CAEUG Computers Are Easy User Group

Abort, Retry, Ignore....

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

August 2021
Volume XXXIX Issue 8

Confirmed meeting dates

Aug 28
Sept 25
Oct 23

Zoom meeting 10:00am

:: ::

Check website for dates and meeting info

:: ::

Mailing address:
CAEUG
P.O. Box 3150
Glen Ellyn, IL 60138

:: ::

MEETING will be held using Zoom until further notice

****

PER GLENSIDE WEBSITE As a precaution, all summer programming will be virtual or held outside. Participants will be required to wear masks and socially distance. Meeting rooms are not available to meet CAEUG needs.

UPDATED MEETING INFORMATION
* * * Saturday August 28, 2021 * * *
4th Saturday at 10 AM via Zoom.
A meeting where you get to stay at home.

There will be a meeting invitation e-mail Thursday evening before the Zoom meeting on Saturday morning at 10:00

Our August 28, 2021
An APCUG video on how to make your photos look better using GIMP by Art Gresham, Editor, Under the Computer Hood User Group.

REMINDER: $20.00 Membership dues for 2021 are due.
Mail dues to CAEUG, P.O. Box 3150, Glen Ellyn, IL 60138

****

Table of Contents

Join CAEUG meeting from Home, Stay Safe!!!!
Stay tuned for updates!!!

Lamp Post 238
August 2021
by John Spizzirri

The brown bear cameras at Brooks Falls in Katmai National Park, Alaska are on **(1)**, but they are solar powered. When it is cloudy for a few days, the cameras go off line and highlights are displayed until enough power is reached to restore live coverage. The late summer salmon run is exciting. The bears are taking as many fish as their bellies can hold and even an occasional wolf will grab a fish. It will continue through September. There is a random dust up between sows for the best fishing spots. Generally, there is not bloodshed.

1) https://is.gd/5XSkeR

Sometime around the 8th of August an unknown cracker or cracking group offered 30 million individuals information claiming it was from a T-Mobile database and asking about $270,000 in the form of six Bitcoins. Motherboard broke the story **(1, 2, 3)**. T-Mobile has 7.8 million current customers and 40.1 million former or prospective customers records that have been cracked. This affects, T-Mobile, Boost, Sprint, and Metro customers. Supposedly, former Boost, Sprint, and Metro customers are not involved **(4, 5)**. I used to have a T-Mobile cell phone, thus my personal information is at risk. If you have EVER had a T-Mobile cell phone, your personal data is also at risk. Per the T-Mobile web site **(6, 7)** the data that was accessed was names, drivers' licenses, government identification numbers, Social Security numbers, dates of birth, T-Mobile prepaid PINs, addresses, unique IMEI numbers, and phone number(s). The data NOT accessed was personal financial or payment information, credit or debit card information, account numbers, or account passwords. At least they kept the financials separate. The site reports that T-Mobile found out about the crack on August 17, 2021. It does not say when the crack actually happened. It says that current customers can get McAfee ID Theft Protection for two years. That doesn't help former or prospective customers. The crackers have enough information to steal identities. This information can be sold to others MULTIPLE times. Check your credit at Experian **(8)**, Equifax **(9)**, and Transunion **(10)**. Freeze or lock your credit (its free to do) while you are there so that no one can open a credit account in your name or mortgage your home without your knowledge.

1) https://is.gd/T5jmPN
2) https://is.gd/qESFbV
3) https://is.gd/aWMi4r
4) https://techcrunch.com/?p=2191033
5) https://is.gd/65TQGr
6) https://is.gd/02ok6A

Con't pg 3

7) https://is.gd/pY4Lhb
8) https://www.experian.com/
9) https://www.equifax.com/personal/
10) https://www.transunion.com/

If you are involved in cryptocurrency trading or investing, you already know that on August 10, 2021 a cracker dubbed 'Mr. White Hat' by Poly Network **(1)**, the company he victimized, stole $610 million in various cryptocurrencies **(2)**. The next day he (? probably male) began returning the money **(3)**. It took some negotiations but all the money was returned **(4**). 'Mr. White Hat' was given a $500,000 reward for returning what he stole **(5).** He was also offered the position of 'Chief Security Advisor' to help stop future cracks **(6)**. This story is just incredible. Kevin Mitnick **(7)**, Matthew Bevan **(8)**, Kevin Poulsen **(9)**, and Jonathan James **(10)** all are infamous crackers. One is dead. One is in prison. One owns a Cybersecurity company. One writes for The Daily Beast **(11)**, an on line newspaper. Most crackers spend some time in jail or house arrest. A very few actually turn their knowledge of computers into a livelihood. This person (probably male but not necessarily) gets a reward and a job for stealing money in a clever way. I jsut blows the mind.

1) https://poly.network/
2) https://is.gd/2HTiEk
3) https://is.gd/kmkrOo
4) https://beincrypto.com/?p=150667
5) https://www.bbc.com/news/business-58193396
6) https://is.gd/GY3h84
7) https://en.wikipedia.org/wiki/Kevin_Mitnick
8) https://en.wikipedia.org/wiki/Mathew_Bevan
9) https://en.wikipedia.org/wiki/Kevin_Poulsen
10) https://en.wikipedia.org/wiki/Jonathan_James
11) https://www.thedailybeast.com/

Artificial Intelligence **(AI (1))** is moving into medicine in a big way. It is being used to analyze X-rays CTs, mammograms, and other medical imaging (MRI?). Motherboard reported **(2)** that in the analysis the AI was also able to determine a patient's race. The doctors and computer scientists tried to isolate a reason for the accurate determination but were unable to understand how the machine devined race from images that contained no significant indicators. This is worrisome in that it can lead to bias in health care based on how care was handled in the past. Stephen Hawking **(3)**, the British physicist, used AI to communicate due to his amyotrophic lateral sclerosis **(ALS (4))** affliction. He 'feared' thinking computers that could do more than the computers that assisted him. He thought that they (AI computers) would perhaps destroy the human race.

1) https://is.gd/bqZd2c

Con't pg 4

2) https://is.gd/WwIrBV
3) https://en.wikipedia.org/wiki/Stephen_Hawking
4) https://is.gd/eguBpE

I found this graph of world history that is very interesting **(1)**.

1) https://is.gd/9BfZDV

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

President's Corner
Do You Trust Your Technology?
by Greg Skalka, President
Under the Computer Hood User Group
www.uchug.org
president (at) uchug.org

Our world runs on technology, yet many of our most contentious disagreements involve whether certain technologies can be trusted, or whether society can be trusted to use them correctly. Is climate change real and man-made? Is nuclear power dangerous? Are electronic voting machines accurate? Are vaccines safe? Does cell phone use cause cancer? Is it time to put on a tinfoil hat?

A strict application of the scientific method should be able to answer our questions and reveal the truth, but only if we all trust science. Unfortunately, with humans involved, there are biases, conflicts of interest, and preferences for one outcome over another. Another problem is that humans are imperfect, and so everything we make and do is also imperfect. Nothing we create is all good; there are always downsides to everything. Often the detrimental aspects of some new thing are not fully realized until much later. Asbestos seemed like a useful fireproofing technology until its toxicity became apparent. When the good aspects outweigh the bad (in some subjective determination), the tech is beneficial. Things are usually not black and white, however, so it is left to individuals and to society to judge their worth.

How we weigh the advantages and costs can be based on reputable information, but it can also come from rumors, false narratives, and speculation. Good things can get bad reputations (like vaccines), while bad things can get marketed as desirable (like tobacco products).

At the individual level, we all have choices to make concerning which technologies we trust and which we do not; which are worth the cost, and which should be avoided. Everyone approaches this differently, bringing our standards, biases, concerns, and experiences. Usually, the benefits are apparent, but the downsides of a particular technology are often hidden and

Con't pg 5

difficult to confirm. They usually involve aspects of safety and security, and it is very difficult to prove something is completely free of risk. The risks are generally to our personal and financial data. Can we get hacked? Can we get tracked? Is someone able to steal from us, or just accumulate more information about us than we'd like? Differences of opinion on these risks can lead to things that are popular with many being shunned by some.

There are lots of examples of mainstream technologies that are not trusted by some nominally rational people. I have some relatives that don't feel safe flying and now only travel by car, bus, or train (though they had traveled by plane in the past). I feel from its safety record that flying is generally safe enough, but have never questioned them on why they hold this view. John Madden, the former football coach, and sportscaster is reportedly afraid of flying and used a bus to travel to games. Some attribute his fear to a Cal Poly football team plane crash in 1960. I am not aware of any specific incident that would be the cause of my relatives' concern; they obviously must have a point of view different from mine on this.

I didn't think much about these differences in points of view until the start of the pandemic last year when I found some good friends who refused to use Zoom. I had set up a personal Zoom account in 2015 to use for some purpose related to UCHUG but never used it much. That changed greatly in March 2020, when we were forced to hold our board meeting virtually on Zoom. Since then, with the help of APCUG, we have been able to use their paid Zoom accounts to hold all our board and general meetings. There are some members we have not seen during this time, but we don't know why. I am aware of security concerns about Zoom but have researched them, and now have used it so much that I feel it can be trusted.

Before the pandemic, I met for lunch periodically with a group of longtime friends that I worked with at one time or another. After we could no longer meet in person due to COVID, I set up Zoom virtual lunch meetings so that we could stay in touch. Many in this group participated, but some would not; they were concerned about the security issues and "just didn't do Zoom." This is unfortunate as I would like to see more of them. I periodically remind them that they could join our Zoom lunches, but I'm always rebuffed. I'm starting to feel like I'm trying to talk them into using heroin. I don't think they are paranoid, as there are other things that these friends do that I find too risky.

There are a few popular things that I don't trust at this point. One is social networks. While I do have an account on LinkedIn (for job search and career purposes), I've never had a Facebook or Twitter account. I don't have any interest in them, and since I do have security and privacy concerns about participating in these sites, I just don't. There are no doubt some things I miss out on by avoiding social networks. My church has a private social network that would probably provide useful information, but my feelings about Facebook

Con't pg 6

have kept me from investigating it further.

Some people don't trust online banking and bill payment. I once felt that way. While I do still have security concerns, the overwhelming convenience of these services has won me over. I take every precaution I can to keep my online financial activities secure, and so feel my use is safe enough. I sure wouldn't want to go back to banking in person or by phone or having to mail paper checks in for payments. The postal system seems less secure than it used to, so mail theft of my paper statements now seems a greater risk than an online breach.

I also have reservations about password managers. I have less distrust in them now but originally feared that if they were not secure and could be hacked, all your passwords would then be vulnerable. I developed my own process for managing passwords and prefer it, but would recommend a password manager to others at this point

Voice-operated assistants (or smart speakers) can be very useful, but there are certainly privacy concerns to consider in their use. While I have several Amazon Alexa devices, I don't trust them fully. I realize I am trading some loss of privacy for their convenience. It is the same with Amazon in general, and with Google. I love Google Maps but have concerns about all the location data I am providing when I use it. It is always a risk/reward evaluation for each service; there are some Google services I don't feel are worth the risk, and so don't use them.

A smart or connected home can be a concern for some. I have a lot of smart home devices that I feel are fairly benign, like smart lights, thermostats, and cameras. While I agree it would be handy, I'm not trusting enough to consider a smart lock for my home just yet. I was once very concerned about home Wi-Fi and kept it disabled when not using it directly. As I found reasons to use it more and hardened my home network with more secure equipment and practices, I became more trusting. Still, the majority of my home computers and the ones I use for my most sensitive computing are on my wired network.

Antivirus is something I've become less trusting of. After research and consideration, I'm now in agreement with those that believe that any external security program opens holes in the operating system and thus increases risk. I'm now using the security built into Windows 10, rather than an external antivirus program (and saving money). I am much more suspicious of security and "cleaning" programs now, as some exhibit malware-like behaviors.

And then there is Windows itself. Some don't trust Microsoft and prefer alternatives like Linux or Apple's products. I don't trust Microsoft on everything, but since I must live in a Windows world at work, I find it easiest to stick with the adversary I know best. Linux seems like a lot more work, and since I don't

Con't pg 7

trust Apple any more than Microsoft, why should I pay a lot more for a computer I'm still concerned about?

No matter what technology you consider, there is probably some way it can be misused, subverted, or hacked. Each of us must consider the benefits against the risks when personally using any tech product or service. Those considerations must be made with the best, most accurate, and unbiased information available. We can't depend on the tech vendors or the government to protect us from harm; we must be our defenders. Perhaps the best we can hope for with our tech is not trust, but a truce.

President's Corner
How Reliable is Reliable Enough?
by Greg Skalka, President, Under the Computer Hood User Group
www.uchug.org president (at) uchug.org

Google defines reliability as consistently good in quality or performance; able to be trusted. We all want our technology to perform well, as we depend on it more and more in our lives. In placing a call, turning on our lights, driving to the store, checking our bank balance, or taking a commercial flight, we all want (and perhaps expect) 100% reliability in our experiences with technology. Nothing can be completely dependable, however, and no matter what we expect, tech failures happen. Reliability can be regulated by government agencies, specified by standards, or simply provided "as-is" by the manufacturer. In the end, it is up to each of us to decide if the reliability levels we get meet our needs.

Most large companies now use an ISO 9000-based quality management system to demonstrate their ability to provide quality products and services that consistently meet their customer's needs. The basics boil down to 'say what you do' and 'do what you say'. Unfortunately, for the customer, the issue is often that not enough is said, and the only standard the customer has is their expectations about quality and reliability; these usually wind up being different from the vendor's.

I have a lot of smart home devices. Many companies make and support products and systems to remotely control lights and devices in your home. You can control them remotely through an app on your smartphone or tablet, or through an Amazon Alexa or Google Home Assistant device. In addition to immediate control, your items can be programmed to turn on and off in a scheduled manner. The manufacturers portray these smart devices as simple and easy to use, so the consumer might assume they are reliable. Unfortunately, they are fairly complex and sometimes not so reliable.

I'm typically up and out of the house to work well before my wife is awake. To make my workday mornings easier (and safer, especially in the darker mornings of winter), I program lights downstairs to come on just before I would come out of our bedroom. This gives me a little bit of light to help me see when going down the stairs before

Con't pg 8

dawn. I use a Belkin Wemo smart plug, with a family room lamp plugged into it, to give me some of that light. I've programmed the ON time in the Wemo app so that at my selected time the Belkin servers send a message over the internet and through my Wi-Fi to the smart plug to turn on. Once I get downstairs, I turn the light off manually with our Amazon Echo Show as quietly as possible, using the screen icons rather than voice control. In this case, the OFF command is sent from my Show over the internet to Amazon's servers, and then passed to the Belkin servers and back over the internet to my Wemo smart plug.

This seems like a lot of complex communications, but it has worked very reliably over the four months since I set this up. Last week, however, it didn't do so well, failing to turn off correctly on two different days. On the first day, Alexa could not turn the light off; I had to go into the Wemo app to do it. On another day, even the Wemo app could not turn the light off, as the smart plug appeared as inactive in the app. I finally had to resort to pressing the button on the smart plug to shut it off. In both cases, everything worked fine again after a short time. I was happy to see it working, but was reminded of the engineering saying "Problems that go away by themselves can come back by themselves."

Though I was not happy that the smart plug worked unreliably those two days, was there anyone I could blame? Perhaps not, as Belkin and Amazon had said I could control my light in this way, but they didn't say it was guaranteed to work 100% of the time. That it had worked reliably all but two days in four months is in reality pretty good, considering the plug cost only $20 (and the Echo Show cost $50).

This brings up one key factor in the reliability equation: high reliability generally costs more. The successful landing of the NASA Perseverance Mars rover last week was a tremendous technical achievement, but it came at a cost of around $2.5 billion. That kind of money can buy a lot of reliability, however. The NASA Opportunity rover, launched in 2003, cost $400 million and had a planned mission duration on Mars of around 90 days, yet it continued exploring and communicating until 2018. NASA's Curiosity rover has been operating on Mars for the last 8.5 years, far exceeding its original 2-year mission life. Hopefully, Perseverance can demonstrate a similarly high level of reliability.

Money can't buy total reliability, however. Since its inception in 1958, NASA has spent over $650 billion (perhaps $1.2 trillion after inflation). It has had many great successes, putting 12 men on the moon, exploring all our system's planets with robotic probes, and currently has put five rovers successfully on Mars. It has had some tremendous reliability successes, such as the Voyager 1 and 2 probes that are still providing communications as they leave our solar system. It has also endured tragic failures, the worst of which are the losses of crews of the Space Shuttles Challenger and Columbia, and Apollo 1.

Not everything needs to be as reliable as a spacecraft, but many things, especially where failure would involve loss of life or a high economic loss, require high reliability.

Con't pg 9

Structural items such as buildings, bridges, and tunnels, and transportation items like aircraft, trains, ships, and cars, all need higher safety and reliability standards. You may sit in both, but you justifiably have greater concerns and expectations about safety and reliability for your automobile than for your La-Z-Boy recliner.

One way to mitigate risks when reliability and safety are not deemed sufficient is through back-up systems. Hospitals may add back-up power generators to compensate for a power grid that is not totally reliable. There probably are measures that should have been taken (and now likely will) to harden the Texas power grid against the extreme cold weather it experienced recently.

Our computers hold information internally in rotating magnetic platter hard drives and SSDs, but these are not immune to failure, so prudent users back up that information. Automobile tires can fail for a variety of reasons, so automakers offer several back-up systems, including a spare tire and changing tools, puncture sealant, and run-flat tires. Tire pressure monitoring systems are now required for all automobiles, as a safety backup.

We have continued to add safety features to motor vehicles over the years to reduce the number and severity of accidents. Safety glass, power steering and brakes, seat belts, airbags, energy-absorbing bumpers, and rear back-up cameras all add safety to cars through technology. Despite these enhancements, however, over 16500 Americans died in motor vehicle traffic crashes in 2020. Now automakers are looking to add self-driving technology to our highways; will it be safe and reliable enough?

Sometimes reliability is not as important as other factors, such as cost or convenience. Often new technologies are not as reliable initially, but in time may improve (or wind up being shunned by consumers). I like my Amazon Alexa devices, but I don't always get the responses I expect. Considering the complexity of the system, low cost to me and less than a critical need for the information, a less than perfect performance is acceptable. Alexa may not always provide the information I’m looking for, but I’m easily able to recognize this and so am not really harmed by her “incompetence”.

Some kinds of unreliability are more acceptable than are others. If your smart home lock is unreliable, it might be better if it occasionally fails to unlock when you get home, rather than sometimes not locking when you leave. It is the same with computer security; it is better to err on the side of being too restrictive than too permissive. Users can put up with only so much in unreliable access, however. New technologies such as fingerprint scanning and facial recognition for login, though more convenient than passwords, won't gain wide acceptance if valid users are not reliably recognized. If the convenience difference is great enough, however, users might be willing to accept having to scan multiple times for access.

Reliability in our technology is important, but the need for it varies with the product and the potential downsides. Our sensitivity to quality issues should be greater for a

Con't pg 10

Boeing 737 MAX airplane than for a wireless router. We as individuals and as a society will have to weigh the cost, quality, and risk trade-offs to determine in each case how much reliability is enough.

August 2021 DVD of the Month

ARI - Monthly newsletter
AudioBook - Free audio book

Buttercup - Password manager update

DVDOMlists - Contents of CDs and DVDs of the Month

FileZilla - FTP file transfer

GIMP - GNU Image Manipulation Program
Glary Utilities - 20 tools to maximize your computer performance

Lacey - Free Music and Video Downloader

MemberContributions - Things members send me

OldTimeRadio - Old radio audio files

Red Button - Tool to optimize and clean Windows

Smart Defrag Portable - Disk defragmenter with an easy to use interface
Snal Linux - Small Linux to use for as a live USB image to troubleshoot HD
StressMyPC - Stress a new PC/Win 10 during warranty

ThisIsWin11 - Try out Win 11 on Win 10 machine

USBDriveLog - Displays a log of all USB drives plugged into Win10 PC

WindowsLayoutSnapshot - Store snapshot of desktop in case of monitor change

Meeting Location and Special Accommodations

The Glenside Public Library address is at 25 E Fullerton Avenue, Glendale Heights, Illinois. Please park away from the building. Thank you. The meeting(s) are not library sponsored and all inquiries should be directed to Mike Goldberg

. 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, Mike Goldberg at at least five (5) days prior to the program, so that reasonable accommodation can be made.

Mailing address:
CAEUG
P.O. Box 3150
Glen Ellyn, IL 60138

Members Helpline

Any member can volunteer to be on the Members Helpline.
Hardware problems, Win 7, Win 10, Linux and Virus Removal
- John Spizzirri

CAEUG OFFICERS

President	Mike Goldberg
	president(at)caeug.net
V.P. (Programs)	Roger Kinzie
Secretary	Position OPEN
Treasurer	Position OPEN
Newsletter	Kathy Groce
Board Member	Frank Braman
Webmaster	John Spizzirri
	webmaster(at)caeug.net