CAEUG Computers Are Easy User Group

Abort,
Retry,
Ignore....

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

July 2024
Volume XXXX Issue 7

Confirmed meeting dates

2024

July 27

:: ::

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 July 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 July presentation various short video presentations

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

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 270
July 2024
by John Spizzirri

The brown bear cams **(1, 2, 3, 4, 5, 6)** at Brooks Falls in Katmai National Park, Alaska is live. The bears are out of hibernation. The salmon have started their trek up the river to spaun. The fishing has started.

1) https://is.gd/5XSkeR
2) https://is.gd/8qsdz0
3) https://is.gd/5RsMdk
4) https://is.gd/BYn1NE
5) https://is.gd/c7jg58
6) https://is.gd/ERw674

With the amount of recent and predicted activity on the sun, it might be a good idea to keep the Aurora cam sites in your favorites. The Northern Lights (Aurora Borealis) cam at Churchill, Manitoba, Canada **(1)** is in the Central Time zone as is the polar bear site **(2)**. If you stay up really late or get up early, try the Alaska Borealis cams **(3)**. Two places to try offer various cams

Con't pg 3

from around the world **(4, 5)**. To check on the space weather (for aurora forecasts) try here **(6)** and NASA **(7)**.

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

I hope you did not try to pay a bill on line, take an airline flight, have to make a 911 call, or get critical care in a hospital the day Trump accepted the Republican nomination for President of the United States. That's the day that Cloudstrike **(1)** released a buggy security update to Windows **(2)** based software that paralized a sizable chunk of the nation with the dreaded Blue Screan of Death **(BSOD 3)**. If you own Cloudstrike stock, I fear it is too late to sell. They will soon be sued out of their major player status. The company that should be sued but will have no ill effect is Microsoft. Why a corporation has to use the same OS is beyond me. This one point of failure is so spectacular as seen in this debacle I would think it would wake up some system administrators to look to open source for an alternative. Cloudzero **(4)** a cost optimizatioon platform estimates the damages of this failure as of Friday morning at $24 billion. Microsoft has a number of help screens that assist in the repair of the problem. Here **(5)** is one of them. You will note that this process must be done to each screen (PC or Virtual Machine VM) that is affected. Rebooting must be done (up to 15 times) as part of this process. When your staff is paid $25 to $75 per hour, do you want them watching a PC or VM rebooting up to 15 times which may or may not work before trying another gambit? How many PCs and VMs do you have to run your business; 100, 500, 1000, 5000? How many staffers do you have; 10, 20, 30? How many staffers can you hire? At what price? The headache gets worse and worse. And to think this was just a mistake and not some evil plan or attack.

1) **https://is.gd/9fSmBr**
2) **https://is.gd/ba5cLN**
3) **https://is.gd/3gqKq3**
4) **https://www.cloudzero.com/**
5) **https://is.gd/HvqzOH**

CordCutter News reports **(1)** that Netflix **(2)** is dumping is low cost ad free streaming service. There are a lot of people who do not like the news **(3, 4, 5, 6)**. I found a couple of people who had solutions **(7, 8)**.

1) **https://cordcuttersnews.com/?p=142239**
2) **https://www.netflix.com/**

Con't pg 4

3) **https://is.gd/BbflgZ**
4) **https://www.techdirt.com/?p=444540**
5) **https://wp.me/pc8hbN-1lAvV1**
6) **https://is.gd/GFN7r4**
7) **https://www.youtube.com/watch?v=RE6s6J7glNI**
8) **https://www.youtube.com/watch?v=Dxl9ggz5ngE**

On July 12, 2024, AT&T **(1)** reported that "a third-party cloud platform exposed the call and text records of nearly all its cellular customers. **(2)**" They became aware of this in April and are working with law enforcement **(FBI 3)** to apprehend the guilty parties (one is already in custody). This release of data includes "AT&T records of calls and texts of nearly all of AT&T's cellular customers, customers of mobile virtual network operators using AT&T's wireless network, as well as AT&T's landline customers who interacted with those cellular numbers..." "While the data does not include customer names, there are often ways, using publicly available online tools, to find the name associated with a specific telephone number," an AT&T filing with the Securities and Exchange Commission said. If you have an AT&T account and wish to check if your data has been affected, you can go here **(4)** to check. This is the result of a cracker attacking a business that may or may not affect your data and life. Please note how the company and law enforcement drag their feet in doing anything about it (even telling you).

1) **https://www.att.com/**
2) **https://arstechnica.com/?p=2036854**
3) **https://www.fbi.gov/**
4) **https://is.gd/XglMGq**

Reader' Digest **(1)** contacted the Electronic Privacy Information Center **(EPIC 2)** to find out what your smart phone knows about you. The question should be what doesn't my smart phone know about me. To start with is your location, all sorts of health information, possibly your religion (location of the church, synagogue, or mosque), sexual orientation, contacts, voice recordings, photos, phone calls, search history, apps, and behavior. There are other apps that both Android and iPhone devices use to collect large amounts of data from their users. Reader's Digest **(3)** and the Federal Trade Commission **(4)** have tips on how to protect yourself from this spying behavior of your phone.

1) **https://www.rd.com/?p=632180**
2) **https://epic.org/**
3) **https://www.rd.com/article/tech-tips/**
4) **https://consumer.ftc.gov/node/77456**

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

Cyber Security

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

Recently, SCSCC Vice President Tom Burt provided members with a link to an interesting article from Malwarebytes about cyber security: https://www.malwarebytes.com/blog/news/2023/10/the-3-crucial-security-steps-people-should-do-but-dont

Malwarebytes (2-week free or trial version) is an excellent product that other SCSCC technicians and I frequently use to search for malware and other potential PUPs (potentially unwanted programs) on computers. Malwarebytes professional is their paid-for real-time protection sold for $30 - $45 per computer per year.

“Everyone’s afraid of the internet and no one’s sure what to do about it.”

The essential point of the article was that many internet users employ "dismal cybersecurity practices" and are too lax in implementing and using security measures designed to keep them safe and secure. Some experts estimate that one-third of individuals experienced a security breach within the past year. This sounds reasonable based on my personal experience. Still, I also find it comforting that older adults (Baby Boomers) are estimated to be four times less likely to experience a security issue than younger users. I'm unsure if we are more careful than younger users or if we do less online.

While anything that makes people aware of the dangers that stalk all of us online is valuable, I disagree with two of the three primary points raised in the article. Malwarebytes provided the article, and since they sell subscriptions to their products to stay in business, it is arguably in their interest to frighten people, who then will be more likely to become customers.

In the following paragraphs, I will discuss the essential three points made in the article that I find misleading, outright untrue, and primarily true (multi-factor authorization).

1. **"Just 35 percent of people use antivirus software."**

I call BS on this. It is rare for me to come across a computer that has no antivirus software running. Microsoft Windows Defender runs by default on Windows computers and does not have to be turned on by the user. This is by far the antivirus software utilized by most individuals, and it has the advantage of having no cost beyond what a user initially pays for a Windows PC.

In addition to being "free," the Microsoft Windows Defender program code is

Con't pg 6

updated at least monthly. The monthly security update release is scheduled for the second Tuesday of each month. The Microsoft Windows Defender virus intelligence database is updated almost daily in case of newly discovered threats, also known as a 0-day or zero-day vulnerabilities. The term zero-day refers to the fact that the vendor has just learned of the flaw – which means they have zero days to address it.

It might be that only 35% of users subscribe to an antivirus software tool other than Microsoft Windows Defender. Certainly, Malwarebytes would like you to buy their product, but the article states an untruth when it says that only 35% of computers are protected.

I believe Microsoft Windows Defender provides excellent protection for most users. The modern version of this security package was implemented with Windows 10 in 2015 and is further improved with Windows 11. I have examined hundreds of computers since 2015 and have never had to remove a virus protected by Microsoft Windows Defender. Before 2015, our club's hardware technicians spent as much as half our time at our Tuesday Repair SIG removing viruses from systems, but this work is no longer necessary.

2. **"Just 15 percent of people use a password manager."**

Again, I call BS on this. It is common for club members who come to the Tuesday Repair SIG when asked for their password to, for instance, their Google account to state, "I don't have a password; I just click on Gmail, and it appears." They are unknowingly and effortlessly using a password manager.

Without a password, you cannot use an application such as Gmail or any other mail program. Many users set up a password for Gmail or any other applications when they initiate use of that service or have this done for them by whomever is helping to set up their device.

Many users forget they have the required password because their browser's built-in password manager enters it automatically and seamlessly. Google, Edge, Firefox, and Safari all have integrated password managers with features like autofill and a password generator. They can also store credit cards and other personal information, which makes your online life more manageable. Smartphone operating systems on the Apple iPhone, Samsung Galaxy, etc. also store user credentials.

A password generator will create a unique password, such as "8X! 4tZ7pas@vFyY" which is impossible to guess and memorize. A password manager best utilizes this bizarre string of characters. I have seen people write down and manually enter a generated password, but obviously, it is tedious and often takes multiple tries.

Are passwords saved by browsers secure?

Google states, "Google Password Manager and the passwords it generates are considered safe compared to similar password managers. Google uses military-grade encryption to protect your usernames, passwords, and payment information."

Microsoft states, "Microsoft Edge stores passwords encrypted on disk. They're encrypted using AES, and the encryption key is saved in an operating system (OS) storage area."

Firefox states, "Firefox Desktop uses simple cryptography to obscure your passwords. Mozilla cannot see passwords, but Firefox Desktop decrypts the password locally so that it can enter them into form fields."

In other words, the "free" password managers built into browsers and operating systems use security schemes that are like paid password managers. Naturally, marketers of these paid-for third-party services, such as Nordpass, Norton, OneLogin, and LastPass, claim built-in password managers are vulnerable.

Unfortunately, third-party password managers have been hacked, severely compromising user information. OneLogin was hacked in 2017, and LastPass was hacked in 2022. In March 2023, LastPass stated that the breach resulted in unauthorized and unknown users gaining full access to customers' vault data, including personal information like usernames and passwords.

Yet third-party password managers urge users to buy their product rather than depend on the security built into browsers and operating systems. But any account or device can be hacked.

Unless you write down your passwords using a pencil and paper, you must trust someone and use a password manager. I would rather trust a massive entity like Google, Microsoft, or Apple over a relatively tiny software provider. Even more prominent entities, such as Norton, have been subject to internal dishonesty and theft of client data.

3. Use multi-factor authentication (MFA)

This is NOT BS. Multi-factor authentication (MFA) requires users to provide at least two of three categories of authentication to access an account.

- Knowledge: a password or PIN code,
- Possessions factor: a secondary device (i.e., Smartphone) or account you

Con't pg 8

have, in addition to a knowledge factor.

- Biometrics: any part of the human body that can be offered for verification, such as fingerprints or facial recognition.

I only have one account, Interactive Brokers, that requires MFA. When I want to access my account, a notification is sent to my iPhone, which opens the Interactive Brokers application on my phone and identifies me using facial recognition. Thus, all three factors of MFA are utilized, which is about as good a set of authentications as you will find today.

Disadvantages of MFA

The second factor, the secondary device or account, is much stronger when a separate device is utilized. Many MFA schemes send a code to an email account, which is useless when that happens to be the account you are attempting to access. Using only an email account for secondary authentication rather than a discrete device, such as your Smartphone, provides weaker security.

MFA can lock you out of your account when your discreet device (phone) is unavailable, runs out of juice, or lacks an internet or cellular connection.

Conclusions and Recommendations

Microsoft Windows Defender runs by default on Windows computers and does not have to be turned on by the user. Microsoft Windows Defender provides excellent antivirus protection.

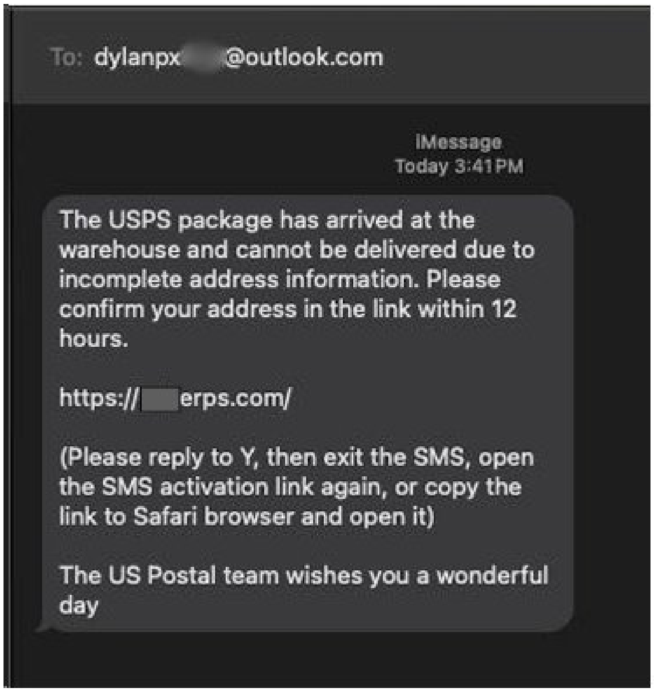
The password managers provided by browsers and operating systems are reasonably secure. I believe they are similar in security compared to password managers offered by third-party vendors, maybe better. These credentials operate seamlessly with the operating system or browser, making for a much smoother internet experience.

Multi-factor authentication is the way to go if you want absolute internet security. Using the three categories of authentication, knowledge, possession, and biometrics provides some of the best security available today.

Another Day. Another Scam. Don’t Fall for it.

By Kurt Jefferson, Editor, Central Kentucky Computer Society
https://newsite.ckcs.org/
lextown77 (@) mymetronet.net

I wonder how many Americans this very minute are being taken for a ride and giving away their personal information to a criminal. You might be surprised. At all hours of the day, people are turning over credit card numbers and more to thugs.



To: dylanpx[redacted]@outlook.com

iMessage
Today 3:41 PM

The USPS package has arrived at the warehouse and cannot be delivered due to incomplete address information. Please confirm your address in the link within 12 hours.

https://[redacted]erps.com/

(Please reply to Y, then exit the SMS, open the SMS activation link again, or copy the link to Safari browser and open it)

The US Postal team wishes you a wonderful day

As Aura writes, “When Mary Anne May received a text from UPS on the day after Mother’s Day, she assumed a family member sent her a gift that she wasn’t home to receive. But when she clicked on the link in the text to reschedule the delivery, and was asked for her credit card number, she started to get suspicious.

While Mary Anne’s caution was well-founded, millions of Americans have fallen victim to package delivery scams like this one.”

In recent days, I’ve received a number of bogus text messages on my phone. I simply report them as junk and delete them.

Here’s an example. The bogus text message alerts me that the US Postal Service is holding a package at its “warehouse” and cannot deliver it because it lacks complete street address details. Look who supposedly sent the text. It’s from a guy named Dylan. This is the first red flag. Think about it. USPS will never text you using a bogus email address starting with “dylan.”

Second, the letter carrier has been delivering mail and Amazon packages to my house for years. USPS doesn’t have my address? Then who’s the guy who’s been delivering junk mail to my mailbox for years?

Third, the USPS doesn’t have “warehouses.” They don’t use that phrase. The USPS has distribution centers. And I’m very glad to know that the bogus US Postal team is wishing me a wonderful day! Finally, the USPS doesn’t use bogus web addresses, as shown in the text. A legitimate message would read usps.com or something similar.

If I click on the link shown in the text, I’ll get a website where I can easily enter my credit card number to be scammed by Dylan or whoever is trying to turn me into a victim. Hey Dylan, have a wonderful day!