Interface

Lorain County Computer Users Group
LCCUG.com (or) info@LCCUG.com
Volume 35 Number 2 February 2024

2024

Inside This Issue

Thursday
February 8, 2024, 11AM

HODGEPODGE

Presented by

AI demo from Ron Brown
A demo of the utility "everything" by Hewie Poplock
A short demo by Chris Guld (Geeks on tour) on digital photos or useful smartphone ideas.

Tech for Senior
&
GEEKS ON TOUR

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

All Meetings will be Virtual and Zoom

LCCC Community Learning Center
201 W Erie Ave, Lorain, OH 44052

Please Email: info@lccug.com
if you have any questions or concerns!

A Word From Our President

Our January meeting, focused on 5G internet options, facilitated a valuable exchange of ideas and discussions! Micky provided an insightful overview and shared his experiences, which you can access through his PowerPoint presentation and a recording of the meeting available here: https://lccug.com/links/

For our upcoming February 13 online gathering, we are thrilled to present a diverse range of recorded clips. These clips will introduce us to new technologies, apps, and software features, sparking engaging questions, answers, and discussions among our members.

Looking ahead to our March 14 meeting, we eagerly anticipate our annual visit from Glenn Pubal. Glenn traditionally updates us on the latest trends in the technology world, and he hints at a discussion on the growing prominence of Artificial Intelligence (AI). This promises to be an enlightening session.

During our December holiday meeting, our dedicated members once again re-elected our officers, who have been steering the ship for several years. While we are grateful for their continued commitment, we also extend an invitation for new individuals to join and contribute to the club's leadership.

Allow me to express my gratitude to our tireless officers:

- Pam Rihel, our Newsletter editor for over a decade, consistently delivers a visually appealing and content-rich newsletter. Special thanks to Sandee, Don, and Micky for their contributions, but the lion's share is thanks to Pam. Much appreciated!

- Richard Barnett, our webmaster for just as long, diligently maintains our website, manages group mailings, and supports advertising efforts. We acknowledge his invaluable contribution to our online presence.

- Don Hall, our dedicated Secretary, ensures meticulous meeting minutes and timely submissions, a role we can consistently rely on year after year.

- Neil Higgins, despite residing in Pennsylvania, continues to serve as our education representative. Neil actively participates in planning meetings and keeps our Facebook page current. Thank you, Neil!

-Micky, our longstanding Treasurer, adeptly manages finances and membership records, ensuring the essential functions of our club operate seamlessly.

Reflecting on the history of our group, my former boss at the Lorain Public Library recently expressed surprise at our continued regular meetings. Having started the group in 1989, she sent us off to continue supporting each

(Continued on page 3)

LCCUG Officers For 2023

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
February 8, 2024, 11AM

HODGEPODGE

Presented by

AI demo from Ron Brown
A demo of the utility "everything" by Hewie Poplock
maybe a short demo by Chris Guld (Geeks on tour) on digital photos oor useful smartphone ideas..

LCCUG Officers are thrilled to present a diverse range of recorded clips.

These clips will introduce us to new technologies, apps, and software features, sparking engaging questions, answers, and discussions among our members.

We are looking forward to seeing you either in-person or on Zoom. Invite a family member or friend to join us.

(Continued from page 2) President column

other, and we extend our appreciation for her well wishes.

Over the group's lifetime, we've had several presidents, and during my tenure with LCCUG, I've had the pleasure of getting to know numerous fantastic individuals. The membership, which has ranged from over 300 to our current several dozen, has made this journey a remarkable experience. The subjects we now discuss and explore were unimaginable at the group's inception, showcasing the dynamic evolution of our shared interests and knowledge.

Sandra Ruth

LCCUG President

Woohoo!

Membership Dues

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.

LCCUG
Director of Membership,
membership@lccug.com.

Executive Board Meeting Minutes

JANUARY 2, 2024

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

The board discussed the December meeting at Golden Corral which resulted in Neil moving, Micky seconding the club send Second Harvest a total of $200 ($85 from the 50/50 raffle and $115 from the club). Motion passed.

Programs were discussed with Micky agreeing to talk on 5G costs and services from 3 suppliers.
Sandee will check when Glenn Pubal is available.

Pam will add a section in the Newsletter listing the day and time for our meeting thru April.

Don moved, Neil seconded the meeting be ad-

General Meeting Minutes

JANUARY 9, 2024

President Sandee Ruth called the meeting to order. A motion to accept the minutes as shown in the January issue of the ***INTERFACE*** was made by Ron Dix, seconded by Pam Rihel. Motion passed by voice vote.

Sandee mentioned the Newsletter was out and again informed members the meetings will be held on the second Thursday of the month at 11AM thru April.

Micky presented a program on "5G INTERNET SERVICES". He listed the three providers - AT&T @ $56, T Mobile @ $50 an Verizon @ $50. He explained what you could expect on upload and download speeds from each along with many technical differences.

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 only, using Zoom

https://zoom.us/j/6681479672?pwd=amh0NmtmalZWa0lmRWVBWEwySkxmZz09&omn=92912561207

Lorain County Chapter is inviting you to a scheduled Zoom meeting.

Meetings are free and the program begins at 7:00 PM.

John Kolb
secretary@loraincoogs.org

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.

Newsletter Editor: Pam Rihel using Microsoft Publisher, 2019

This Month's contributors: Micky Knickman, Sandra Ruth, Pam Rihel, Don Hall, Neil Higgins, Michael John Neill, Phil Sorrentino, Kurt Jefferson, Scambusters, Ask Leo, APCUG, Google mages, Microsoft Office art online, AARP
Newsletter is now
Online at:
lccug.com/newsletters or **lccug.com**

Lorain County Computer Users Group

2024 Calendar of Events

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

Using Zoom & In Person

Meeting & program starts at 11:00 am

2nd Thursday of each month until May. Changes are announced on the webpage and the newsletter.

All meetings are open to the public

If you have anything you would like to know about, PLEASE let up know. We would really like your input.

January 11, Thursday Wireless 5G Internet services

February 8, Thursday HodgePodge

March 14, Thursday

April 11, Thursday

May 14, Tuesday

June 11, Tuesday

July 9, Tuesday

Genealogy Tip of the Day

Widow Survived?

michaeljohnneill, 03 Feb 10:04 PM

If your ancestor's widow survived him, ask yourself the following questions:

- Could she have applied for a widow's pension based on his military service?
- Could she have applied for a military land warrant based on his military service?
- If her husband owned real property, how was it disposed of after his death?
- Did the wife get a life estate in any of her husband's property?
- Did the wife get married after her husband died?
- Did the wife move after her husband's death to live with a child a distance away?...

Every Date, Every Place, Every Witness

michaeljohnneill, 02 Feb 01:04 PM

I've reviewing a Mexican War pension application for a widow whose veteran husband was never divorced or widowed from his first wife. The claims made in the pension are confusing and not always consistent with other records. It's claimed that the first wife died in the 1850s, but she's living with her children for at least twenty years after that. Because the situation is confusing to begin with and because some of the statements are inconsistent, I've decided to make an chart with every date or event given in the pension application, including columns for:

- Date
- Place
- Event
- Witness
- Comments/Miscellaneous
- Document/Source

This way I have extracted key items from the application and can sort them in a variety of ways.

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 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:Thursday– February 8, 2024
Time: 12PM –Please show up by 12:00
Instructor: Micky Knickman
Place: LCCC @ 201 W. Erie Ave., Lorain, OH

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

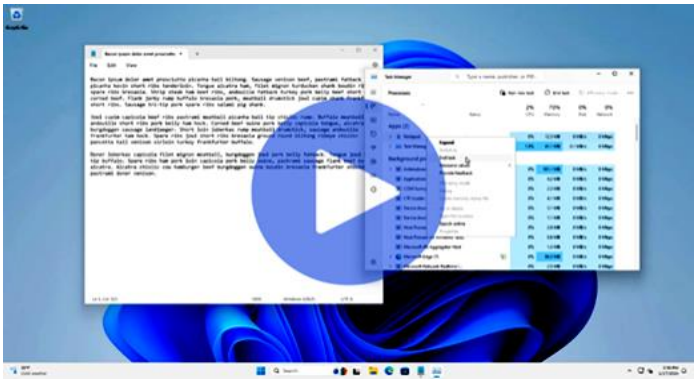
Date:Thursday - February 8, 2024
Time: 12PM –Please show up by 12:00
Instructor: Sandee Ruth
Place: LCCC @ 201 W. Erie Ave., Lorain, OH
Learn how use you electronic devices.

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.

Member of Association of Personal Computer Users Groups

Tip of the Day: Kill an App Using Task Manager

Applies to Windows: 10, 8, 7, Vista, XP



(Animation: askleo.com)

There are several "right" ways to close or terminate an application (or app) in Windows.

Type ALT+F4.

Close all the windows of the application.
Right-click on the app's icon in the taskbar and click Close.

Click on the "x" in the application's upper-right corner.

Click on the File menu, if it has one, and then on Exit.

Heck, there are probably ways I've overlooked.

But what happens when the application has hung or crashed in such a way that none of the "right" ways work?

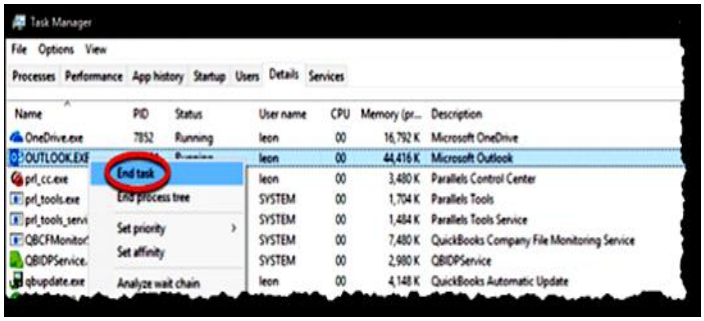
Task Manager to the rescue.

Run Task Manager. Click on "More details" in the lower left of the Task Manager window if it appears.

Task Manager's displays the "Processes" tab by default, which lists all the apps, applications, and background processes running on your machine. Right-click on the misbehaving application and click on End Task.

That should do the trick.

Another option you can use — perhaps if it's not clear which application you want on the Processes tab — is to click on the Details tab. On this tab, the processes running on your computer are displayed in a little more technical way.



End Task in Details
Closing a program in Task Manager's Details tab. (Screenshot: askleo.com)

Once again, right-click on the misbehaving process and click on End task to kill it.

Caveat #1
Using Task Manager to kill a process is a last resort. Any work you haven't saved in that program will likely be lost, and it's possible that when you run the application again, it'll be confused since it didn't shut down properly.

But sometimes you have no other choice.

Caveat #2
Use extreme caution when attempting to kill a process that is part of the system itself (i.e. a Windows application) or of which you're uncertain. If you kill a key process, you can cause your system to misbehave, crash, or shut down immediately.

Visit Tip of the Day: Kill an App Using Task Manager for moderated comments, related links, and updates.

ScamBusters.org

REMOTE HEALTH MONITORING IS THE LATEST TARGET FOR MEDICARE FRAUD

SCAMBUSTERS #1,103

Medicare fraudsters are constantly finding new ways to trick both program members as well as the organization itself.

The latest ruse is to pretend to be providing necessary equipment and services to monitor chronically ill patients in their homes.

But that's just the tip of the iceberg, and your health and finances could be put at risk if you fall victim, as we report in this week's issue.
Let's get started…

15 WAYS TO BEAT MEDICARE FRAUDSTERS

A new type of scam has been heaped onto the pile of Medicare frauds that are costing the US health insurance program - and its 60 million members - billions of dollars every year.

Fraudsters are taking advantage of advances in technology to exploit what is known as remote patient monitoring (RPM) - using internet-linked devices to check on patients, such as those with heart pacemakers, glucose monitors, or blood pressure cuffs.

In a recent alert, the US Department of Health and Human Services' Office of Inspector General (HHS-OIG) warned: "Unscrupulous companies are signing up Medicare enrollees for this service, regardless of medical necessity."

Scammers use cold calling, internet, and even TV ads to target victims with unsolicited offers of RPM equipment and services, which they may never receive, they don't need, or which haven't been authorized.

"Billing then occurs for set-up, patient teaching, and monthly monitoring of data. Most often, the monthly monitoring never happens, but the enrollee is billed monthly anyway," the alert says.

Another scheme to have surfaced recently involves allegedly fraudulent Medicare Advantage program activity. Medicare Advantage programs are those that mirror traditional Medicare, packaged with other additional benefits.

One suspected offender, accused of submitting false information about chronic ailments, recently agreed to return $53 million in alleged overpayments to the Centers for Medicare and Medicaid Services (CMS).

These incidents are merely the latest in a host of frauds that swallow up an estimated 10% of the entire Medicare annual budget.

And it's not just CMS and US taxpayers who are losing out. Individual Medicare enrollees face a number of risks that can affect them directly, both financially and health-wise.

TODAY'S MOST COMMON MEDICARE SCAMS

In addition to the schemes highlighted above, today's most common Medicare and Medicaid scams recently identified by AARP, the organization for retired people, include:

A new round of Covid 19 fraud, mainly involving test kits but leading to theft of identity information.

Bills for unneeded diabetes supplies and equipment.

Poor quality medical equipment, notably knee and back braces.

Fake genetic testing at events like health fairs. Medicare doesn't normally cover these tests, so victims may end up paying out of pocket as well as having to reveal their Medicare number.

Hospice fraud, when individuals are unknowing-

(Continued on page 9)

(Continued from page 8) Medicare Fraud...
ly enrolled in hospice programs. Sometimes, they're tricked into thinking they're signing up for another type of program or benefit.

Medicaid recertification. Victims are told they need to pay to avoid losing their Medicaid coverage.

New Medicare cards. The flimsy nature of Medicare cards is being exploited by scammers offering a plastic card with a microchip. Of course, you have to give them your number first, and pay. (We focused on card scams in issue #777: Crooks Ramping Up New Medicare Card Scam.)

Dubious telemedicine services. Cold-calling scammers have been known to charge victims or Medicare for the call itself, claiming it was a consultation.

More Scam Reports: Top 3 Targets for Reloading Scams
(Source: AARP)

Many of these scams lead to identity theft as well as billing Medicare for services, prescriptions, or equipment that have never been provided. Sometimes, the same items are billed twice. Or victims are offered coverage that's not approved by Medicare.

Other known scams that defraud Medicare include billing for unnecessary or non-provided ambulance services and fake medical facilities that submit large volumes of claims.

PROTECTING YOURSELF AGAINST MEDICARE SCAMS

Medicare beneficiaries owe a duty not only to themselves but also to the American taxpayer to do all they can to spot and stop Medicare scams.

Here are 15 key actions you can take to protect yourself:

1. Carefully review all summaries and explanations of benefits (EOBs) and report discrepancies both to the provider and, if not satisfied, to CMS.
2. Safeguard your card and your membership number. Only give details to your known health service providers.
3. Hang up on unsolicited sales calls, whether for equipment or program membership.
4. Be equally cautious of texts and emails with links seeming to relate to your Medicare coverage. Don't click on those links.
5. Hang up on calls claiming to be from Medicare unless it's a returned call or you filed a fraud report. Those are generally the only reasons they'll phone you.
6. Never accept offers of free medical equipment or other incentives to sign up for devices or services.
7. Don't accept telemedicine services or house calls from unknown providers.
8. Don't pay upfront for services beyond deductibles and/or copays.
9. Beware of aggressive sales tactics that urge you to act quickly or take tests that may be unnecessary. Always talk to your health care provider first.
10. Use in-network providers if you can. If you have to go outside the network, carefully check out the credentials of providers.
11. Keep copies of all Medicare notices and other documentation.
12. Monitor your credit report for evidence of identity theft.
13. Trust your instincts. If something doesn't feel right, it could be a scam.
14. Be wise online. Check privacy policies carefully before providing information about yourself to organizations offering services, equipment or supplies.
15. Report suspected fraud on the Medicare hotline (1-800-MEDICARE) or via the US Department of Health.

Among other risks, individuals victimized by Medicare scams can suffer serious health dangers, either because they don't get the treatment they need or because of the stress associated with identity theft, which could even lead to loss of coverage.

There's one more action to consider in the fight

(Continued on page 10)

(Continued from page 9) Medicare Fraud

against Medicare fraud - volunteering to join the Senior Medicare Patrol or your State Health Insurance Assistance Program (SHIP).

THIS WEEK'S ALERTS

Scary clones: We all know about fake distress calls from supposed friends and relatives asking for money. But now scammers have stepped up their game by using artificial intelligence to clone voices and videos to trick their victims, according to the British Daily Mail newspaper. Yes, you can no longer believe your eyes, even when it comes to people you already know.

Live Package Tracking Comes to Gmail

By Kurt Jefferson, Editor, Central Kentucky Computer Society
https://ckcs.org/
lextown2 ** gmail.com

Gmail users anxiously awaiting a package's delivery may smile when they hear about this late-2022 feature.

Mashable reports, "Gmail will initially ask users in a pop-up at the top of the inbox if they wish to opt-in to receive tracking updates before enabling package monitoring. Users can choose whether to click "Allow" or "Immediately now" based on their preferences."

If users opt in, a small green label with the estimated package delivery day will automatically appear under the sender's name and subject line in the Gmail inbox. Mashable reports that a small truck icon and the order's progress status are shown after the estimated delivery date.

Most major freight delivery companies are expected to provide the new feature. However, according to Tom's Guide, the user must have an order confirmation with a tracking number for Google to offer live tracking in its Gmail service.

Of course, you must be using the Gmail app for this to work. This feature won't be available if you're viewing your Gmail account messages using a different email app (such as Apple Mail, Outlook, Thunderbird, Postbox, or Canary Mail).

Modern-Day Bonnie and Clydes Are Trying To Steal Your Identity and Your Money

By Kurt Jefferson, Editor, Central Kentucky Computer Society
https://ckcs.org/
lextown2 ** gmail.com

I've written in the past that if Bonnie and Clyde were alive today, they definitely wouldn't waste time robbing banks. If you're not familiar with the couple, they were ruthless gangsters who robbed banks, stores, and other places of business and killed lawmen, shopkeepers, and owners of cars they were stealing in at least four states.

They were, perhaps, best known for robbing more than a dozen banks– some of the same banks twice–over a four-year period, primarily in Missouri, Oklahoma, New Mexico, and Texas. Back in their heyday, they also targeted stores in small towns and funeral homes located in rural areas. Make no mistake about it. They were dangerous lawbreakers. That was

(Continued on page 11)

(Continued from page 10) Modern Day Bonnie & Clydes...

how it was in the Depression-era 1930s.

- If you don't already have a warranty and you get a "reminder," it's a scam.
- If there's no contract, don't buy.
- If there's a contract, read every line of this and any other terms and conditions documents. Ask questions about anything you're not clear about. You need to know exactly what's covered. And keep records of all communications.
- Establish exactly what extra fees and deductions you'll have to pay.
- Understand the call-out times and claims process and compare with others. It should be quick and easy.
- Check the source of any reminder or notification. If it seems to come from an organization you already do business with, contact them directly. If it comes out of the blue, beware.
- Get recommendations from friends, family, neighbors, and realtors.
- Be wary about providing confidential personal information until you're at the right stage of the research and decision process
- Check if you might be duplicating existing coverage such as manufacturers and retailer warranties, especially on newer appliances. Unscrupulous warranty providers will use this as a get-out.
- Know the scope of coverage - just wear and tear, manufacturing defects, or accidental damage, for example.
- Try to speak to a human and know how and when you can contact them - 24/7 for instance. If everything seems computer driven, beware.
- Find out what the usual call-out time is. The best firms send a tech out within 48 hours.
- If you just bought a home and it doesn't come with a warranty, have systems checked as part of a home inspection so you'll have an idea of likely risks.

Fast forward to today. Modern Bonnie and Clydes don't rob banks. It's too much work. Instead, they steal personal data from computers, phones, and tablets. They're called hackers. One of their main goals in this life is to steal, rob, and gain access to your hard-earned dollars. Their goal is to grab your money and run; your goal is to keep that from happening. So, whether you're tech-savvy or not, how in the world are you supposed to keep this from happening? There are simple steps you can take.

1. When someone calls you on the phone from an unknown number, DO NOT answer the phone; wait for a voicemail message. Microsoft, Apple, etc., will not call you. These thugs want to get their hands inside your computer or other device to steal your passwords or personal information. If you answer the phone, your number may be sold for more money.

2. Don't open emails from unknown sources. Don't open attachments from unknown senders. Don't respond to schemes alerting you that a friend has been hurt in London, Paris, Sydney, or some other location. Could you send money to help them? Your friend is in the hospital and needs your financial help. Their wallet's been stolen. Their purse has been snatched. And I'm the king of Spain.

Please don't fall for it. Don't click on links in an email from someone you don't usually hear from, urging you to view these great photos. There are no photos. Once you click on the link, malware infects your Windows PC and sends emails to everyone in your address book with the same message, urging them to click on a link to view photos. Phishing is the most successful cybercrime in America.

There were nearly 324,000 victims last year alone. (Phishing refers to an email that appears to be from a legitimate company or organization. There's often a threat – your account will be closed, or the sheriff will come to your house unless you respond. It's all bogus. But plenty of Americans fall for it.) Ever gotten an email that you owe $500 for Norton 360

(Continued on page 12)

(Continued from page 11) *Modern Day Bonnie & Clydes...*

(virus and malware protection software) that you never even purchased? You'd be surprised by how many folks respond to the email and even pay for the software they don't own. The thugs sending the email are not from Norton. Most junk email trying to get into your wallet originates in Russia, Germany, the U.S., and China.

3. Yes, it's a pain. But what tech folks call two-factor authentication can save your bacon. Turn it on. You'll be blocked if you decide to change your Gmail password, Facebook log-in, iCloud username or password, or some other account, you'll be blocked. You must enter a code you receive in a text message, an email, or even using the Gmail app on your smartphone to get permission to change your password. Yes, as I said, it's a pain. But it's preventing crooks from gaining access to your account. So instead of just changing your passwords, you must first receive a code and enter it into a website or Gmail app. That proves you are who you say you are.

4. Run antivirus software.

For Windows PCs:
Safety Detectives: The Best Windows Antivirus
https://www.safetydetectives.com/

PC Mag: The Best Antivirus Software for 2023
https://www.pcmag.com/picks/the-best-antivirus-protection

For Macs:
Safety Detectives: Ten Best Antiviruses for Mac in 2023
https://www.safetydetectives.com/best-antivirus/mac/

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

Macworld: Best Mac Antivirus Software 2023
https://www.macworld.com/article/668850/best-mac-antivirus-software.html

For Linux:
Safety Detectives: Five Best Antiviruses for Linux in 2023
https://www.safetydetectives.com/best-antivirus/linux/

Ubuntu Pit: Top 15 Best Linux Antivirus Programs in 2023
https://www.ubuntupit.com/best-linux-antivirus-top-reviewed-compared/

5. Don't go on a fishing expedition on the Web. The World Wide Web is remarkable. It's the best library in the world. There are an estimated 1.6 to 1.9 BILLION websites currently accessible. Less than 400 million are currently active. More than 51% of all people in the world are online. Asia accounts for half the Internet traffic worldwide. Talk about diversity. Websites appear in more than 200 languages. But watch your step. Don't put your foot into horse dung. Make sure the website you visit starts with https. No, this is not always possible.

Some websites refuse to use the "https:" system. The "s" stands for secure. You're accessing a secure website. Don't randomly visit online gambling websites, sites with outdated addresses, websites with shortened addresses, sites ending in .onion, torrent websites (file sharing sites), porn sites and others.

Google constantly scans websites, looking for legitimate websites that have been compromised, unsafe sites, or other questionable pages. If you wonder whether a website is safe or not, visit the web address below and paste your website into Google's Safe Browsing website:
https://transparencyreport.google.com/safe-browsing/search

It will tell you whether it's safe to proceed or not.

(Continued on page 13)

(Continued from page 12) **Modern Day Bonnie & Clydes...**

5. Use a well-regarded virtual private network (VPN).

This tool sends your Internet signal through a tunnel so that hackers and other thieves cannot access the web pages you visit, your email, your passwords, or additional private information. Do your homework. Find a good VPN you can afford.

Steer away from free VPNs because many sell your data online, bombard you with ads, and some even use your computer's processing power.

For Windows PCs:
Privacy Savvy: Five Best VPNs for Privacy
https://privacysavvy.com/vpn/best/windows/

VPN Reports: Best of the Best VPNs
https://www.vpnreports.com/best-vpn/windows/

For Macs:
VPN Reports: Best VPNs for Mac in 2023
https://www.vpnreports.com/best-vpn/mac/

Safety Detectives: Ten Best VPNs For Mac
https://www.safetydetectives.com/best-vpns/mac/

For Linux PCs:
Safety Detectives: Five Best Linux VPNs
https://www.safetydetectives.com/blog/best-linux-vpns/

Pro Privacy: Ten Best VPNs for Linux
https://proprivacy.com/vpn/comparison/best-linux-vpn

6. Use a password manager to track your passwords and log in to many websites requiring a username and password automatically. Experts say this is smarter than allowing your browser to remember your passwords. Unfortunately, web browsers are not really safe to keep that sort of information. As Tom's Guide writes, "That's because desktop web browsers, despite their best efforts, tend to do a lousy job of safeguarding your passwords, credit card numbers, and personal details, such as your name and address. As a result, web browsers are fairly easy to break into, and lots of malware, browser extensions, and even honest software can extract sensitive information from them."

Here are websites where you can read about the best password managers and pick one that works for you:

PC Mag: https://www.pcmag.com/picks/the-best-password-managers

Tom's Guide: https://www.tomsguide.com/us/best-password-managers,review-3785.html

How To Geek: https://www.howtogeek.com/780233/best-password-manager/

Missing a Drive Letter? – This might help

By Phil Sorrentino, Secretary and APCUG Rep
Sun City Center Computer Club, FL
https://www.scccomputerclub.org/
philsorr ** yahoo.com

When you plug a portable or external drive into a computer USB port, you expect the drive to be immediately available.

You may hear a few familiar sounds at first, but eventually, you expect to see an indication that the drive is usable. First, you should see the new drive in File Explorer with a new drive letter. The drive letter will typically be the next available letter in the alphabet. (Drives installed on your system start at the beginning of the alphabet with the exceptions that A: and B: are reserved for floppy drives (I wonder how many of us ever had a B: drive), and C: is reserved for the main drive, where the OS is located. So added drives can start at D: unless you have other mechanical, electrical, or optical drives.)

(Continued on page 14)

(Continued from page 13) Missing a Drive Letter? – This might help

So, in a typical laptop with a C: and D: drive, it will be assigned the E: drive letter when you add a USB drive.

Just as an aside, if you have a network of local computers, drive letters may also be assigned by the "map a network drive" feature. These drives typically start from the end of the alphabet, so the first will be Z, followed by Y, and so on. To map a network drive, open File Explorer and click "This PC." Click on the Computer tab, click "Map network drive, " browse, and select the network drive from the list. (To be on the list, the drive must have been shared on the computer it is attached to.)

While we're talking about temporarily added drives, when you are finished with the drive, it is always a good idea to eject the drive in the prescribed way by first clicking the "Safely Remove Hardware and Eject Media" icon. It should be in the notification area on the right side of the taskbar. If you don't see it, you may have a taskbar setting chosen to not display the icon in the notification area, or there may be too many notifications chosen. If you don't see it and you see an up-pointing caret (^), click the caret, and the "Safely Remove Hardware and Eject Media" icon should show up.

Safely Remove the Hardware and Eject Media Icon.

Yesterday, I had a house full of friends and relatives I had invited over to see some movies that I created from some family and friend activities over the past few years. Knowing this, I connected the portable drive with the movies to my computer in the living room, where everyone could comfortably enjoy the pictures and movies on the connected big-screen TV. Unfortunately, the drive never showed up, though I did hear the familiar sounds. And I could tell the computer knew a drive was there because the "Safely Remove Hardware and Eject Media" icon was in the notification area, but no new drive appeared in File Explorer.

I couldn't show any of the movies on the new drive. So, what's up? I was anxious to show the movies on the new drive to a large group of friends and relatives, so I postponed trying to solve the immediate problem. Fortunately, the living room computer is on a network, so I removed the new drive from the living room computer, the safe way, and brought it to another computer on the network. When I plugged it into the kitchen computer, the installation went as expected, and the new drive showed up as the E: drive in File Explorer. Now all I had to do was share the E: drive on the kitchen computer and then go to the living room computer and map the shared kitchen E: drive. All this went as expected, and we could watch all of the movies and pictures from the new E: drive, which was on the kitchen computer and the living room computer/TV; the party was saved. Everyone enjoyed the movies, but at the end of the day, I was still stuck with the problem of the missing drive letter.

Disk Management

So, before I head to the Computer Lab, I always take a little time to try to solve the problem, or at least try to narrow the problem down using Google to look for a solution. I tried "no drive letter for USB device, " pointing me to a few possibilities. One Google hint showed me that related areas could be found with a right-click of the start button. "Disk Management" is one of those areas. (Be very careful if you go into this area, you can easily turn your computer into a brick with a few short commands, and

(Continued on page 15)

(Continued from page 14) Missing a Drive Letter? – This might help

then you'll have no choice but to go and see "Bob.") When you click "Disk Management," you see the disk drives on your computer and their assigned letters.

After I plugged in the USB drive and got into "Disk Management" on the living room computer, I clicked on the newly added USB disk to select it. I noted that the USB drive was "Disk 1" and a "Healthy Primary Partition," all good indications, but no drive letter was assigned. So the next step was to click on the "Action" menu and then click "All Tasks," where "Change Drive Letter and Path" was found. Again, no drive letter was assigned, so I clicked "Add" to assign an unused letter, in my case, E. After I assigned E: to the USB drive, I could see the drive and its contents in File Explorer, as expected. When I removed and reconnected the drive, it connected as expected and had the E: drive letter.

Epilog: Unfortunately, when I used a different portable drive, it reacted the same way; it showed up without a drive letter. So, now I know how to get around the problem, but I should think that any portable USB drive connected should show up with the next unused letter. So, I may still have something amiss.

Should I bother with an External Hard Drive?

The Golden Rule of backups states that data in only one place isn't backed up. Multiple backups prevent data loss even if one fails. External drives and online services can fail, but having additional copies means you won't lose anything. The Rule of Three says three copies on two different media types with one stored offsite maximizes practical protection.

The Golden Rule
The golden rule of backups is this:
If it's in only one place, it's not backed up.

When you have data backed up (meaning you have made multiple copies on any media: cloud, external drive, etc.) then data loss will only happen if all copies are destroyed at the same time.

Failure

You're quite correct in that things can go wrong with external drives. They are hard drives, after all. They can and probably will fail eventually. But if you still have your original files, you just replace the external hard drive and resume backing up.

Online services can fail too. Your account could get hacked; your data could be destroyed. The service could suffer a failure of some sort or even go out of business. But again, you still have your originals; you move to a different backup service and resume backing up.

When it comes to backups, it's a numbers game, and more is always better. However, if I could get everyone to back up to an external hard drive, 99% of the disasters that I hear about would stop happening.

The rule of three
So what about that 1% of disasters that wouldn't be prevented with an external drive? Well, one rule of thumb is to have:

Three copies
On (at least) two different media types
With one stored elsewhere
That reduces the probability of disaster even more.

The Rule of Three

The Rule of Three **How to Back Up Windows**
Using free and included tools, here's how to back up Windows and all your data in eight easy steps.

For example, if you add an online backup service for your data in addition to backing up your entire machine to an external hard drive, then your data is protected from things that could take out both the computer and the external hard drive, like fire or theft.

I personally would not use an online backup as a replacement for backing up to a hard drive. But I do see it (and use it myself) as an additional part of an overall backup strategy to reduce the possibility of disastrous data loss further.

Do this
Above all, back up.
I recommend using an external drive, but regardless of the technique you choose, it's critical that your important data be backed up and protected from disaster.

More protection: Subscribe to Confident Computing! Less frustration and more confidence, solutions, answers, and tips in your inbox every week.