

Interface

Lorain County Computer Users Group
www.LCCUG.com
Volume 32 Number 2 February 2021



2021

Inside This Issue

President's Letter	Pg.2
LCCUG Officers	Pg.2
Program	Pg.3
LCC-OGS	Pg.3
Genealogy Tip of the Day	Pg.4
Minutes	Pg.4
Classes & Workshop	Pg.5
Calendar of Events	Pg.6
NEOPC	Pg.6
Costly & Dangerous...	Pg.7
Ask Leo	Pg.8
Next Virtual Meeting	Pg.10
Helpful Memory Bytes...	Pg.12
Why Browsers Incognito...	Pg.13
Interesting Internet Finds	Pg.14
What Happens when you Zoom...	Pg.15



**Tuesday
February 9, 2020**



Bitwarden password manager

*Presented
By*

**John Kennedy
from APCUG**



**UNTIL FURTHER NOTICE MEETINGS ARE HELD
ON ZOOM DUE TO COVID19**

Meeting opens at 6:00 PM, program starts at 6:30 PM

**GENERAL MEMBERSHIP MEETINGS CONDUCTED VIA THE
ZOOM APP**

A Word From Our President



First a caution to all of us: **Covid Vaccine Scams** are reported to be rampant!! Please beware that if you are contacted by phone, email, or social media (ex. Facebook) about sharing your personal information or asking for money for a position on a list to get the vaccine..... do NOT do it. Anything like this is not real and can put your information at risk. FBI alerts can be found: <http://tiny.cc/4dmbtz>

There also continues to be those who want to trick us out of any stimulus money we might be entitled to.

[Stimulus check scams: here are red flags to watch for - CNBC](http://tiny.cc/8dmbtz) or <http://tiny.cc/8dmbtz>

Our **January meeting** had an interesting presentation from Bob Gostischa (Avast Evangelist). He spoke about security and about **Avast Free** - that can keep you safe on the internet and protect your computer. He also provided us with 2 pages of useful websites, tips and tricks to secure our computers and exchange our computer experience.

I want to remind everyone that his handout and a video recording of the meeting is posted on our links page (<https://lccug.com/links/>) along with most of our recent meetings.

Our February meeting will be presented by John Kennedy of APCUG. John recently gave us a presentation on Linux in August and on Free Software in October. Check out the program description of his February program elsewhere in this newsletter. He will be informing us about the usefulness of the password manager, Bitwarden. Password managers are essential nowadays with the many passwords we are accumulating!! You will appreciate the security and the convenience.

I would like to share an inventory I made last month. I made a list of all the items that I pay for directly out of my checking account or from my credit card. I checked on how much I'm paying for each and when it's due. It is good to make a review like this regularly. I have learned that I need to be careful of trials that I start and forget about and then discover that I am now being charged for them.

My last tip of the day is to suggest you visit this web site:

GCFLearnFree.org. *"It has been around for 20*

LCCUG Officers For 2021

President	Sandee Ruth president@lccug.com
Vice President	Vacant vp-programs@lccug.com
Secretary	Don Hall secretary@lccug.com
Treasurer	Micky Knickman treasurer@lccug.com
Newsletter Editor	Pam Rihel newsletter@lccug.com
Web Page Editor	Richard Barnett webpage@lccug.com
Statutory Agent	Sandra Ruth statutory_agent@lccug.com
Director of Membership	Dennis Smith membership@lccug.com
Director of Advertising	Richard Barnett advertising@lccug.com
Director of Education	Neil Higgins education@lccug.com

years and has helped millions around the world learn the essential skills they need to live and work in the 21st century. From Microsoft Office and email, to reading, math, and more—GCFLearnFree.org offers more than 200 topics, including more than 2,000 lessons, more than 1,000 videos, and more

than 50 interactives and games, completely free." <https://edu.gcfglobal.org/en/topics/> It is full of great information and it is exceptionally well done!



Sandra Ruth
LCCUG President



**Tuesday
February 9, 2021**

Bitwarden password manager

Presented By
John Kennedy from APCUG



THIS WILL BE A ZOOM MEETING Please join us via ZOOM. A link to the ZOOM meeting will be provided in a reminder email to be sent a few days before the meeting. This should be a very informative meeting.

As we use the Internet more and more, we find ourselves having to set up "accounts" for more and more places. We're taught that we need to use different passwords for every place. That becomes a challenge when trying to remember them, so we end up writing them all down. That not being a very secure option, we might consider having a program remember them all for us. Thus the creation of Password Managers. At this month's meeting, we will take a look at one of the popular & free password managers named "Bitwarden". Our presenter, John Kennedy, will share his thoughts on passwords, and password managers. He uses Bitwarden so he will take us on a tour of what the average Password Manager can do, and what features he uses and confesses that he doesn't always use it to its fullest. But he will say that the two main reasons that he uses a Password Manager is "speed" and "convenience". Come and see how this program might help you out in your surfing of the Internet and managing all your passwords.

Bitwarden is one of the top three password managers rated by Consumer Reports in their July, 2020 issue (page 22). It was also mentioned in the Online Safety article on page 30 from the February, 2021 issue..

GENERAL MEMBERSHIP MEETINGS CONDUCTED VIA THE ZOOM APP 

The Lorain County Chapter of OGS

is having its next meeting online:

Check our webpage for the next program.
<http://loraincoogs.org/events.html>



We are having our meetings virtually using bluejeans.com.

To join the meeting on a computer or mobile phone:
<https://bluejeans.com/5006724159?src=calendarLink>
Also a link will be sent to you before the meeting.

North Ridgeville Library, 35700 Bainbridge Rd. North Ridgeville, Ohio. Meetings are free and open to the public. Social time is at 6:30 PM and the program begins at 7:00 PM. **Cancelled Until further notice due to Covid-19**

Jean Copeland: jecopeland1975@gmail.com.

ROYAL business equipment

365-2288 - Elyria 1-800-238-8973 - USA
591 Cleveland Street Elyria, Ohio 44035

- * COMPUTER REPAIR
- * PRINTERS & SUPPLIES
- * UPGRADES
- * CUSTOM PC'S & LAPTOPS
- * CALL FOR BEST PRICES
- * EDUCATION DISCOUNTS
- * LCD MONITORS & TVS



Shop at www.ROYALBUSINESS.com and save \$\$\$

Financing Available - 90 days same as cash



Executive Board Meeting Minutes

JANUARY 5, 2021

The board Zoom video meeting for December was attended by Sandee Ruth, Don Hall, Micky Knickman, Pam Rihel, Dennis Smith and Neil Higgins.

The board discussed some of the many programs available from APCUG. Micky liked Password Managers and Pam liked Evernote.

Dennis will send out membership renewal notices.

Pam moved, Neil seconded meeting be adjourned.



General Meeting Minutes

JANUARY 12, 2021

President Sandee Ruth called the Zoom video meeting to order. A motion to accept the minutes as shown in the January issue of the *INTERFACE* was made by Cliff Salisbury and seconded by Pam Rihel. Motion passed by voice vote.

Bob Gostischa, retired banker and security expert for AVAST, presented a program “YOUR ONLINE SECURITY”. Bob explained the eight essentials of secure computing using AVAST available for a cost or by using the free version. He also gave tips for smartphone use. There were many questions from members which Bob easily answered.

Pam Rihel won the attendance raffle.

Genealogy Tip of the Day

Michael John Neill Genealogy Tip of the Day
Rootdig.com mjnrootdig@gmail.com

Were They Really Born on the Ocean?

There is no doubt that pregnant women got on ships that were headed to the United States.

There is no doubt that some of them had their babies on the ship.

I tend to doubt the story unless I can find some relatively contemporary evidence of it. The infant listed on the manifest as a newborn is a prime example. Stories of the baby being born on the ship make for nice dramatic stories and, when it actually happened, there is no doubt that it would have been a dramatic birth and the baby was fortunate to have survived.

But try and find something that backs up that story.

How Did They Say It?

Do you really know how someone actually pronounced the last name you are researching? One place to find out is from someone who actually has the last name. But there’s no guarantee that someone with the last name today is pronouncing it the way their ancestor did in 1800.

If the name is not in English, find someone who speaks the language and ask them what it sounds like—online genealogy groups may be one place to find these people. For names that are in English are there online genealogy groups from the area where the person or family lived who may be familiar with how the name is pronounced? It is not always necessary to find someone with the last name in order to see how it was pronounced.

The way a name was said matters as it impacts how it gets spelled in records and occasionally those renderings are significantly different from what we would expect.



**Member of Association of Personal
Computer Users Groups**



Thinking of shopping with Amazon? Well you can now go to our lccug.com website and just click on the amazonsmile link and start shopping.

Our club gets rewarded for any items purchased from our website. So the more you buy the better it is for our club. **SO START SHOPPING.**

NEED HELP?



Here's Who to Contact:

Neil Higgins

440-985-8507 - higgins.neil@gmail.com
Evenings 6 p.m. -10 p.m. + Weekends
Hardware, Linux & Windows Operating Systems,
Chromebooks, Tweaking your system

Micky Knickman

440-967-3118 - micky@knickman.com
Daily 6:00 am to 4:00 pm. Leave message if no answer.
General Software Configuration, Hardware Installation,
Basic to Advanced Windows

Richard Barnett

440-365-9442 - Richard216@aol.com
Evenings & Weekends
General Software Configuration, Hardware Installation,
Basic to Advanced Windows & Web Page Design

Sandee Ruth

440-984-2692 - sandee29@gmail.com
Basic Word Processing, Windows, & Web Design
Advanced Internet

Pam Casper Rihel

440-277-6076
6:00 p.m. to 9:00 pm Monday thru Thursday
Genealogy help
prihell1947@gmail.com

Denny Smith

440-355-6218 - dennis.smith@windstream.net
Microsoft EXCEL
Leave message on machine if no answer

If any of our members are interested in helping other users with what programs you are adept at, please contact any of our officers with you name, what program or programs you would be willing to give help with, you email address and or phone number and when you would like to have them call

Newsletter Editor: Pam Rihel using Microsoft Publisher, 2013

This Month's contributors: Micky Knickman, Sandra Ruth, Pam Rihel, Don Hall, Dennis Smith, Neil Higgins, Michael John Neill, Steve Costello, Phil Sorrentino, Jim Cerny, Scambusters, APCUG, Leo Notenboom, NEOPC, Microsoft Office art online, <https://www.intivix.com/20-computer-tricks-know/>

Newsletter is now
Online at:

lccug.com/newsletters or lccug.com

Woohoo!

Your renewal dues have been reduced from \$25.00 to \$15.00. When everything else is raising their prices our Computer Club is lowering their dues.

LCCUG ONGOING WORKSHOP

ALL ARE FREE AND OPEN TO THE PUBLIC

Problem Solving Workshop

Date: Tuesday - February 19, 2021

**Time: 5:30 - 8 pm Instructor: Micky Knickman,
Neil Higgins, Richard Barnett**

**Place: Lorain County Community College
@ 2600 Ashland Avenue, Lorain**

**Learn how to repair or update your computer by
changing hard drives, memory, CD ROMs, etc.**

Members are encouraged to bring their computers anytime before 7:30 pm for assistance from Micky, Neil & others.

Learning About Electronics

Date: Tuesday - February 19, 2021

Time: 5:30 - 8 pm Instructor: Sandee Ruth

Place: LCCC @ 2600 Ashland Avenue, Lorain

Learn how use you electronic devices.

Members are encouraged to bring their tablets, iPod, kindles, etc. at 5:30 pm for assistance from Sandee and any other knowledgeable members. The public is welcome to sit in on these classes.

Learn About- Hands on Demonstration

Date: Tuesday- February 19, 2021

Time: 5:30- 8 pm Instructor: Neil Higgins

Place: LCCC @ 2600 Ashland Avenue, Lorain

Do you know the specifications of your computer? What is really inside? We'll demonstrate three portable Windows programs (run from a USB Stick) that will tell a computer's storage, CPU, video, and other useful information (including your Operating System Product Key) . This will help determine if your computer will run certain programs, and will help find out what memory or video card upgrade you need.

Please bring a flash drive to obtain software and handouts. If you would like to participate and get copies of the material for this presentation, please let Neil know by sending an email to Education@lccug.com.

Lorain County Computer Users Group

2020 Calendar of Events

<http://lccug.com>
email: info@lccug.com



Using Zoom

Meeting opens at 6pm – program starts at 6:30

*2nd Tuesday of each month. Changes are announced on the webpage and the newsletter.
All meetings are open to the public*

January 12, 2021, Avast & PC Security

February 9, 2021 Bitwarden Password Manager by John Kennedy from APCUG

March 13, 2021 TBA

April 13, 2021 TBA

May 11, 2021 TBA

June 15, 2021 TBA

All other months to be announced.



NEOPC Meetings

lenorebman@gmail.com if you plan to come.

Meetings have been canceled due to the Coronavirus (Covid-19) until further notice

Check out their website at:
<http://www.neopc.org>

MEMBERSHIP WITH LCCUG:

Yearly dues are now \$15.00. For more information contact:

Dennis Smith
Director of Membership,
membership@lccug.com.

Meeting Location:

LCCC Community Center at the College
2600 Ashland Ave., Lima, OH 44845
9:00 AM - 12:00 PM
Elevator access is available for those in need.

No Meetings at the College

Computer Club News

Don't Forget to Bring
in Your Used Ink Cartridges
LCCUG is collecting empty ink
Cartridges



*For every cartridge you will receive a
ticket for our special drawing.
Recycle & Help Our Club Too!*

LCCUG WORKSHOP Class Ideas?

Neil needs your input into what classes you would like him to present to our members.

Please tell Neil or the other officers what you would like to see and we will be happy to help you with classes on your subject./subjects.

Neil Higgins Education@lccug.com.

No Meetings at the College

LCCUG'S NEXT VIRTUAL GENERAL MEETING WILL BE HELD February 9, 2021.

This is our eighth virtual meeting. We are hoping for more members to join in on these programs.

These meeting are fun and interesting and you also get to visit with other members that you have not seen in months, due to the Corona-virus - Covid 19 Pandemic.

It is not hard to join in on these meetings, as Sandee sends out the web address and all you have to do is click on it and when it opens up, find the icon that says JOIN, its as easy as that. Then Sandee will sign you in;

So please join in the fun on
Tuesday February 9, 2021 at 6:30.
Bitwarden Password Manager
By
John Kennedy - APCUG

If you are in need of some help, well just call one of the board members and you will be helped.

If there is a program you would like to learn about just let the officers know and we can fix you right up.

Hope to see new faces at our next meeting. You know we miss you all. Be there or be square...



Our links can be found at:

LCCUG.com/links, There you will find many interesting places to visit. Check them out and see what you can find interesting

Costly and Dangerous: Ignore This Fake Mercury "Cure"

By [Keith](#)

Snippets issue exposes mercury hoax, password scandals plus more phishing and extortion tricks: Internet Scambusters #939

A mysterious form of the liquid metal mercury is being touted as a disease cure. But experts say neither the mercury nor the cure exist.

But, as we explain in this week's Snippets issue, that doesn't stop scammers asking for up to \$25,000 for this supposed elixir.

We also have a trio of warnings about password usage and a clutch of other new scams currently doing the rounds.

Costly and Dangerous: Ignore This Fake Mercury "Cure"

A couple of centuries ago, word got around that potions containing the liquid metal mercury could be used for treating all manner of serious diseases. Not true, however, with the result that people who took the potions generally got worse or died.

Evidence that some scams have been around for hundreds of years has emerged in the shape of renewed claims that a form of the metal — this time called red mercury — can help with disease treatment, including Covid-19.

It's a weird scam because, according to some experts, red mercury doesn't actually exist, though rumors that it does have been around for the past 50 years — possibly connected with the old "red" Soviet Union during the cold war era.

But that hasn't stopped people offering something with that name for sale on the black market and even on some social media sites.

This includes liquid mercury that has been stained with red coloring, other compounds that happen to be red or even, in one reported case, mercury compounds being sold in bottles painted red with nail polish!

The implications of this are really serious. And the stuff is hugely expensive — up to \$25,000 a gram (but more usually around \$350) according to global news site vice.com.

(Continued on page 8)

(Continued from page 7) Costly & Dangerous...

An investigator for Vice who responded to an ad via messaging site WhatsApp was told by a seller in North Africa that the potion can cure the coronavirus. However, he would have to hand over that \$25,000 for evidence as well as the product. Money upfront without evidence is a sure sign of a con.

Consuming mercury is likely as dangerous — or more — as drinking hand sanitizer or disinfectant. Vice quotes Professor Andrea Sella, a chemistry professor at University College London, as saying: “Mercury is bad news, no matter what you do with it.”

Any product that has “mercury” in its name should be given a wide berth, the professor says, adding it would be “insane” to even try it.

As COVID-19 infections may ramp up in the coming weeks before vaccination starts, beware of anyone offering red mercury or any other supposed cure. You could end up worse off — financially and health-wise — than if you got the disease.

Copyright Audri and Jim Lanford. All rights reserved. Reprinted with permission. Subscribe free to Internet Scambusters at <http://www.scambusters.org>

Tricks for Typing

Here are a few tips that will save you lots of time when typing documents:

- Move the cursor quicker to the beginning of the previous word by pressing CTRL+Left Arrow, instead of doing it manually.
- To get the cursor to the beginning of the next word, use CTRL+Right Arrow.
- Recover a deleted item with ALT+Backspace.
- Delete an entire word by pressing CTRL+Backspace.
- Select a word you want to highlight quickly, without dragging the mouse, by double-clicking on it.
- Highlight a whole paragraph by triple-clicking on it.
- Make superscript and sub text by pressing CTRL + = for sub, and CTRL+ Shift for superscript.

Paste in plain text and not what was originally formatted, after copying, by pressing CTRL + Shift

<https://www.intivix.com/20-computer-tricks-know/>



Why Password Managers Are Safer than the Alternatives

by Leo A. Notenboom

Password vaults really are your most secure solution

If you're not using a password manager, you're likely compromising your security more than necessary. Here's why using one is safer.

Recently I tried to use RoboForm for an account at a large financial institution, but I couldn't get it to work. In response to my inquiry, this institution said they do not permit log in using credentials that are stored on software because the security of the password could become jeopardized if my computer were hacked, invaded, etc. Is this true? Am I safer not to use tools like RoboForm?

Some believe using password managers presents a single point of failure. *Very technically*, they are correct: if someone gains access to your password manager, they have access to everything in it.

Not so technically, I strongly believe they are misguided.

Using a good password manager is *significantly* safer than any other alternative.

Good security demands you have a unique and strong password for every site or service ideally kept only in your head. Without a password manager to aid you, you'll likely need to make a tradeoff that compromises your security. There's no such thing as perfect security, but using a password manager ensures you're as secure as possible without needing to make those tradeoffs.

Security best practices

Password security demands that you:

- Have good, strong passwords (long and complex).
- Keep them nowhere but in your head (memorable).
- Use a different password on every site or service (unique).

Yes, indeed, that would be ideal.

Without using a password manager, it's also completely impractical.

Those requirements simply can't all be met at the same time. At least one, if not two, will be compromised without the aid of a password vault.

(Continued on page 9)

(Continued from page 8) *Why Password Managers...*

Without a password manager

Without a password manager, you'll compromise your security in some way.

- You'll choose a less secure, easy-to-remember password (short and/or not complex).
- You'll use the same password at multiple sites (not unique).
- You'll save the password using technology that is not secure (not memorable).

Any one of those can significantly compromise your security.

With a password manager

Password managers make best practices trivially easy. Using a password manager allows you to:

- Generate and use secure, complex, and appropriately long passwords.
- Avoid the need to remember passwords yourself.
- Use different passwords on different sites.

These are things people *don't* do unless they have a tool in place to help them. Password managers are specifically designed to securely do exactly that.

Most password managers add several features that make improved security even more convenient. They can:

- Synchronize your information across multiple devices.
- Be used on mobile devices.
- Automatically fill in not just passwords, but common web forms.
- Securely store other information of many types.

And they do all of that with more security than almost all alternatives.

If you're compromised, you're compromised

It is true that if your computer is compromised, all bets are off. Malware *could* gain access to whatever it is you have stored on the computer. For example, while I'm logged into LastPass, all the information could technically be available to software running on my machine — good software or bad.

That's a serious concern, and not to be taken lightly.

But it's a concern that exists *regardless of whether you use a password manager or not*. All bets are off if a keylogger captures what you enter when you log in to your bank account.

Avoiding a password manager doesn't increase your security one whit.

But are password managers safe?

Yes. Password managers are *safer than any practical alternative*.

There are no absolutes — that, too, is a practical reality. There is no such thing as absolute security. As I said earlier, if you fall victim to malware, all bets are off, *no matter what technique(s) you use*.

Password managers are the safest way to keep a record of your online account information, but they are no safer than:

- The master password you use to access the password manager.
- Your own ability to use your computer safely.

The last one scares most people, but my claim is that using password managers is, in fact, one way to use your computer more safely.

What I do

I keep my machines secure by doing the things you hear over and over: keeping software up to date, running scans regularly, avoiding malicious websites and downloads, not falling for phishing, and so on.

I use LastPass to manage all my passwords and additional security information.

I use Google Authenticator, a form of two-factor authentication, to access my LastPass vault. You can't get in to my LastPass account *even if you know my master password*. To get access, you need both my master password *and* my mobile phone.

I have LastPass automatically log out after some amount of time on any device which I'm not 100% certain won't get stolen or accessed without my permission.

I keep my master password secure and complex.

I back up my LastPass vault regularly.

I'm not going to claim it's impossible for anything bad to happen — that'd be a foolish claim. I am, however, *very* satisfied with the risks and trade-offs, and absolutely convinced that using LastPass (or any reputable password manager) keeps me as safe as possible, and safer than not using one at all.

Let's face it: even doing business *offline* has risks and trade-offs.

This work by [Ask Leo!](#) is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](#). Additional information is available at <https://askleo.com/creative-commons-license/>.



Virtual Classes – are Real

By Phil Sorrentino, Contributing Writer, Sun City Center Computer Club
www.sccccomputerclub.org
philsorr@yahoo.com

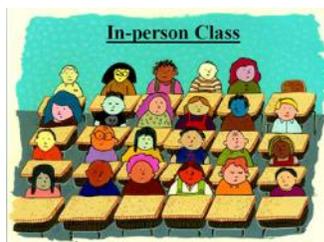
That almost sounds like an oxymoron like “Jumbo Shrimp” or “deafening silence.” Well, the coronavirus has elevated teleconferencing to a level never seen before or maybe even ever expected. Almost everyone, by now, knows of Zoom and other computer Apps like GoToMeeting for teleconferencing. Zoom appears to have a lion’s share of the business. If you’re not quite sure what Zoom is, here is what Wikipedia says. “Zoom Video Communications, Inc is an American communications technology company. It provides video telephony and online chat services through a cloud-based peer-to-peer software platform and is used for teleconferencing, telecommuting, distance education, and social relations”. For many of us, we can think of it just as an “easier to use” Skype. Two years ago, I did a presentation to a User Group on the west coast using Zoom (surprisingly not Skype). It was the first time I had heard of or used Zoom. Now Zoom has over 40% of the teleconferencing market. (Boy did I miss an investment opportunity. Zoom went public in March 2019 at \$36 and is now around \$250.)

Before the virus, teleconferencing was used mostly in the corporate world. But now everyone is familiar with it, from the seniors who are self-quarantining to avoid crowds, to elementary school students and teachers staying at home to avoid classrooms and crowded schools, to employees who are working from home to avoid the workplace gathering places like the coffee pot, the copier, and the water cooler.

Almost all of us are trying to avoid groups of people where the virus might easily be transferred. I recently needed to go to a shopping mall, and I was amazed to see how empty it was. We are staying away from gathering

places. (Although the beaches do still seem to be pretty crowded.) So, now that we are not going out and gathering as much, we are staying home a lot more, which gives us a lot more time to learn new things. How many of us have taken up a new instrument or are learning a new language? Now’s the time to learn how to play that guitar or keyboard you bought a few years ago. Well, language and instruments may be too much to expect but we probably can more easily learn about things we are involved in or are using daily, like our computer and our phone. And that is where virtual classes can be of some help.

Virtual classes are educational classes held remotely using teleconferencing software like Zoom or GoToMeeting, or others.



With an in-person class, students and teachers gather in a classroom and interact there. With a Virtual class, we interact through our computer Clients (apps) which are then gathered together in a Server. (Remember Client-Server Technology?) Each of our computers is connected to the server via the internet,

and it is the Server software that provides the magic that lets us all share the Video and Audio from our client computer’s cameras and microphones. The popular servers support many different clients. You can attend a virtual class using almost any device such as a Windows computer, an Apple computer or an iPhone or iPod, an Android phone or tablet, a Chromebook, or even a Linux computer. A reliable, fast internet connection will greatly improve the experience. A wired connection to your router may be desirable, but not very common. Fortunately, modern wi-fi is typically more than adequate. (But unfortunately, not everyone has the latest wi-fi, especially if it is being supplied by the Internet Service Provider.)

(Continued on page 11)

(Continued from page 10) Virtual Classes are Real

The internet connections to the server in the cloud allow us to interact “virtually” and avoid gathering together. The server “connects” each of us to each other. And the server presents a classroom presentation to each of us (the Users) so we can see who is participating in the virtual class. (There are controls on the Users screen that allow the Video and Audio, separately, to be turned on or off. The audio control is the “mute” control, mute turns the audio off, and un-mute turns the audio on. The video control is typically just Video on or off, though initially, it might show up as “join with Video”.)

The classroom presentation also has some different ways of showing the group of participants. Gallery view, as it is sometimes called, shows each of the participants (if their video is on) in a box on the screen. (If a Participant’s video is off, the box will just have the User Determined name.) The screen is divided among the number of participants, so as the number of participants gets larger it might be harder to determine who is in attendance, though each participant box does show the name. Another classroom presentation shows predominantly the person who is speaking with others shown in small boxes to the side or bottom, sometimes called “speaker view”. If there are a lot of speakers this might be helpful, though if someone has a slow internet connection, it might end up less helpful, due to the delay.

For any Virtual class, a very comprehensive PowerPoint presentation would be recommended, in general, to guide the class through the subject matter. Some classes readily lend themselves to the Virtual format. These are the “lecture” type of classes where there are no “hands-on exercises” to be undertaken. Demonstrations of hardware or software can mostly be accomplished using a “Share screen” feature that lets the instructor share the contents of his computer screen with all the participants. (Software on a particular device can be easily demonstrated by having that device as another class partici-

pant and allowing it to share its screen.) When the instructor does this, the instructor’s screen shows up on every participant’s screen.

So, it’s just like watching the big screen TV in front of the classroom, only everyone sees the teacher’s screen on their computer screen, at their location. A class like “Cut the Cord” works well as a virtual class because it is mostly lecture. Other classes, that are more interactive, may not lend themselves as easily. A class that requires a lot of interaction may be difficult as a virtual class. This type of class may be more like a discussion group and maybe more dependent on having a definite agenda and a very strong moderator/instructor. Smaller class sizes may help this type of class be successful. The Special Interest Group on smartphones is an example of this type of class. All the participants of this class are encouraged to bring questions and ideas to the class for discussion, and it is anticipated that everyone will have an opportunity to speak. Questions from the class participants in any class are handled with either a “Chat” feature where the question can go to all participants or a specific participant or a “Raise Hand” feature that shows up on the screens to get the participant’s attention.

Hopefully, this brief description (and time spent watching YouTube videos on the subject) will give you the courage to participate in a virtual class the next time an interesting one is offered.

How To Send A PDF via Email

I find if I save the pdf to my desktop, I can go into my Gmail, open the send box, put the person’s email address in where to send it, type in the subject sending file or something like that.

Go to the bottom of your email box and click on the paperclip, then go to your desktop, hit on the file and let it load in your email.

Once it is done loading, go ahead the send it.

Hope this helps.



Helpful Memory Bytes

By Jim Cerny, Help Desk Host, The Saratoga Users Group
July 2020 STUG Monitor
www.thestug.org
jimcerny123@gmail.com

Let's review and explore what we really need to know about basic computer storage (bits and bytes) and how it helps us get an idea of the data space needed to save and backup our stuff.

Suppose you landed on a planet and the aliens there only had one hand and only one finger on it (not ten fingers like we do). All they could do is flash a single digit or none at all (hence, a zero or one). How high could they count? Could they do basic math?

All computers use the binary system (a single digit of 1 or 0) – that is, they store and work with data saved in memory as zeros and ones. But there is NO LIMIT to how high you can count – you just keep adding on more zeros and ones. For example, the digits we know in our numbering system such as 1, 2, 3, 4, 5, 6, 7, 8, 15, 16, 31, 32, 33, etc. would be the following in binary = 1, 10, 11, 100, 101, 110, 111, 1000, 1111, 10000, 11111, 100000, 100001, etc. So, adding a new digit to the left doubles the size of the memory (or number). Believe it or not, math gets a lot simpler with only two digits. A single binary digit is called a BIT. Eight bits together form a BYTE of data. Eight bits allow for 256 different combinations, enough to cover not only our 26-character alphabet but special characters and more. Every keystroke on your keyboard enters one byte into memory!

I love the old science fiction movies – where the spacecraft command center was filled with gauges and dials! To read a value on a dial you had to look closely and see where the arrow was. It showed measurement on a scale of lines and it was up to you and your eyesight to see the amount or “reading.” But with binary digits, you don't care about “how much” you only need to know if it is there or not there -- a one or a zero. To get more accuracy, you just add more binary digits. So, you will need a lot of them, but they are cheap and much easier for use in electronics.

One KILO-byte of memory is 1024 bytes, but when

we start dealing with really large amounts of computer storage, we round it off and call it a thousand.

One MEGA-byte of data is one million bytes or one-thousand kilobytes. Those old 3.5-inch computer disks (remember them?) held about one and a half megabytes or about 220 pages of text. A CD-ROM (computer disk) could hold about 700 megabytes, that's over 400 of those old floppy disks and about 90,000 pages of text. It is good to remember that photos, depending upon the number of pixels in them, can be from 10 or 20 kilobytes up to 2, 12, 24, or more megabytes each! So, is a picture worth a thousand words? You bet, and more!

One GIGA-byte is one trillion bytes or one-thousand megabytes. Now we are talking serious (and very inexpensive) memory! You can buy a small portable USB drive (called a “thumb” drive or “flash” drive) in various gigabyte sizes – I tend to like the 32 or 64-gigabyte size because it can easily hold all my photos and documents as my backup. Just one gigabyte can hold almost 700,000 pages of text. That's a den full of books. One HD (high definition) movie can take 2 to 5 gigabytes of memory. Movies and videos are moving pictures, of course, several pictures (or “frames”) per second. Fortunately, the data used to store photos and movies are “compressed” or coded to take up much less space than you would expect.

One TERA-byte is one thousand gigabytes. For us normal people, this is a HUGE amount of memory! You can get a one-terabyte drive for about \$50. It can hold 300,000 photos or about 500 hours of movies. And, unlike my memory, it will never forget anything.

The next memory size up is the PETA-byte -- yup, one-thousand terabytes! And, no, they are not going to run out of prefixes. All just to store ones and zeros.

I use a nice little thumb drive I use to back up my memory, but I seem to forget where I put it!



Why Browser Incognito Mode Doesn't Protect Privacy

Have you ever clicked on the "in private," "incognito" or similar private mode option in your browser and thought you couldn't be tracked? Forget it. With a couple of minor exceptions, you really haven't done anything to protect your privacy.

Most people realize by now that it's next to impossible to surf the Internet securely using a conventional browser. Sites you visit can place cookies (small pieces of code) on your device, unless you severely restrict them.

This enables them to recognize you when you return -- which can actually be helpful to you by avoiding the need to keep signing in. But cookies may also tell site owners where you visited previously and what kind of things

you've been looking at.

Yes, you can impose restrictions but, without other security elements, this has limited effect on concealing your activities. So, when you stumble across the "in private" option in your browser, it's reasonable to assume you've closed all the doors to the prying eyes of hackers and scammers, as well as legitimate sites that want to know what you're up to so they can exploit it.

But that's not so, as more and more people are discovering. As PC magazine Computer Active recently put it: "Enabling your browser's private mode won't stop you being tracked by advertisers. It won't make you anonymous online. And it certainly won't protect you from malware or phishing sites."

In fact, all that private mode does is stop the browser itself from keeping track of your activities. So, if other people also use your PC, they won't be able to identify which sites you visited by, for example, checking the "history" setting. Some cookies and images may also not be stored, but that's about it.

Your Internet service provider (ISP) still knows which sites you visit and, depending on who your ISP is, they may even provide this information in response to official requests from

government, law enforcement, and so on.

Security software developer Psafe explains: "Incognito mode doesn't mean that your boss or Internet service provider can't track your browsing history. Many major websites can still track and record your behavior in incognito mode, too, which means that you won't be able to escape data collecting and targeted advertising."

And, if you're unlucky enough to already have malware installed on your device, this will ignore your incognito setting and continue to operate as normal behind the scenes. A number of hacking tools can also track and share information about your cell phone browsing activities via a technique known as "canvas fingerprinting."

How to Be Incognito

What can you do to truly protect your privacy and keep you safe from prying eyes?

Here are five key actions you can take:

1. Block or limit cookies. As suggested, by itself this has only limited effectiveness. But it's an important first step. You'll find options both to block and clear out cookies in your settings.

The main idea is to block what are called "third-party cookies," which are placed on your PC by advertising trackers and data gatherers. "First-party cookies" are those placed on your device by the actual websites you visit so they know when you come back.

These days, many websites won't allow you to visit them unless you accept their first-party cookies but, as a default, you should block the third-party code.

2. Use an add-on that blocks on-screen ads and trackers that are sometimes buried in online advertisements. Most of these blockers have settings that enable you to allow exceptions from sites you know and trust.

However, increasingly, some sites recognize that you're using an ad blocker and refuse to give you access unless you turn it off.

Examples of popular ad-blockers include Ghostery, AdGuard, AdBlock, and uBlock.

(Continued on page 14)

3. Use a browser that never records your searches. Most search engines, like Google, store details of sites you visited. A couple don't. These include the new and increasingly popular Brave browser and the long-standing one with the curious name -- DuckDuckGo.

4. You can go one step further by using a browser that routes your activities through multiple computer services all over the world. This makes it almost impossible for anyone to detect who and where you are and what you're doing.

The best-known one is called Tor (torproject.org). Unfortunately, it has two disadvantages. First, because of the convoluted routing, it can be extremely slow and some times won't load pages at all.

Second, it's the browser of choice for crooks, scammers, and hackers -- a key gateway to the Internet underworld. That means you could be in bad company. Plus, high-tech Internet crime specialists devote a lot of time trying to track some users' activities on Tor, so you could end up drawing attention to yourself.

Your ISP knows when you're using Tor, even though they can't tell the sites you're visiting.

We wrote about VPNs in Issue #813 (<https://scambusters.org/vpn.html>). Some are free, some are paid for, and some have different policies. For example, since they obviously know your IP address, you need to know what their policy is on sharing this with others. To get the best one for your needs, it's worthwhile checking reviews and comparison sites. Here's a good starting point: <https://www.techradar.com/vpn/best-vpn>

As online activities become more and more central to our daily lives, protecting your privacy has become crucial. Simply opting for incognito mode on your browser just won't cut it.

Alert of the Week

A scam email pretending to come from PayPal is the latest in a never-ending procession of attempts to steal customer sign-on information.

The crooks are phishing for details so they can drain victims' PayPal accounts.

As usual, the email looks remarkably like the real thing. It claims your account information is incorrect so you supposedly must click an "Update" button, which, of course, will take you to a fake sign-on page.

Legitimate or not, you should never click on links like these in emails. If you want to know if there are issues with your PayPal or any other account, go straight to the correct site, in this case: paypal.com.

Interesting Internet Finds

Steve Costello
scostello@sefcug.com

Vivaldi Browser Tips And Tricks
<https://www.thewindowsclub.com/vivaldi-browser-tips-and-tricks/>

I have been using Vivaldi (on both Windows 10 and Linux) off and on for a few months now, and I like it. This post gives some tips and tricks, that should make using it a better experience.

Can You Use Bluetooth Speakers If Your TV isn't Bluetooth Ready?

<https://thevisualcommunicationguy.com/2020/06/22/can-you-use-bluetooth-speakers-if-your-tv-isnt-bluetooth-ready/>

I have two TVs that are over 10 years old but work fine. I have plenty of Bluetooth speakers and headphones, but neither TV supports Bluetooth. (Note: I have a soundbar hooked to the main TV now, and it supports Bluetooth.)

This work by [Steve Costello](#) is licensed under a [Creative Commons Attribution 4.0 International License](#).

As long as you attribute this article, you can use it in part, or whole, for your newsletter, website, or blog.



President's Corner

What happens when your Zoom host has a power outage – and other happy tales

By Greg Skalka, President, Under the Computer Hood User Group

August 2020 issue, Drive Light

www.uchug.org president@uchug.org

In these COVID times, large gatherings are prohibited, so groups like ours can no longer meet in person. Fortunately, technology has come to our rescue, as many groups now hold virtual meetings through Zoom or another video conferencing service. As was made clear to me at our last meeting, however, technology runs on electricity, and you can't participate when your power goes out. Several factors played in our favor, so for most attendees, the show went on without me with many probably unaware. As long as the outage is not too widespread and the meeting is set up correctly, we found Zoom is very robust and fault-tolerant, even when the meeting host drops off.

Our last physical meeting was in the first week of March, just before our meeting venue was closed to outside groups. Since then, we have met in the cloud on Zoom quite successfully. A large part of that was due to APCUG (Association of Personal Computer User Groups), of which our group is a member. APCUG has provided us access to one of their paid Zoom accounts, so our meetings can run their normal two-hour duration (avoiding the time limits of a free account). Additionally, our board meets once a month using Zoom. For three of our four Zoom general meetings, APCUG also provided us with presentations through their Speakers Bureau presenters. We are now so used to the virtual meeting format that it has become routine. That is often when fate decides it is time to throw a curveball.

Our July meeting initially followed our now-familiar script. I had scheduled our meeting using the APCUG Zoom account and sent the meeting information to our editor, Art, so that it could be sent out through the member email list. Thirty minutes before the meeting start time, I logged into Zoom and started the meeting session.

While we so far have not had any of the virtual meeting problems other non-APCUG groups have reported (like Zoom-bombing), we try to follow all recommended security precautions. We now use a passcode for our meetings to reduce the chance of random interlopers. We have also enabled the Zoom waiting room, which keeps those joining in a virtual holding area until admitted to the meeting by the meeting host. We don't publish our meeting's Zoom information, but instead, send it only to our members, vetted guests, and those that have requested it through email (and have provided a name so that they can be recognized in the waiting room).

To help me in this waiting room filtering, our editor tries to come into the meeting early. I make him a co-host, giving him the power to see and admit from the waiting room (and, as it turns out, take over should something happen to me, the host). In those 30 minutes before the meeting, I also share my screen periodically, showing a few presentation slides with basic meeting information for the evening, so attendees know they are in the right place and know what to expect.

At about 7 PM I started our July meeting with an introduction of the evening's agenda. Following tradition, I then made our Webmaster, Bob, a co-host, so that he could share his screen and show us the links to new, exciting and helpful software he had added this month to the Library Links section of our web site (www.uchug.org).

Following Bob's report, I introduced our APCUG Speakers Bureau presenter for the evening, Francis Chao, and made him a Zoom co-host.



Francis then shared his screen for the first of his two presentations, a comparison of cloud storage services. I'm not that enamored with cloud storage, so I was waiting for his second presentation (which I had suggested to the board), USB-C.

Francis was probably about halfway through his interesting USB-C presentation (around 8:15 PM) when I suddenly heard the sickening sound of a power outage. Some might say that a power outage makes no sound, that it is more an absence of sound, but I disagree. The clicks of relays switching off, the change in pitch of computer fans slowing down and the frequency of power supply hum changing all make up the sound I recognize as

(Continued on page 16)

(Continued from page 15) What happens when your Zoom host has a power outage – and other happy tales

power failure. Even before my eyes could tell my brain about the sudden loss of photons, it knew from the sound what had happened.

Since the desktop PC, I was Zooming on did not have a UPS or uninterruptible power supply, I sat there in the dark for a moment, wondering how widespread the outage was. Though it was past sunset, I could see by the dim outside glow enough to get up and out of the upstairs computer room. I saw through the front windows that my street was dark and neighbor kids were starting to come outside with flashlights.



My first concern was for the safety of the first lady. I found my wife downstairs in her office, on her computer. She has a practically brand-new desktop PC with dual monitors and a UPS with a brand-new battery. I had replaced everything for her at the beginning of the year in response to that now insignificant crisis, the Windows 7 end-of-life. She sat in the glow of the monitors. I told her to save and close everything, and then shut her computer down.

The next course of action was to get flashlights. We have a handy rechargeable flashlight plugged into an outlet in our downstairs hall. The flashlight part sits in a charging base, so it is always ready. The light comes when it loses its input power (either from being lifted out of its base or by an outage). When the power went off, the flashlight came on like a beacon. I took the flashlight out of the holder and proceeded to the garage, where our emergency flashlights were stored with our camping gear.

Going into the garage, I instinctively flipped on the light switch, and then realized that was a pointless action. I would find myself doing the same thing several more times before the power came back. I got to the camping gear and found the flashlights, but they were all dead. “Time to buy more 6V lantern batteries,” I told myself. I took my rechargeable auto trouble light from the garage and went back to the house.

It was finally time to send a text to Art to tell him my street’s power was out. Was the Zoom meeting still going? He replied that it continued without me. Having others as co-hosts allowed Zoom to handle my dropping out and continue with the meeting. Likely, most attendees didn’t even notice.

I next went around the house looking for things that should be turned off, so surges, when power is restored, won’t cause additional damage. I turned off the PC I had been using for the Zoom meeting. My laptop was on as it has a built-in UPS, its battery. Not sure how long the power would be off, I shut it down. I also have an old XP desktop in my home office that now was quiet. It normally is always on, except during a power outage. The automated call we received from SDG&E indicated the power was estimated to be restored by 2:30 AM. I went around the house turning off light switches, in case it did come back on after we had gone to bed.

Around 9:30 PM the power came back on. I sent Art another text; he said the meeting had ended about 30 minutes earlier. The meeting had worked out fine despite my being powerless.

Next came the most annoying part of a power outage – resetting the many clocks that have no power backup. I also had to wait for the modem and router to come back up, for my Wi-Fi mesh router to restart and for all my Wi-Fi devices to reconnect. Since I’d need my desktop PC working in the morning to take my online health assessment so I could go into work in these COVID times, I had to verify it would boot up. I tried turning on my XP computer, but it would not show any signs of life. The last time I had shut it off I had problems getting it to start again. At the time, I thought the power supply has a problem but managed to get it running. Now I left its diagnosis for another time.

It turns out this outage was just a warm-up (pun intended) for another one we had about a week later. An excessive heatwave in the west meant the possibility of rolling blackouts instituted by the utility company. We had our power shut down for about 30 minutes, but this time it was around dinner time and still light outside. I’d at least learned my flashlight lesson and bought some lantern batteries a few days before.



With our hottest days in San Diego probably still ahead this year, we should count on losing power again soon. Whether due to rolling black-outs to reduce stress on the power grid or shut-downs to reduce wildfire risk, any of us could have that powerless feeling in our future. Now is time to prepare – stock up on batteries, get those UPS units working and back up and save your computer work often.