CAEUG Computers Are Easy User Group

Abort, Retry, Ignore....

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

September 2023
Volume XXXIX Issue 9

Confirmed meeting dates

2023

Sept 30

Oct 28

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 **September 30th** 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 **September 30** presentation will have various short video presentations about Windows 11

October is Cybersecurity month.
Make sure your software is up to date. Stay safe.

Dues for 2023 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

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
president(at)caeug.net
V.P. (Programs) Roger Kinzie
Secretary Position OPEN
Treasurer Kathy Groce
Newsletter Kathy Groce
newslettereditor(at)caeug.net
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
Phone 6pm-9pm
630/858-6933

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 261

September 2023
by John Spizzirri

The Brooks Falls brown bear fishing (**1**) is starting to wind down. The fishing tactics have changed. Fewer bears sit on the falls. Bears sit on rocks in the riffles **(2)** and scan the water for fish. The same is true at the Kat's River view **(3)**. There are more sows with cubs. Loons can be seen and heard. River otters can be seen occasionally in the calmer waters.

1) **https://is.gd/5XSkeR**
2) **https://is.gd/8qsdz0**
3) **https://is.gd/BYn1NE**

Windows 11 comes with about nine themes. You can access themes by right clicking on the desktop and selecting Personalization then click Themes. You will be able to select a theme, light or dark mode, or just a desktop back ground picture. If you want to pick from more themes than the ones that are showing, click on the Browse Themes phrase at the lower right corner just below the themes. It opens themes in the Microsoft Store. I think that all the themes are free (at least for now). I gleaned most of this information at How To Geek **(1)**.

1) **https://is.gd/NjPbCh**

Con't pg 3

A quick way to get to the task manager in Windows 11 is **CTRL-Shift-ESC.**
Windows key + w opens Widgets menu.
Windows key + a opens the Quick Settings (WiFi on/off, BlueTooth connections, Airplane mode on/off, Screen Brightness control, Audio level control, plus other controls).
Windows key + n opens Notification menu and Calendar.
Windows key + z opens snap layouts for Windows layouts on the screen.
Windows key + ; open the emoji picker that includes gifs, symbols, and kamojis. When you wish to paste after copying, use the
Windows key + v to select anything that you have copied (Ctrl key + c) during this computer session.
Windows key + h to dictate to the PC in Word or Notepad.

To keep the main menu clutter free, right click on the start button, select Personalization then click Start. Turn off 'Show recently added apps' and 'Show recently opened items in Start, Jump Lists, and File Explorer'. To keep adware popups at bay, right click on the start button, select System then select Notifications. Scroll down and uncheck 'Get tips and suggestions when I use Windows'. On the left hand panel select Privacy and Security then select Windows Permissions. Select General, turn off 'Let apps show...', 'Let websites show...', 'Let Windows improve...', and 'Show me suggested....'. Select Speech, turn off speech recognition (you can still use dictation). Select diagnostic data, turn off all collection and erase all data previously collected. Select Activity History, uncheck 'Store my activity history on this device'

Volt Typhoon **(VT 1)** is a cyber actor (**2)** sponsored by the People's Republic of China **(PRC 3)**. VT is being hunted by the Five Eyes **(4)** consisting of the U.S. National Security Agency **(NSA 5)**, U.S. Cybersecurity and Infrastructure Security Agency **(CISA 6)**, U.S. Federal Bureau of Investigation **(FBI 7**), Australian Signals Directorate's Australian Cyber Security Centre **(ACSC 8)**, Communications Security Establishment's Canadian Centre for Cyber Security **(CCCS 9)**, New Zealand National Cyber Security Centre **(NCSC-NZ 10)**, and the United Kingdom National Cyber Security Centre **(NCSC-UK 11)**. VT is a serious threat to Western infrastructure. It works surreptitiously through common Window network controls to corrupt "the communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors." **(12)** That was according to Microsoft **(MS 13)**. VT is just one reason to keep Windows up to date. Do NOT use unsupported Windows versions on the Internet. Only login with a standard user privilege and not administrator rights. If you are the sole user of the PC, you should have at least two users created for your PC. One standard user and one administrator (with a common name so as to create confusion to a cracker). If the logon name you use every day has administrator rights, any cracker (including VT) and use your PC to do harm to you or the Internet at

large. Do Not give them a free hand.

1) **https://is.gd/CwkCQya**
2) **https://is.gd/yuFA5o**
3) **https://www.mfa.gov.cn/eng/**
4) **https://is.gd/bl10ED**
5) **https://www.nsa.gov/**
6) **https://www.cisa.gov/**
7) **https://www.fbi.gov/**
8) **https://is.gd/4rgOFC**
9) **https://www.cse-cst.gc.ca/en**
10) **https://www.ncsc.govt.nz/**
11) **https://www.ncsc.gov.uk/**
12) **https://www.microsoft.com/en-us/security/blog/?p=130214**
13) **https://www.microsoft.com/**

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

How Do I Remove a Virus from My Browser?

By David Kretchmar, Computer Technician
Sun City Summerlin Computer Club
www.scscc.club
dkretch (at) gmail.com

Our computer operating systems have become more secure, so developers of malware have turned their attention to a more vulnerable target, our web browsers.

Chrome, Edge, Firefox, Safari, and Opera are the browsers most of us use to connect to the Internet. All of these browsers can be infected by a redirect virus, despite their built-in security.

Redirect viruses, also known as hijackers, can make your online life very difficult
In this article, I'm going to describe the process of acquiring, identifying, and removing an infection from your browser. I'm going to focus on Google Chrome; the techniques are similar, yet slightly unique for each browser. Most users should be able to use the described procedures on their own systems, with small variations depending on the browser and underlying operating system (Windows, Apple, or some flavor of UNIX/Linux).

Redirect viruses can come from several sources.

Extensions
Hijackers can sometimes be "Trojan Horsed" in with browser extensions; extensions are small programs for a browser that serve the desired purpose, such as weather, price comparison, coupons, or productivity tools. If you install these extensions, you could unknowingly grant them the ability to influence your browser settings or change

Con't pg 5

your preferences such as your home page or your default search provider.
Extensions are usually the first place to examine if you suspect you might have an infection.

Spam emails
On at least a weekly basis I receive an email telling me that my account at Amazon, Facebook. eBay, PayPal, etc. have been frozen due to suspicious activity. The email contains a link to click on to resolve the problem. In reality, if I clicked on the link provided, my problems would be just starting. If you receive an email informing you of a problem with, for instance, your Amazon account, access your Amazon account the way you would normally if you think there might be a problem.

Social Media
Links from your Facebook or Twitter feed could also be rerouted in phishing, redirects, or browser hijacking. Facebook is notorious for allowing questionable items to appear in your feed. Some bad links might be posted by unsuspecting Facebook friends who find it easier to copy and paste or just click Share than to vet an item. And no, Costco is not going to send you a $50 voucher if you just take this survey revealing all sorts of personal information.

Free software downloads from unreliable sites.
Hijackers can get added along with free software downloads. Often web sites will offer a desirable program but try to trick the user into downloading malware. Always look at the address bar to make sure you are downloading software from the legitimate provider’s site.

Without realizing it, you could lose control of your browser by clicking on the wrong link on the wrong website.

Do I have a browser virus?
A browser virus on a PC or Mac is a browser hijacker that targets your browser. This type of malware is used to generate web traffic and collect information.

How do you find out if your browser has a virus? Here are the main symptoms:
- Your homepage redirects to a website different from what you expect.
- Unwanted extensions appearing in your browser (you might see icons at the top right side of your browser).

Con't pg 6

• Ads show up more often than they should, usually in unexpected places.
• Pop-ups and banners that advertise fake updates or software regularly appear.
• The link you click in search results redirects to dubious or possibly malicious websites.
• Your browser performance decreases dramatically no matter where you go on the Internet.

A virus can also ask you to update a program such as Adobe Flash Player or download any other tool (program) that would help you fix the problem it is creating. These warnings don't always mean that you have issues with the browser but should be suspect.

If you notice any of these signs, your computer browser is possibly infected with a virus.

Potential risks of a browser virus

As a browser hijacker, a pop-up virus is categorized as a potentially unwanted program (PUP). Once the malicious program attacks your computer, it starts modifying browser settings. For instance, it changes the default search engine and homepage, without asking for your permission.

The most serious problem created by having this virus is the ultimate invasion of your privacy; secretly harvesting as much of your personal information as possible to engage in identity theft. Some browser viruses are all about collecting personal details (IP address, location, searches, etc.) and sharing them with third parties. This may cause serious problems related to privacy and data security.

How to get rid of the browser virus

Delete unrecognized extensions

1. Go into your browser settings (in Chrome it is the three perpendicular dots at the upper right side of the browser).
2. Click on the Extensions tab.
3. Look for any extensions that shouldn't be there. If you find anything, select it and hit the Uninstall button to remove it.
4. Check your homepage and search engine settings

These settings appear in the settings area of your browser. In Chrome go into the browser settings and click on Settings. Make sure your homepage and default search engine are correct.

Additional things to check

1. Go to the Applications or Applications and Features folder and find any suspicious

software. It may disguise as the desired application, so search for anything you don't remember downloading. Also, note the install date to identify possible problems and look at the last program you downloaded before noticed problems.

2. Check your Downloads folder for items recently downloaded from the Internet for clues about the possible problematic vector that has introduced the malware into your browser.

3. Once you detect the malware, drag it to Trash and empty it, or delete it and then remove it from your Recycle Bin.

Get rid of every trace of malware

After the above steps, download and perform a Malwarebytes scan as well as a full scan with your installed virus protection to make sure no harmful PUPs are left on your system.

Conclusions and Recommendations

To avoid getting browser viruses, pay attention to the websites you visit, files you download, and apps you install. Avoid using third-party software downloaders and installers - they usually include PUPs. Never ignore the warnings if your browser alerts you that a website is not secure.

Still, it's always better to prevent the problem than to try to deal with it. Browse wisely!

Interesting Internet Finds - February 2021

By Steve Costello
scostello (at) sefcug.com

In the course of going through the more than 300 RSS feeds, I often run across things that I think might be of interest to other user group members. The following are some items I found interesting during January 2021.

The Two Types Of Cloud Data Threats And How You Protect Yourself

https://askleo.com/two-cloud-data-threats/

Leo Notenboom explains the two types of threats for having your data in the cloud and suggestions for protecting yourself from them. (Note: I have been using the cloud for years without any problems, but I only keep data that is recent and encrypted.)

How To Use Linux Live CD To Back Up Data From Windows PC

https://www.maketecheasier.com/rescue-your-pc-with-linux-live-cd/

If you use a Windows PC it is a matter of when not if you will have a problem being unable to access the PC. This article explains how to use a Linux Live CD to perform a rescue of your data.

Change Your Secret Router Password

https://cynmackley.com/2021/01/19/change-your-secret-router-password/

Something most people overlook for security is changing the router password. Cyn explains how to change this password, though the specifics vary depending upon the

 Con't pg 8

specific router.

Does Your IP Address Expose Your Home Address?

https://askbobrankin.com/does_your_ip_address_expose_your_home_address.html

I have heard this question asked at many user group meetings. This post from Bob Rankin gives the best answers I have seen so far.

What Linux Is And Why It Has Persisted?

https://www.askwoody.com/newsletter/free-edition-what-linux-is-and-why-it-has-persisted/

This article is from the free edition of the AskWoody newsletter. The article provides information about what Linux is and why it is still around and used. (Note: I subscribe to the paid edition, which contains mostly Windows-related articles.)

Why You Should Delete Emails Instead Of Archiving Them

https://www.howtogeek.com/709693/why-you-should-delete-emails-instead-of-archiving-them/

This is something I have not thought about until reading this. I have been using Gmail since 2005, so have many emails that are no longer necessary to have, and am working to clean them out to increase my storage capacity. I was surprised to have so much unnecessary stuff saved.

****

“Default” apps or programs in Windows

By Jim Cerny, Vice President, Education Chair, and Forums Coordinator
Sarasota Technology Users Group
https://thestug.org/
jimcerny123 (at) gmail.com

Most of us know what “default” means when talking about computers or technology. But in case you forgot, “default” means: “This is what you get until you change it to something else.”

Computer technology is full of defaults (you may have also heard the term “default settings”). The best way to understand this concept is to use an example. Suppose you are writing a document using Microsoft Word (or some other word processor app); you can start typing words in your document immediately without selecting the FONT or FONT SIZE first. That’s because the app has a default font setting (such as “Times New Roman” in the font box and “12” in the font size box). Yes, you can go to those boxes and pick any other font size you want, but the app already starts with something in the box. That’s the default. Other examples in everyday life are thermometers using Fahrenheit, but you can change it to Centigrade, or your speedometer from miles-per-hour to kilometers-per-hour. If you don’t like the default setting, change it to something else.

Con't pg 9

Let’s go one step further and discuss using that essential Windows app called “File Explorer.” With file explorer, you can find any file on your computer. And when you find the file you want, you can OPEN that file by double-clicking on the file name. Of course, there are many different types of files – photo files, document files, spreadsheet files, and many more. So, when you double-click on a file name in Microsoft File Explorer, Windows uses the DEFAULT app to open that file. Let’s take a photo file as an example. In File Explorer, if I double-click on a photo file (a file type of “.jpg”), it will open the photo in the Windows Photo Viewer app, and I can see the photo. But if I want to open that photo in a different app, say the Windows Paint app, I have to open that app first and use the app to open the photo file.

It turns out that your Windows computer already has selected specific apps for many file types to use as the default apps. And it’s no surprise that your default apps are Windows or Microsoft apps.

Here is one more example. If you click on a web page link, your computer will open and use the default web browser to go to that web page, probably Microsoft Edge. But you can change your default web browser to Google Chrome, Safari, Firefox, or any other browser you want. To do this, click on the Windows start button in the far bottom left corner of your desktop, type in “Default apps” in the search results, select “Default apps,” and then click on the Web browser to see a list of the web browser apps you have and click on the one you want as your new default browser.

This is how to change ANY default app on your computer to a different one. You can also get to the “default apps” area through your computer “settings” or “control panel.” In addition, you can change the default app used for different file types. It is not difficult to do this. For example, to learn how to use Google search on the internet, enter “How do I change my default app for .jpg file types” or anything else.

The benefit of knowing about default apps is that you will understand why a specific app is used when you click on something to open it. This also explains the question you sometimes get “Select the app you want to use to open this file,” which could mean you may not have an app that can open it. The best way to make sure you use the specific app to open a file is to open the app first and use the app to select the file. Unfortunately, the default is not the de-fault of your computer!