Interface

Lorain County Computer Users Group
www.LCCUG.cominfo@LCCUG.com
Volume 32 Number 8 August 2021

**Tuesday
August 10, 2021**

2021

Inside This Issue

PURCHASE DECISIONS FOR PRINTERS IN 2021

PRESENTED
BY

RAY BAXTER,
APCUG PRESIDENT & TREASURER;
PRESIDENT, PAYSON COMPUTER MEET-UP CLUB

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

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 UFA

A Word From Our President

Our **July** meeting was an interesting look at music over the years. Great nostalgia!! Ray Baxter of APCUG reviewed examples of songs and how they have been presented to us in various music formats over the years.

Ray maintains his master playlist online. With each song he chooses he provides background for the song and performer. It's very enjoyable, treat yourself

https://www.youtube.com/playlist?list=PLi6B6bF8hCO6u3hYsJKC9kZZ0EpY5OIuB

or https://bit.ly/3xfN9NF

Our **August** meeting will be an overview of choosing a printer. Ron Brown will present,
"How to make an informed decision when buying a 2021 printer." Ron is the Program Director of Silvercom Technology & Computer Club in Arizona and an APCUG speaker. He always does a nice job in his presentations.

Remember that we have links to recordings of our meetings and their handouts at our website: https://lccug.com/links/. If you missed a meeting and want to still watch it, that is where you need to go. If you were at a meeting and you want to review a portion of it for clarity – it is available to you at that link.

There is a lot of talk about the newest version of Windows that is projected to be released by the end of the year. I'm sure we'll be talking a lot about Windows 11 as we go along.

Now there is a new "wake" word you can set up with your echo. You can now use **Ziggy** as well as Echo, Computer, Amazon and Alexa. The other change you can make is to change the voice of your speaker from the usual female speaker to a male voice. This is kind of a refreshing change. It only works on the somewhat newer speakers. I recently gave one of my echoes the new "wake" word option – Ziggy.

Big and small, things are always changing in the technology world!

Sandra Ruth
LCCUG President

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

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!

Tuesday
August 10, 2021

PURCHASE DECISIONS FOR PRINTERS IN 2021

Presented By

Ray Baxter,

APCUG President & Treasurer;
President, Payson Computer Meet-Up Club

What are your options for choosing a printer in 2021? Selecting a printer to meet your printing requirements is very important. Many printers also function as scanners, copiers, and print your most cherished pictures. This presentation looks at the many choices you have and how to select the best device for you. Ron also discusses the many on-line services available in your community and the recent changes at Costco.

Ron Brown, Program Coordinator Silvercom Computer & Technology Club

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.

zoom

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. Canceled Until further notice due to Covid-19

Jean Copeland: **jecopeland1975@gmail.com**.

Executive Board Meeting Minutes

JULY 6, 2021

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

The July member Zoom program will be “Digital Asset Estate Planning” by Judy Taylour.

The board discussed programs for August and decided on Ron Brown’s program on printers.

The board set August 3 as the date to meet to view the LCCC computer facility in downtown Lorain.

The issue of using a copyright cartoon in the ***INTERFACE*** was discussed. No action.

Pam moved, Neil seconded the meeting be adjourned. Motion passed.

Genealogy Tip of the Day

Michael John Neill Genealogy Day 2021 Rootdig.com
mjnrootdig@gmail.com

Always Get the Widow’s Pension

04 Aug 08:38 AM

After the person of interest apparently died in Illinois in the 1870s, his wife, Susan, was married two more times and ended up surviving all three of her husbands. The last husband was a Union Civil War veteran and Susan qualified for a pension based upon his service.

There is a good chance that her widow’s pension application contains at least some brief details about her first marriage and how that marriage ended–including when and where that husband, the actual person of interest, died. Even though the third husband had no connection to the person of interest (other than marrying the same person), his military service could have resulted in a great way for me to locate information on the actual person of interest.

General Meeting Minutes

JULY 13, 2021

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

Sandee announced the August program will be about printers by Ron Brown,

Tonight's program by Judy Taylour was about “Digital Estate Planning “.

Judy did a great job in pointing out areas where we are vulnerable to fraud after we are gone and what we should do to prevent it from happening. We should have a digital executor which we have appointed and to whom we have given all of our digital accounts, logins and passwords. That is a big change in our perspective of our digital property.

Micky moved, Don seconded meeting be adjourned.

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 Lorain High School
2600 Ashland Ave, Lorain Ohio
[illegible] - [illegible]0 PM
Meeting rooms on the second floor.
Elevator access is available for those in need.

No Meetings at the College

LCCUG WORKSHOP
Class Ideas?

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

Please tell Neil or one of the other officers what you would like to learn and we will be happy to hold classes on your subject./subjects.

Neil Higgins **Education@lccug.com.**

No Meetings at the College

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 Password Managers by John Kennedy from APCUG

March 13, 2021 The Cloud is Here - Don't Get Left Behind - by Judy Taylour from APCUG

April 13, 2021 TeamViewer and AnyDesk - by John Kennedy from APCUG

May 11, 2021 Back Up Your Stuff - by Micky Knickman and Neil Higgins

June 15, 2021 How Technology Has Changed How We Listen to Music - by Ray Baxter APCUG

July 13, 2021 Digital Asset Estate Planning...

August 10, 2021 Purchase Decisions… By Ray Baxter APCUG

All other months to be announced.

Genealogy Tip of the Day

Michael John Neill Genealogy Day 2021 Rootdig.com
mjnrootdig@gmail.com

Do You Know the Location Genealogy?

michaeljohnneill, 01 Aug 10:49 PM

If your relative lived in an area before the current county in which it is located was formed, do you know the names of the parent counties? Is it possible that early records of your ancestor are in the county seats of those counties, which may be some distance from the county where your ancestor lived and several counties "over" from the current county's location.

Most counties in the United States have a genealogy–they just don't have two parents and four grandparents–grin!

Member of Association of Personal Computer Users Groups

amazonsmile

You shop. Amazon gives.

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
prihel1947@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 you. Thanks

LCCUG Ongoing Workshop

All Are Free And Open To The Public

Problem Solving Workshop

Date: Tuesday - August 17, 2021
Time: 5:30 - 8 pm Instructor: Micky Knickman, Neil Higgins, Richard Barnett
Place: Lorain County Community College @ 2600 Ashland Avenue, Lorain

Canceled

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 - August 17, 2021
Time: 5:30 - 8 pm Instructor: Sandee Ruth
Place: LCCC @ 2600 Ashland Avenue, Lorain

Canceled

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– August 17, 2021
Time: 5:30- 8 pm Instructor: Neil Higgins
Place: LCCC @ 2600 Ashland Avenue, Lorain

Canceled

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.

ScamBusters.org

INSTAGRAM SCAMS FOOL HUNDREDS OF THOUSANDS

PERSONAL INFO TARGETED IN MULTIPLE INSTAGRAM SCAMS: INTERNET SCAMBUSTERS #585

Instagram scams are among the latest con tricks to hit social networking sites.

Crooks are targeting the 150 million users of the photo-sharing site with phony offers aimed at stealing their identities or their cash.

We have the details in this week's issue, along with tips on how to avoid being scammed -- not just on Instagram but on all social networks.

Let's get started...

INSTAGRAM SCAMS FOOL HUNDREDS OF THOUSANDS

It sounds hard to believe but an estimated 100,000 people have willingly given away their usernames and passwords in an Instagram scam.

Instagram is one of the big players in the latest craze for image-sharing social networking sites. It's owned by Facebook and has more than 150 million members, many of whom use it to legitimately share family, fun and friendship photos.

It's also used legitimately by many celebrities and businesses to visually promote themselves.

Often, Instagram photos are cross-shared via other networks, like Facebook and Twitter.

And, just like most social networking sites, it relies on "likes" and other actions to spread connections, which makes it another ready-made target for scammers.

Internet security company Symantec reported two big Instagram scams towards the end of 2013.

In the first, an app that was available on most smartphones and other mobile devices promised to get users lots more followers.

In return, they had to provide their Instagram sign-on details, which, when you think about it, then gave the app maker the ability to log on to victims' accounts and use them to fulfill its offer of following others -- and do whatever else they wanted!

Remarkably, Symantec estimates that 100,000 people did just that, creating what the security firm called a "social botnet," a network of accounts that the app operator controlled.

Symantec reported: "(U)sers actually opt(ed) in to having their Instagram account externally controlled for the purpose of auto-liking and auto-following others. When we tested the application, right away our Instagram account began liking pictures without any consent or interaction from us."

But that's not all. The app then started asking users to pay to get new members via a "virtual currency" -- "coins" they could buy with real dollars.

Users were also offered free coins if they recommended the app to others.

(Continued on page 8)

Newsletter Editor: Pam Rihel using Microsoft Publisher, 2016

This Month's contributors: Micky Knickman, Sandra Ruth, Pam Rihel, Don Hall, Dennis Smith, Neil Higgins, Michael John Neill, Scambusters, APCUG, Leo Notenboom, Cal Esneault, Dorothy Fitch, Greg Skalka, Google images, Microsoft Office art online,

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.

(Continued from page 7) **INSTAGRAM SCAMS FOOL HUNDREDS OF THOUSANDS**

It's not known if the sign-on details the app maker obtained were used for any other sinister purpose, like trying them out on other accounts.
Action: The app has since been removed from online stores but if you were a victim, you should change your password.

You should never provide sign-on details to a third party, and always use different passwords for every account.

ANOTHER 100,000 FOOLED

Just a few weeks after that incident, Symantec reported that another 100,000 Instagram users had fallen for a hoax in which they received a message saying a huge number of accounts were going to be randomly deleted.

Victims were asked to repost the picture announcing the supposed deletion, on their pages, in effect causing them to "follow" the hoaxer's own account.

The account was subsequently deleted, with no real harm apparently done.

"However," says Symantec, "the message is clear: social network users are constantly targeted by scams, spam and hoaxes and these campaigns succeed, which is why those responsible for them keep pursuing them."

Action: If you're an Instagram user and receive any warnings or other messages that purport to come from the site, check Instagram's blog.

Better yet, follow the official Instagram account, where you will see all legitimate updates.

YET MORE SCAMS

As if to echo Symantec's warning, a number of other Instagram scams have been uncovered in the past few months.

Many of them are photos offering free air tickets or other gifts in return for taking actions like reposting, tagging, following, commenting and so on.

No need to go into the details of what each of these terms means here. If you're a social networker, you'll likely know.

But the effect is to direct more and more attention to the scammer's posting, which often contains a link that leads to a page either laden with advertising or hosting malware that infects your PC.

According to the Internet tech news and intelligence site Mashable, other recent Instagram scams include:

- A claim by a scammer that he/she knew a trick that would add zeroes to a $2 Green Dot Moneypak card.

All you had to do was buy the card and tell the scammer the number, which, of course, he/she promptly spent!

- A student loan forgiveness hoax, which again requested victims to follow.

The scammers set up an account using the name of the official student loan organization known as Sallie Mae and claimed 150,000 students' loans were to be canceled.

Students who fell for it were asked to provide personal information, which was then used for identity theft.

- A dieting scam using before and after photos purporting to show the same woman after she had followed the diet plan.

Mashable noted: "Weight loss scams are rampant on Instagram. The mobile photo app lends itself perfectly to this type of scam, because it's easy to post oh-so-convincing before and after photos."

The tech site said the supposed product did exist but, according to reviews, didn't work at all.

(Continued on page 9)

(Continued from page 8) INSTAGRAM SCAMS FOOL HUNDREDS OF THOUSANDS

Sadly, there are many more Instagram scams, some of them trying to convince victims they're genuine by highlighting other scams.

HOW TO AVOID THE SCAMMERS

What can you do to avoid being snared?

First, be wary of any site supposedly belonging to a company like an airline that specifically offers giveaways and nothing else.

As Mashable says: "Why would a company create a new profile just for promotions and have to build up a following all over again, when they already have a profile?"

If there's only one picture posted on the account, that should immediately raise a red flag.
If the posting purports to be a competition, check if the rules and regulations are shown.

Watch out for links with shortened domain addresses. Crooks use these to hide their real Internet location.

See this Scambusters report for more on this trick, How to Spot and Stop a URL Shortner Scam.

Finally, of course, don't give away personal information, including passwords and bank or credit card details, to someone you don't know.
That applies to all social networking sites, no matter how tempting the offer. In fact, the more tempting, the more likely you're being lined up for an Instagram scam.

Ask Leo! by Leo Notenboom

Should I Update to Windows 11? When it's time, you'll know.

by Leo A. Notenboom

Windows 11 has been announced to much fanfare, hype, and confusion. Windows 11 certainly isn't ready for prime time, and likely not ready for you.

Applies to Windows: 10

The questions have started rolling in, and I have an answer prepared.

While my most common answer — "It depends" — certainly applies, I'm going to go one step further.

No. No you should not update to Windows 11 yet.
Let me share my reasons.

Is Windows 11 for me?
Windows 11 has not yet been released, and is not yet ready for general use. The requirements are confusing and likely to change. There's no compelling reason to upgrade at this time. Windows 11 is not something the average consumer should even be concerned about until its actual release, and even then, it'll be worth waiting a while longer.

It's not yet released
The single most important reason not to update to Windows 11 is very simple: IT HASN'T BEEN RELEASED YET.

Yes, there are pre-released beta releases, test versions, and whatnot. Those are not for you. Those are for developers and technologists (and, sadly, over-eager reporters) to try out

(Continued on page 10)

(Continued from page 9) Should I Update to Windows 11...

the technology, give Microsoft feedback, and just generally play around with it.

What's important to understand about Windows 11 in its current form is that it'll break, perhaps seriously, perhaps annoyingly, and it'll change, perhaps a lot, before it's released.

It's not done.

And it won't be until the end of 2021 at the earliest. I'd expect 2022 for general availability.

The requirements are confusing and likely to change

One of the most frustrating aspects of Windows 11's announcement is the changing system requirements.

To me, Windows 11 really feels more like a Windows 10 feature update, except for this change. Renaming it Windows 11 allows Microsoft to more easily change the minimum requirements to run the system.

Initial results are really confusing. Even machines with TPM (a new requirement — Trusted Platform Module chips) are being told that they can't run Windows 11. In fact, many machines, even newer ones, are failing the compatibility test.

Yes, there are workarounds for some of the issues. Are those workarounds going to work when Windows 11 releases? Your guess is as good as mine.

More pragmatically, are the requirements going to remain unchanged, given the large number of systems that apparently won't meet them? It seems possible, if not likely, that the requirements might be "adjusted" based on feedback and publicity.

There's no compelling reason

Windows 11 feels like a Windows 10 feature update, and there's nothing terribly compelling about the features listed so far.

And of course, they're changing the Start menu. Again.

If there were something truly exciting about Windows 11, I might be more interested. Most of the features I've seen announced are either borderline boring, or available already via other means.

Aside: the every other version "curse"

This isn't a reason, but . . . well, maybe it is.

Windows XPPopular

Windows Vista: Not so much.

Windows 7:Popular

Windows 8/8.1 :Not so much.

Windows 10: On over a billion machines. Very popular.

Windows 11???

It's as much superstition as it is anything else, and by itself, it's not a reason to avoid anything.

And yet. There does seem to be a pattern.

Make of it what you will.

If you know, you know

There are people who can, should, and will play with Windows 11. That's why it's available now, before it's done. Those folks will give valuable feedback to Microsoft and expose to the rest of us just what Windows 11 is or will be all about.

Those people know who they are. They know how to stay safe, and they know why they want to play with unreleased software.

If you don't know — if you have to ask — then Windows 11 is not for you.

Not yet, anyway.

(Continued on page 11)

NEW!!!

$5.00 given away to members joining our meeting. If your name is called you will receive the full amount, no matter how many names we pull before someone is at the meeting.

(Continued from page 10) Should I Upgrade to Windows 11

Maybe when it's done.

Related Questions

Will Windows 11 be a free upgrade?

Initial indications from Microsoft are that Windows 11 will be a free upgrade for compatible machines running legitimate Windows 10 installations. It's unclear if there's an upgrade path from older versions.

Can I get Windows 11 now?

You can get Windows 11 now by joining the Microsoft Insiders program. Unless you are a developer or have specific reasons to play with this unfinished product, you should avoid it until it's been released.

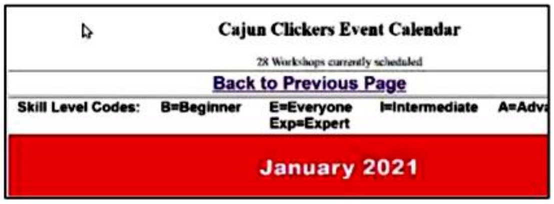
Windows 11 release date?

Microsoft has not yet provided a specific Windows 11 release date, saying only that it'll be available on new machines in late 2021, and upgrades to existing compatible machines sometime in 2022.

Changing the Mouse Pointer

By Cal Esneault, former President of CCCC and leader of many Open-Source Workshops & SIGs
Cajun Clickers Computer Club
February 2021 issue, CCCC Computer News
www.clickers.org office@clickers.org

A key item in the Windows desktop graphical interface is the "pointer" (controlled by either a mouse or by a laptop touchpad). Since we use it often, finding it quickly makes our sessions more efficient. The default setting has a white pointer with a black outline. It can take time to locate when on a white background (see screenshot below)



Cajun Clickers Event Calendar

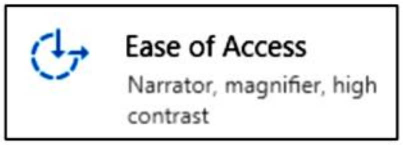
28 Workshops currently scheduled

Back to Previous Page

Skill Level Codes: B=Beginner E=Everyone Exp=Expert I=Intermediate A=Adva

January 2021

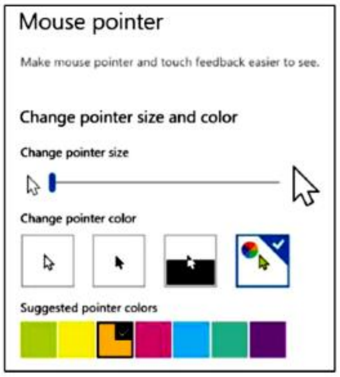
Windows 10 (as with previous versions) gives us an easy way to customize this pointer. From the "Settings" menu, chose the "Ease of Access" item (see below)



Ease of Access

Narrator, magnifier, high contrast

Pointer options are shown below.



Mouse pointer

Make mouse pointer and touch feedback easier to see.

Change pointer size and color

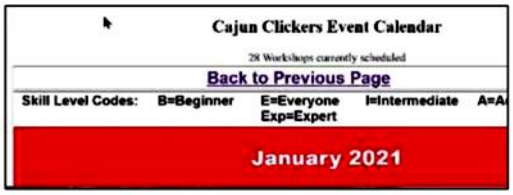
Change pointer size

Change pointer color

Suggested pointer colors

You can change the color of the pointer to any other basic color that you desire.

For example, below the cursor has been changed to a black fill (with white outline) over the same screen as seen earlier. This may allow for improved recognition. Other colors can be selected based on your preference (for example, green or yellow).



Cajun Clickers Event Calendar

28 Workshops currently scheduled

Back to Previous Page

Skill Level Codes: B=Beginner E=Everyone Exp=Expert I=Intermediate A=A

January 2021

You can also choose the "inverted" option. This changes the color of the pointer depending upon the color of the background. Thus, better contrast is automatically selected, but you must reconcile your mind-muscle connection to accept the fact that the cursor will not always be the same color.

In the mouse pointer dialog, there is also a slider to change the size of the pointer. By default, it is set to "1", but you can make it larger (for example, "2" or "3) using the slider. This improves recognition, but it takes some getting used to having a large object constantly moving on your screen.

As with any personalization setting, results vary based on your perception of what is "better". Give it a try to see if this helps. There are many other ways to customize the screen, text, taskbar, dark mode, etc. Search the internet to see if you can find somethat improve your situation.

ScamBusters.org

COPY AND PASTE PLEA EXPOSES YOUR IDENTITY

WHY YOU SHOULD BE WARY OF FACEBOOK COPY AND PASTE REQUESTS: INTERNET SCAMBUSTERS #801

What crosses your mind when a Facebook friend asks you to copy and paste their post rather than just sharing it?

Their intention may be a genuine attempt to widen the spread of their message -- but there's also a downside if the original poster was planning to harvest information about you.

In this week's issue, we'll explain the risks of copying and pasting, as well as highlight a couple of other tricks to be wary of.

Now, here we go...

If you're a Facebook user, have you ever wondered why some of your "friends" post items they ask you to copy and paste rather than share?

Do you feel a little uneasy about why they asked you to do this?

Well, of course, they likely didn't ask you. They simply copied and pasted the item themselves that one of their friends previously posted -- and the request to pass it on in this way was already built in.

The trail goes all the way back to the original poster. It's a sort of chain letter, which aims to reach as wide an audience as possible.

But why? Is it a scam?

Its purpose could certainly be dubious -- but not always. First, you need to understand something important about the way sharing and copy/pasting work on Facebook.

In very simply terms, when you share a post from someone who has tightly controlled privacy settings, their privacy status effectively restricts who can see it. It can't be made "public" and may not even be further shareable.

But when you copy and paste an item, you're really creating a new post that can be seen by all your friends and beyond. In other words, it gets wider circulation.

So, you're being used to help amplify a message. That may or may not be a good thing depending on its content.

But that's not all. By copying and pasting, you're effectively enabling the original poster to track everyone else who is repeating it.

How?

The original poster inserts some text with a couple of spelling mistakes in the message. Then they do a search using the misspelt phrase. This returns a list of everyone who has copied and pasted the message.

Now, let's say the message was about gun control, animal abuse or another contentious subject.

The original poster will now have a list of people who seem to support his/her cause and they can go about trying to contact them via Facebook with "friend" requests and other messages. Their findings could also contribute to a profile of you that some marketing and research companies build.

Furthermore, the original poster can delete their message and, therefore, not be easily traceable, while the copied-and-pasted versions live on.

That's not what happens with a shared message. If you delete something you shared, all the forward-shared versions of it disappear as well.

AMEN TO THAT

The same tracking tactic works for any message. You know, the type that says something like, "If you agree, comment 'Amen'." Again, by doing a search, the original poster will be able to identify all his/her supporters.

Copy-and-pasting can also be used for other sinister purposes. For instance, if the original message is a hoax or fake news of some sort, the copy and paste version becomes much more difficult to delete because each is effectively a new original.

So, as mentioned above, while deleting a shared message would remove the entire chain of forward shares (note, not earlier shares), that wouldn't happen with a copy and paste.

And, again, the original hoaxer could delete their message to keep their own identity secret, while their false message continues to circulate.

Another chain-style trick that sneaky Facebook users apply is to solicit information about you by offering to tell you something trivial about yourself, like which celebrity you most resemble, or which one would make you a perfect partner, or some other trick created to pique your curiosity.

They might ask your birth date, your favorite color or even your mother's maiden name.

See where this is leading? You're giving information about yourself that potentially could be used for identity theft.

Plus, by taking part in this "game," your celebrity identity (or whatever) is entered into the post's comment field, which means the message will now most likely go to your friends. And so it goes on.

So before copying and pasting, adding "Amen" etc., or playing the celebrity game, it makes sense to pause and consider the possible implications of what you're doing -- and the information you're giving away about yourself.

The original poster's intentions may have been perfectly honorable. Or maybe they're not. And you may not find out until it's too late.

Google Voice and Its Many Uses

By Dorothy Fitch, Editor, GVR Computer Club
March 2021 issue, Green Bytes
https://www.ccgvaz.org/ dmfitch@cox.net

I recently had a use for an additional phone number. Google Voice to the rescue! It's free (for calls within the U.S.), works nicely, and is easy to use. Here is what I learned in the process.

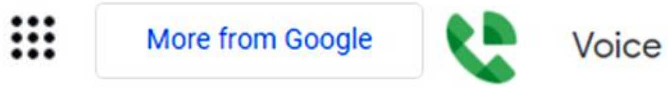
What is Google Voice? Google Voice is a software tool that allows you to obtain a free phone number. It can't be your only phone number and you need a Google account. You can set up a Gmail account for free if you don't already have one. It doesn't require any hardware or physical phone (other than what you already own).

Why would you want an additional phone number? Here are a few reasons:

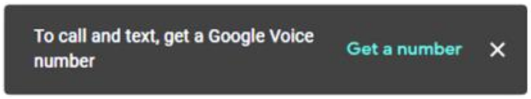
- You temporarily want a phone number that you can delete later.
- You want a phone number for a different U.S. city.
- You have a side gig, perhaps selling hand-crafted items, and don't want to use your own phone number for that business.
- You want a phone number for specific people to use, such as family members.

I recently read of two teachers in Maryland who set up a Google Voice phone number for seniors to call if they needed help setting up a Covid vaccination appointment. The possibilities are endless.

How do I sign up? To get started, go here and sign into your Google account. If you are already logged in, click on the grid of nine dots for Google apps at the upper right of the screen. Scroll to the very bottom and click "More from Google". Then scroll down until you see the Google Voice icon and click on it. Here are the icons to click on.



You now see the "dashboard" for your voice account, even though you don't yet have a number. To get your number, click the box at the bottom that prompts you to get a Google Voice number.


To call and text, get a Google Voice number

Type in the location where you want the phone number to be based, then choose your new number from a list of available ones. It can be either in your local area or else where in the United States.

How does it work? Calls to your new number will forward to a number you specify. It might be your cell phone or landline. The number it forwards calls to is your linked number, and you can set up more than one number to ring at the same time. You can also edit the name for the number that will appear on the recipient's caller ID.

One of the settings lets you see the number that the person dialed, as opposed to the number of the phone it is linked to. That lets you know that they are calling the Google Voice number. Adding that number with an identifying label to your Contact list shows you immediately the number the caller dialed. This allows you to answer the phone with a different greeting if you want.

You can also create a personalized message that people hear when they leave a voice mail. The default message, designed to eliminate spam and automated calls, asks the caller to speak their name so you get to decide whether or not you want to take the call.

When someone leaves a message at the new number, you can listen to it in your account dashboard, where a text version is also stored. You will also receive an email at your Gmail account when someone leaves a message.

There are dozens of settings you can adjust in the app or your computer dashboard. For example, you can limit the hours that phone calls to the number will ring (a "Do Not Disturb" setting). You can set up more than one phone to ring at the same time if you want. Be sure to have the other phone handy so you can enter the verification code that Voice will send you before it links the device to the number.

This is the article that convinced me to give Google Voice a try:

www.businessinsider.com/what-is-google-voice-how-to-set-up-use

For complete instructions on setting up Google Voice, go here.

All in all, it's a very powerful tool and may be just what you need.

President's Corner

Do You Trust Your Technology?

by Greg Skalka, President, Under the Computer Hood User Group
www.uchug.org president@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 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

(Continued on page 15)

(Continued from page 14) Do You Trust Your Technology?

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 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 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.