CAEUG Computers Are Easy User Group

Abort, Retry, Ignore....

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

June 2026
Volume XLII Issue 6

Confirmed meeting dates

2026

June 27

:: ::
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
:: ::

****

PER GLENSIDE Library (Masks are optional)

INFORMATION for Saturday June 27 start time in person at Library Board Room is 9:30am or at home Jitsi is 10:00am. There will be a meeting invitation e-mail Thursday evening before the Saturday meeting.

On Saturday June 27
Presentation will be various videos about
Internet Privacy

NEW MAIL ADDRESS!!! **NEW MAIL ADDRESS!!!**

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

****

Thank you! to all who paid the low $20.00 dues for 2026!
Your support helps pay for our APCUG membership and CAEUG website

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) Position OPEN
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

Lamp Post 291

June 2026
by John Spizzirri

The Decorah bald eaglets fledged **(1)**. They will stay close to the nest for a week or two until they realize that they have to feed themselves. Once that happens they use the nest as a place to rest.

1) https://is.gd/YAuMF0

In Lamp Post 250 I told you how to avoid paywalls hiding artilces using 12 foot ladder web site. Sad to say 12 foot ladder is no more. I found another web site that does the same thing called Bye Bye Paywall **(1)**. It has the added advantage in that is uses six web sites that it can try to bypass paywalls.

1) https://byebyepaywall.com/en/

Arstecnica **(1)** reported that Microsoft **(2)** found a worm called Crypto Clipper that uses infected USB drives to steal crypto coin credentials. Once an infected USB drive is plugged into a computer it installs some software that, "...monitors the contents of device clipboards for patterns consistent with wallet addresses or seed phrases. When found, the malware also takes five screenshots over a 10-second period. Both the credentials and the screenshots are then sent to the attacker through Tor." If Microsoft could find this, I would think that most if not all anti virus companies have detected it. Hopefully, they have been able to neutralize it. I have yet to see any word from any of those companies

Con't pg 3

about this threat, yet.

1) https://is.gd/k1l6vB
2) https://www.microsoft.com/

Taste of Home **(1)** web site has an interesting article about 'safe' symbols on kitchen-ware and house-ware. It is in your best interest to know what these symbols look like and what the unauthorized symbols mean.

1) https://www.tasteofhome.com/?p=2173250

Doxing is when a person's name and address is revealed on the Internet **(1)**. It comes from the term 'dropping docs' that means publishing documents that reveal personal information about someone that the person does not want revealed. This practice predates the Internet by quite a bit. It was used during the Revolutionary War **(2)** to show who the Tories and tax collectors were. Kristi Noem **(3)**, former Secretary of Homeland Security **(4)**, the agency responsible for Immigration and Customs Enforcement **(ICE 5)** wanted to make doxing ICE agents a criminal offense. These are the people that are dressed like pseudo-soldiers with their faces covered wearing sun glasses and ball caps to hide their identities because of their lawless behavior (unprovoked attacking unarmed civilians). Wired Magazine **(6)** pointed out, at the time, that some of these, not to bright bullies, doxed themselves by posting their names, addresses, pictures and more on LinkedIn **(7)**. A spokesperson for U.S. Customs and Border Protection **(8)** had the testicular fortitude to state that the reason that federal agents wear masks is because they were doxed (and not the other way around). All this happened last January. I waited to report on it until now due to the vindictive nature of the current administration and Brenden Carr **(9)**.

1) https://en.wikipedia.org/wiki/Doxing
2) https://is.gd/texFAs
3) https://is.gd/ac07nu
4) https://www.dhs.gov/
5) https://www.ice.gov/
6) https://is.gd/UGd7Aj
7) https://www.linkedin.com/
8) https://www.cbp.gov/
9) https://is.gd/a0emcQ

Illinois Governor J. B. Pritzker suspended tax breaks for data centers effective July first **(1)**. He is responding to the continuing protests about the negative effects of data centers on the local environments. Local officials want the data centers for the property taxes they generate

initially. The water use and energy costs seem not to matter to local officials. The legislature may try some compromising legislation or overrule the Governor.

1) https://wp.me/pftPyu-viB

Anthropic **(1)** disabled access to its AI **(2)** LLM (Large Language Model) **(3)** Claude **(4)** Fable 5 and Mythos 5. Fable and Mythos were banned for use by 'foreign nationals' by our government (Pete Hegseth). It is claimed that these two AI LLMs are a threat to our national security. If that is true, can we trust the makers of Fable and Mythos? How about Pete Hegseth? Exactly who has access to these LLMs? What kind of computers do they have access to and how do we know we can trust them with our national security? This story **(5)** is one of the most unsettling of the year, for me.

1) https://www.anthropic.com/
2) https://is.gd/bqZd2c
3) https://is.gd/ozjWGQ
4) https://is.gd/nNKeBH
5) https://wp.me/p5gGh3-B8l

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

Private Browsing: Is it all it's cracked up to be?
By Chris Taylor, President
Ottawa PC Users' Group, Ontario, Canada
https://opcug.ca
Published in Ottawa PC News (November 2023)
Editor: brigittelord (at) opcug.ca

For well over 10 years, web browsers have offered private browsing, designed to keep your browsing—well—private.

Google Chrome calls it an Incognito window, Firefox, Opera & Brave call it a Private window, and Microsoft Edge calls it an InPrivate window. The easiest way to get there is to right-click the browser's icon on the taskbar and choose the appropriate New... item from the pop-up context menu.

When in a private browsing window, browsing history, cookies & site data (such as images and contents of webpages), and information entered in forms are not saved to your computer. Other users on your computer will not be able to see your web browsing activities. When browsing, web servers won't

Con't pg 5

automatically recognize you as a returning user, and you won't be automatically signed into websites.

When you close a private browsing window, the browser discards site data and cookies created during that session. Note that you need to close the private browsing window to remove traces. Until you do, a simple click on the back button will return you to the previous page visited in that window.

Private browsing deactivates extensions. You can enable extensions in private browsing windows if you need them. For example, in Google Chrome, click the kebab menu ( ) at the top-right of the window. Choose Settings. Find the extension you want to allow in Incognito windows and click Details under that extension. Toggle on Allow in Incognito.

Private browsing is not a panacea
It does not prevent all tracking. While websites do not have the luxury of using cookies to track you, there are many other means of tracking. For example, a web server can know your operating system, browser version, extensions you have loaded, screen resolution, IP address, and more. These data items can be used to fingerprint and track you.

Private browsing does not prevent ads. It does not prevent malware. It does not hide where you are browsing from your ISP or employer.

As Gizmodo reported in October 2022, Even Google's Own Staff Thinks 'Incognito Mode' Isn't All It's Cracked Up to Be - https://gizmodo.com/google-incognito-mode-google-chrome-1849648071

Where is private browsing useful?
If you are using a computer at a public kiosk, it will prevent the next person using the computer from easily seeing where and what you browsed.

If you use multiple accounts on a single website, a private browsing window can help you keep things separate.

If you are using another person's computer, it can be helpful in making it less likely you leave traces behind.

Strangely, I have encountered shopping sites that required private browsing for the checkout process to work properly. I guess they didn't want to sell things to me all that badly.

For more information about private browsing, see https://en.wikipedia.org/wiki/Private_browsing.