Interface

Lorain County Computer Users Group
LCCUG.com (or) info@LCCUG.com
Volume 33 Number 12 December 2022

Lorain County Computer Users Group
Users Helping Users

2022

Inside This Issue

Thursday
December 15, 2022

Get Ready for Our Holiday Lunch At Golden Corral

See page 3 for more information

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

A Word From Our President

Well, I blinked and it happened it again. The year is almost over!! Unreal how that keeps happening!

At our November meeting we had Glenn Pubal return and talk to us about computer trends and what he foresees happening this year. He brought his young assistant, Joel, with him who gave us his perspective on several technology issues. It was great to have such a knowledgeable & vibrant presenter in person!!

Glenn left us several nice prizes that we will use at our Christmas lunch meeting.

Hopefully most of you can come to our holiday lunch at Noon on **THURSDAY**, **December 15** at the Golden Corral Buffet Restaurant in Elyria. 1519 W. River Rd, N., Elyria. Ten dollars of the lunch cost will be rebated for each paid membership (1 per paid membership). Golden Corral charges $9.89 for senior early bird lunch (includes beverage) for ages 60 & up. We will have raffles and make a donation to Second Harvest food bank.

It would be very helpful if members would email us at info@lccug.com if they plan on attending.

Watch your email for details.

What next year holds for us is up to our members. We need the input from each of you if we are to keep going. We hope to continue with our hybrid meetings that will meet both in person and on ZOOM. What will make it useful, convenient and valuable to you?

The November meeting with Glenn Pubal can be found here: https://www.youtube.com/watch?v=gwQRYoE-ke0

Sandra Ruth

LCCUG President

LCCUG Officers For 2022

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	**Vacant** membership@lccug.com
Director of Advertising	Richard Barnett advertising@lccug.com
Director of Education	Neil Higgins education@lccug.com

Thursday
November 15, 2022

Get Ready for Our Holiday Lunch

Mark your calendar for meeting on
Thursday
December 15, 2022
at Golden Corral in Elyria at 12:00 P.M
Note the day change from Tuesday to Thursday
Come and enjoy a fun afternoon with family & friends
We are looking forward to seeing you all there.
There will be a 50/50 drawing
Other prizes to be announced at the luncheon.

Look for more information on our Website or email: info@lccug.com

Woohoo!

Your renewal dues have been changed from $15.00, To 3 years for $15.00. When everyone else is raising their prices our Computer Club is lowering their dues, so tell your friends to come and Join in the fun and learn computer information.

Tell your family and friends about this great deal. Once in a lifetime opportunity.

Executive Board Meeting Minutes

NOVEMBER 1, 2022

The October board Zoom meeting was attended by Sandee Ruth, Don Hall, Micky Knickman, Pam Rihel and Richard Barnett.

Sandee will mail out a flyer to all members announcing the November 8 meeting with Glenn Pubal of Royal Business speaking on the latest in the Intel world.

Also included in the flyer will be information on the December 15 ,Thursday, holiday luncheon at Golden Corral with cost and 50/50 raffle.

Pam Rihel moved, Richard Barnett seconded the

Member of Association of Personal Computer Users Groups

Computer Club News

Don't Bring in Your Used Ink Cartridges. LCCUG is not collecting them as we have no recycling options anymore. Thank you to all who have supported us in collecting the ink cartridges.

General Meeting Minutes

NOVEMBER 8, 2022

President Sandee Ruth called the combination in-person / Zoom video meeting to order. A motion to accept the minutes as shown in the November issue of the *INTERFACE* was made by Ellen Endrizal, seconded by Bill Schubmehl. Motion passed by voice vote.

Sandee explained the December meeting will be held at Noon on Thursday December 15th at the Golden Corral.

Glenn Pubal of Royal Business gave an interesting program describing the "PAST/PRESENT/FUTURE" of computing. There were many questions asked by attending members.

Newsletter Editor: Pam Rihel using Microsoft Publisher, 2016

This Month's contributors: Micky Knickman, Sandra Ruth, Pam Rihel, Don Hall, Neil Higgins, Michael John Neill, Scambusters, Ask Leo, APCUG, Google images, Microsoft Office art online,

Newsletter is now
Online at:

lccug.com/newsletters or lccug.com

MEMBERSHIP WITH LCCUG:

Yearly dues are now $15.00 For 3 years. For more information contact:

LCCUG
Director of Membership,
membership@lccug.com.

Meeting Location:
At a new time: from 10 am. - noon
in a new location: LCCC facility at
201 W. Erie, Lorain

Our meeting space is on the first floor – easily accessible – larger – refreshments available! Please email info@lccug.com if you have any questions.

Lorain County Computer Users Group

2022 Calendar of Events

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

Using Zoom & In Person

Meeting & program starts at 10 am

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

January 11, 2022 - Useful Websites and Utilities presented by our Board Members and Our members

February 8, 2022 - Preserving Digital Photos By Mark Schulman

March 8, 2022 - The Pro's and Con's of BACKUPS; introducing "Tech for Senior"

April 12, 2022 - Geeks On Tour Presented by Google Lens

May 10, 2022 - Cyber-Safety in the Digital Age Presented by Norbert "Bob" Gostischa,

June 14, 2022 - Snapseed – Presented By Chris and Jim Gould

July 12, 2022 - Bringing Up Baby starring Cary Grant and Katharine Hepburn

August 09, 2022 - Discover more about using YouTube

September 13, 2022 - Cool Websites & Apps

October 11, 2022 - Health-related apps for the smartphone and the smartwatch

November 8, 2022 - To Be Announced

December 15, 2022—Notice the date change- it will now be on Thursday. Holiday Lunch being held at Golden Corral in Elyria at NOON

Please check our website LCCUG.com for more updates. If you have anything you would like to know about, PLEASE let up know. We would really like your input.

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.

Interesting Internet Finds

August 2022

by Steve Costello
scostello@sefcug.com

Windows 11 Has A Secret Start Menu — This Is How You Can Access

https://trendblog.net/windows-11-has-a-secret-start-menu-this-is-how-you-can-access/

I now have a Windows 11 PC, as my primary desktop completely died so I had to get a new one. My worst problem, so far, has been getting used to the new start menu. This post has been helpful to me, check it out if you end up going to Windows 11 yourself.

NEED HELP?

CALL FOR HELP! Computer Services

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 5:00 am to 3:00 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 or 440-308-8196
6:00 p.m. to 9:00 pm Monday thru Thursday
Genealogy help
prihel1947@gmail.com

Denny Smith Unavailable at this time
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 Workshops

All Are Free And some are Open To The Public

Problem Solving Workshop

Date: Tuesday- December 13, 2022
Time: 12PM –Please show up by 12:30 Instructor: Micky Knickman
Place: LCCC @ 201 W. Erie Ave., Lorain, OH

Canceled

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

This workshop is limited to LCCUG members in good standing.

The Problem Solving Workshop is being held at our new building, LCCC, 201 W. Erie Ave. Lorain, Ohio

You are asked to bring in your computer, laptop and other electronics that you need help with unless the problem/question can be replicated on any device.

Learning About Electronics

Date: Tuesday - December 13, 2022
Time: 12PM –Please show up by 12:30
Instructor: Sandee Ruth
Place: LCCC @ 201 W. Erie Ave., Lorain, OH
Learn how use you electronic devices.

Canceled

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

LCCUG WORKSHOP Class Ideas?

Neil would like some ideas on what type of projects you are interested in learning about. Contact:

Neil Higgins Education@lccug.com.

Officers Nominations

Elections of Officers 2023

Elections to be held at the December 8th Meeting

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

Webpage Editor Richard Barnett
webpage@lccug.com

Statutory Agent Sandra Ruth
statutory_agent@lccug.com

Director of Membership: Vacant
membership@lccug.com

Director of Advertising Richard Barnett
advertising@lccug.com

Director of Education Neil Higgins
education@lccug.com

If you would like to run for one of these offices, please contact any officer and let them know which office you would like to be nominated for.

Thank you and hope to see you all Thursday Dec.15, 2022 for our Holiday Lunch. Step up and become an officer; your dues are paid for by the club.

We are depending on you to volunteer and help the club out with your new ideas.

Happy Holidays

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

John Kolb
secretary@loraincoogs.org

LCCUG is on Facebook

Come and visit our Facebook page for interesting facts and ideas. You can get a lot of computer information from our Facebook page. Have a question ask it on Facebook.

https://www.facebook.com/groups/lccug

Genealogy Tip of the Day

michaeljohnneill,
Rootdig.com mjnrootdig@gmail.com

Who Died and Made You Administrator?

If your relative died without a will and there was a need to probate the estate, an administrator would need to be appointed. The spouse and heirs usually have priority in being appointed to that office. Spouses can refuse their right of acting as administrator and children may or may not choose to accept the position.

Heirs other than children may be administrators or creditors may choose to accept the role as well. But if the name of the administrator doesn't "ring a bell," research them to find out (if you can) what their relationship was to the deceased person whose estate they are being appointed to administrate.

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 OFTHOUSANDS

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!

More Scam Reports: SCAMMED! Don't Let What Happened To These Victims Happen To You

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.

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."

More Scam Reports: ID Protection: How to Hide Yourself on the Internet

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

(Continued on page 9)

(Continued from page 8) Instagram Scams...

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 student's 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.

More Scam Reports: Red Flags Signal Possible Investing Scams

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.

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 Shortener 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.

Copyright Audri and Jim Lanford. All rights reserved. Reprinted with permission. Subscribe free to Internet Scam-Busters at
http//www.scambusters.org

Genealogy Tip of the Day

michaeljohnneill,
Rootdig.com mjnrootdig@gmail.com

The 0th Birthday

The “0th” birthday sign was a literally correct age for the human who had arrived a few days before.

Technically, in most cultures, a person is considered by 0 years old at the moment of their birth. It’s also reflective of the age many records use to list individuals within the first 12 months of their birth.

And it’s difficult to get mixed up on whether someone is 0 years old or 1-year-old–even if there is no record of their birth. But as that person ages, it’s easier for a record to be a off or inconsistent with other records. It’s more difficult to be off by much when someone is under the age of 3. When that person with no birth record has aged to their seventies, it’s much easier to be off a year or two on their age.

The older a person gets, the more their age is to vary especially if they do not have a record of their birth and someone else is determining their age for them.

Please Set Up and Maintain Account Recovery Information

Without it, you risk losing your account forever.

by Leo A. Notenboom

Account recovery information is an important yet often overlooked part of account security. Managed poorly, it can lead to permanent account loss.

Some Gmail account recovery options. (Screenshot: askleo.com)

It might be as important as backing up. It's certainly close.

The number of people I hear from desperately trying to regain access to their accounts would surprise you.

The number of people who'll never regain access would surprise you more. I see it at least daily.

It doesn't have to be that way!
Set up recovery info

Recovery information is crucial to regaining access to your account if you can't sign in for any reason. Make sure not only to set it up, but *keep it up to date*. I see many accounts permanently lost because recovery information was either out of date or never set up at all.

Recovery information has one purpose

You know you are who you say you are. If you lose your password, all indications are that you are *not* who you say you are. If you were the rightful account holder, after all, you would know the password.

I know, I know! That's not the case if someone has hacked you or you lost that little green notebook with all your passwords scrawled in it. But the service has no way of knowing that. Your username/password combo[1] is how you prove to them you are who you are.

What most services do realize, though, is that people are people. Sometimes we forget our password. Sometimes our accounts are hacked.

Recovery information is an alternate means for you to prove you are who you say you are and should be given access to the account. You must set up recovery information before you need it.

The reason recovery information works is because you set it up *while you have access to your account*. It's information you add to the account in case of future problems.

Hopefully, you'll never need to use it. But you must set it up, just in case.

If you never set it up, then should your password ever stop working, you'll have no way to prove you are authorized to access the account.

You must keep recovery information up to date. Honestly, most people facing account loss due to failed recovery attempts *did* set up recovery information when they set up their accounts. That's good, but it's not enough.

Many of these accounts are years old (and that's one reason you care so much about it). The recovery information you might have configured back then falls out of date. Maybe your recovery phone number is no longer in use, or your recovery email address has long since disappeared, for example.

Out-of-date recovery information is just as bad as not having it at all.

It might even be worse if it gives you a false sense of security. You must keep it up to date. Check it periodically (some services now occasionally prompt you to do this), and/or proactively update it when something changes.

Type of recovery information

These are the kinds of things we're talking about here.

Alternate email addresses.
Make sure you still have access to the email account to which the recovery code will be sent. If you do not, recover *that* account or configure a different one.

Mobile phone number. Contrary to conspiracy-minded folks, this is not used to gather more tracking data on you. (The mobile services already have plenty.) Make sure that any mobile number configured in your account is a number at which

(Continued on page 11)

(Continued from page 10) Ask Leo

you can currently receive a text message. If you change numbers, make sure to change your recovery information. If you lose your mobile, replace it quickly and have your phone number ported to the new device; text messages are tied to your mobile number, not a specific device.

Landline phone number.

This is less common, but some services allow you to use a landline and call you with a recorded confirmation code in case of recovery. Like a mobile number, if your landline number ever changes, make sure to change it in your account recovery information.

Recovery codes.

This is also less common, but doesn't suffer from issues relating to change. Some services let you generate one or more "recovery codes" — random numbers that, in the event of password failure, can be used *once* to sign in to your account. The issue here is that you must create and save them somewhere secure so they're available when needed.

Secret questions.

Some services still use them, but they should not. It's been shown that they're often guessable and significantly less secure. If you have a choice, use one of the alternatives above. If you have no choice, make sure you do not forget the answers to the questions you choose.[2]

Do this

Set up account recovery information and keep it up to date.

You run the very real and serious risk of losing access to the account if you do not.

For other ideas on staying safe, reducing risk, and using your technology with more confidence, subscribe to Confident Computing! Less frustration and more confidence, solutions, answers, and tips in your inbox every week.

ScamBusters.org

HOW TO IDENTIFY, REMOVE, AND PROTECT AGAINST MOBILE SPYWARE, CROOKS SWITCH TO MOBILE SPYWARE AS USERS MOVE FROM PCS TO PHONES AND TABLETS: INTERNET SCAMBUSTERS #1,034

Mobile spyware - apps that track you and steal information from your phone or tablet - is on the rise.

Android devices are most affected, but it can also turn up on iPhones and iPads.

Cell phones and other mobile devices are increasingly under attack from spyware and other malicious software.

As more consumers switch from using desktop PCs to mobiles for their day-to-day online browsing, hackers and scammers are doing the same.

Furthermore, they've gotten their hands on highly sophisticated surveillance apps previously only used by big organizations and governments.

The full range of mobile spyware stretches from basic stalkerware capable of monitoring a user's location, text messages, and phone calls to malware capable of reading keystrokes and stealing confidential information.

Stalkerware is widely available online and is used legally for monitoring kids' activities and, more dubiously, the activities of employees or spouses and partners under suspicion from their other half.

We covered stalkerware in an earlier issue: Stalkerware Sees and Hears Everything on Your Phone + Coronavirus Latest.

The worry now is that crooks are finding ways to install dangerous and intrusive spyware on smartphones and tablets, which can be used to collect data for identity theft.

By far the biggest threat targets smart phones using Google's Android operating system but Apple's iPhone and iPad are not immune to attack. Experts say that Android accounts for up to 98% of spyware infestation, with the remainder on Apple devices.

(Continued on page 12)

(Continued from page 11) How To Protect Against Mobile Spyware

More Scam Reports: Spybot Search and Destroy

Just a few days ago, an updated version of one of the most damaging pieces of Android spyware, known as Banker, was detected. It infects phones via a link in a text message and is capable not only of stealing data and monitoring all of a phone's activity but also of detecting and secretly deleting additional (multi-factor) security codes.

In other cases, many victims bring troubles on themselves by not using the two companies' official app stores, where programs are rigorously checked for malicious code.

Using other app sources is relatively easy on Android - using settings or an app to allow this, known as "rooting." Apple devices have to be "jailbroken" with special software before they can be used in this way. However, crooks have still managed to get malware onto regular phones using "zero-day exploits" - security vulnerabilities on installed apps before they're found and fixed.

As we discussed in our stalkerware issue, it's also easy for anyone who has access to your device to manually install spyware, which, once set up, can be hidden from view.

In a recent update, security specialist Check Point says: "The current mobile malware landscape is a minefield with more and more vulnerabilities being exploited and spyware software being deployed."

The firm specializes in commercial clients, but it's concerned that individuals whose mobiles become infected may then also provide access to corporate networks.

"Our phones are hubs of confidential data, both personal data such as banking information as well as business data," it says, "with many employees now connected to their company's networks and data via their mobiles, which multiplied over the pandemic with thousands working from home.

More Scam Reports: Social Security Administration scam alert, am I really getting more spam, and am I being too paranoid?

"Cybercriminals are utilizing this silent and persistent practice to gain as much access as possible."

IS MY PHONE INFECTED WITH MOBILE SPYWARE?

It's not always easy to know if you have mobile spyware on your device. Some malicious apps are totally hidden. But if it seems to be behaving strangely, like overheating, slowing down, or the battery seems to be draining faster, that could be a sign of infection.

You may also see apps you didn't install, messages you didn't send, higher than usual data usage, unexpected opening when your device is in standby mode, or strange words that keep popping up during autocorrect.

HOW TO PROTECT YOURSELF AGAINST MOBILE SPYWARE

As always, the most important protection against mobile spyware is to install, auto-run and regularly update security software. There are even some apps that specifically look for spyware and others that can tell if your device has been rooted or jailbroken.

Other actions you can take include:

- Keep your operating system and individual apps up to date with the latest versions, which usually include security fixes.
- Don't allow others to use your device or to know your passwords. Always keep it locked too.
- Don't root or jailbreak your device.
- Only use the two official app stores for downloads.
- Don't click on links in texts or emails from unknown sources. And even be wary of links from people you do know - their account may have been hacked.
- Check app settings and use the strongest privacy ones, especially to avoid giving away your location.

Use a virtual private network (VPN) to cover your online tracks. We wrote about VPNs here:

Do You Need a VPN (Virtual Private Network) for Your Internet Safety?

Interesting Internet Finds
July 2022

by Steve Costello
scostello@ sefcug.com

While going through more than 300 RSS feeds, I often encounter things I think might interest other user group members. The following are some items I found interesting during July 2022.

Google One Explained: Is It Worth Subscribing To?

https://helpdeskgeek.com/reviews/google-one-explained-is-it-worth-subscribing-to/

If your 15GB Google Storage is not enough, check out this post that explains just what Google One is, how it works, and its advantages and disadvantages. (Note: I have already been using different options, so I decided this was not worth it.)

Does Your Internet Provider Know That You're Using A VPN?

https://www.reviewgeek.com/122229/does-your-internet-provider-know-that-youre-using-a-vpn/

If you use a VPN to obscure your identity, this is a good post to read.

How To Find Out Which Kindle Model You Have

https://www.online-tech-tips.com/computer-tips/how-to-find-out-which-kindle-model-you-have/

If there is a problem with your Kindle or you need an accessory for it, you will need to know which model you have. Check out this post to learn how.

Tor Browser's Connection Assist Takes The Frustration Out Of Censorship Circumvention

https://www.ghacks.net/2022/07/16/tor-browsers-connection-assist-takes-the-frustration-out-of-censorship-circumvention/

If you use the Tor browser you should read this post.

Wordpress Users Need To Watch Out For Fake Copyright Infringement Warnings

https://www.techlicious.com/blog/wordpress-users-need-to-watch-out-for-fake-copyright-infringement-warnings/

Are you a Wordpress user? If so, you need to read this post so you know how to protect yourself.

How To Spot Fake Amazon Reviews

https://www.dailybits.com/how-to-spot-fake-amazon-reviews/

I get a lot of stuff from Amazon, and I am always looking for ways to spot fake reviews. Sometimes the fake reviews are to make us buy certain items or sometimes not to get them.

****