrote me about the problem. He told me the following:

"Lately (past several months) I have been deluged (several a day, literally) with messages offering to improve the SEO ranking on my website. Since a) I don't have a website, and b) the messages never mention the URL, I know they are just phishing. I finally decided to construct filters to block these kinds of messages. I have been partially successful, but in order to do a complete job I need to construct a filter that looks for two separate words, separated by other words. For example, if I receive a message that contains the sentence I checked your website, you have an impressive site, but the ranking is not good on Google, Yahoo and Bing, I want to create a filer that looks for both ranking

and Google. I know you have to use an operative word, such as AND, but I can't make it work. I have tried various iterations, with and without spaces, etc. but I can't make it filter. Any ideas? What the heck am I doing wrong?"

I wrote back about 'training for junk email' which was not much use. I also wrote;

"Do you get much email with the word website in it that you want to read? Maybe you could filter that for the word website and the name of person you get it from to a special folder and all the other email with the word website in it to junk or trash."

Larry thought about it and figured out how to solve the problem. He wrote me about how he did it;

"A week or so ago I sent you a message asking about how to construct a filter in Thunderbird to block spam messages. I wanted the filter to find two or more specific words before the message would be blocked. Yesterday, after reading some more on the subject of filters, I figured it out on my own. It's actually pretty easy, and I feel a bit stupid for not seeing it earlier.

Instead of trying to write a string of words to search for, you simply block each word individually, and then tell the filter to "match all". By block each word individually, I mean give each word its own search line. If you want to block messages that contain both Google and ranking, then you enter a line that says .... "If the body of the message contains ranking", and a separate line that says "If the body of the message contains Google"....., and then check the box for "Match All". For the action, choose "Move to Junk." This is fast to do because the If the body contains lines are pre-written in the filter form; all you have to do is type in the offending word. So is the Action. The Move the message to line is already there, you just click on the line and then on the the folder. Tell the filter OK. You're done. I created 4 such filters in a few minutes.

I find this to be an effective way to rid myself of unwanted mail where I can't simply block a sender or a subject. I was getting multiple messages every day from people who want to sell me their services to improve my website ranking on Google, or other search engines. But they were from different people, and different subjects. I don't have a website, and I have nothing to sell, so I am of course not interested. I have no idea why I started getting this crap, but now I'm no longer bothered by it."

1) https://www.thunderbird.net/en-US/

It's not that I'm so smart, it's just that I stay with problems longer. Albert Einstein

Do You Use Two-Factor Authentication?
By Phil Sorrentino, Secretary & Newsletter Contributor
Sun City Center Computer Club
https://scccomputerclub.org/
philsorr (at) yahoo.com

If not, you might want to consider it for specific accounts if it is offered. Two-factor authentication is a way of adding an additional level of privacy to a computer account. When you set up an account, typically on a computer server, you assign a "User Name," which is not private, and a Password, which you are advised to keep private. This provides a certain level of privacy because to access your account, you must provide the User Name, which is not private, and the password, which is, hopefully, known only to you. This is probably all you need to do for most of your accounts. However, adding another level of privacy would be prudent to guarantee that you can access the account only for specific accounts. These accounts would be those that you would be very unhappy if someone else, or some other computer, could access and download or manipulate its contents. An account that contains very personal information or an account at a financial institution might be just this type of account.

Client-Server Architecture

Keep in mind the internet employs a Client-Server Architecture. Using this architecture, your account is on a server computer, not your home computer, tablet, or phone. These (client) devices only provide the ability to connect to the server and manipulate the account contents. So if someone else knew your User Name, which is not protected, and knew or stole or guessed your Password, which is hopefully protected, they could access the account and manipulate the contents. If it's a financial account, they could probably manipulate its value. Unfortunately, no matter how diligent you are in protecting your password, sometimes passwords become known to the bad guys, such as "hackers." If hackers get into your financial account, they can possibly use it for fraudulent financial transfers or payments, or worse, a password alone may not be enough. Even many services that don't offer two-factor authentication have instituted various checks on the computer attempting to use a particular server account, like sending an email to the email of record indicating a new computer is trying to access the account and asking, "Is this you?". If you are concerned about this, google "What happens if someone accesses my account" and see the possibilities. Nowadays, many services employ two-factor authentication to help guarantee that only the account owner can access a particular account.

Two-factor authentication is not a new concept. Banks have used a second form of identification for years, using ATMs to secure access to safe deposit boxes. When a bank customer visits a local automated teller machine (ATM), one authentication factor is the physical ATM card that the customer slides into the machine ("what you

Con't pg 7

have"). A second factor is the PIN the customer enters through the keypad ("what you know"). When you want to get into your safe deposit box, you have to provide the account number ("what you know") and a key ("what you have") before they will let you into the box.

Fortunately, many, if not all, financial institution servers provide the ability to use two-factor authentication. Two-factor authentication requires a second form of identification, which you typically have. Two-factor authentication increases the probability that the requester is who he says he is. The more factors used, the higher the likelihood that the requester is the account owner. Two-factor authentication is sometimes confused with "strong authentication," but these are different strategies. Soliciting multiple answers to challenge questions may be considered strong authentication.

However, unless the process also requires "what the user has" or "what the user is," it would not be regarded as two-factor authentication.

What you know + What you have = Positive Authentication

In general, authentication can be done by "what you know," like a password or pin, or "what you have, "like a badge or a smartphone, or "what you are," like a fingerprint or iris eye-print. (Some highly classified systems may require all three for authentication, which would involve possessing a password and a physical token used in conjunction with biometric data, such as a fingerprint, a voiceprint, or a retina scan.)

For most typical internet servers, the second form of identification is "what you have." The "what you have" can be a code sent to you by text, email, or phone; the account owner usually makes the choice. The code is typically a one-time-use series of six or so digits. Once the code is sent, you will have enough time to enter it into the screen that starts the authentication process. If email is selected, the server will send an email with the code to your email address of record on that server. Once you provide the correct code, you will be granted access to the account. If a voice phone call is selected, the call is made to the phone number on the record on that server. Once the phone call is answered, the digits are announced, and you can enter them on the screen that starts the process. If a text is selected, the text will be sent to the phone number of record on that server (ensure the phone number can receive texts). The code in the text can then be entered into the screen that starts the process.

Two-factor authentication adds an extra step to your login process, and depending on how the service has implemented it, it can be a minor inconvenience or a major annoyance. (And it also depends on your patience and willingness to spend the extra time to ensure higher security.) However, in the long run, using two-factor authentication improves the security of your private information, which is undoubtedly something we all want. So, take the time to set up two-factor authentication on at least all of your financial and very private accounts.