Interface

Lorain County Computer Users Group
LCCUG.com (or) info@LCCUG.com
Volume 36 Number 08 August 2025

scams

2025

Inside This Issue

Tuesday
August 12, 2025
10:00 AM

Living on a Cruise Ship
&
More Topics that are Interesting.

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

This meeting will be held in person and on Zoom
Tuesday, August 12, 2025 at 10:00 am.
Join us in person at:

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

More and more I am fascinated by the swift changes that AI is creating! A recent interview I watched mentioned that a project that his company designed and developed a few years ago took 4 years to complete. This past year they worked with AI to have it designed again "from scratch" and it took only 1 week to have AI write the program for this project.

Everything is happening exponentially!

Over the next five years, we can expect daily life to change at a pace that will feel faster than ever before, largely driven by the rapid growth of artificial intelligence (AI). AI is already showing up in ways many people use without even thinking about it—like smart assistants, personalized recommendations, and advanced language tools—but these are just the beginning. In the near future, AI will become more deeply woven into how we work, learn, and communicate. Tasks that once required hours of human effort will be completed in seconds by machines, and new tools will make it possible for anyone to create videos, designs, or written content with little more than a simple request. This will make many things easier, but it will also challenge us to adapt quickly to new ways of doing things.

The impact on jobs will be one of the most visible changes. Some roles—especially those involving repetitive tasks—may shrink or disappear entirely, while new careers will emerge in fields we can barely imagine today. People will need to develop new skills, often more than once in their lifetime, to keep up with shifting technology. Remote work and automation will likely continue to grow, reshaping where and how people earn a living. In our personal lives, AI will increasingly assist with decision-making, healthcare, transportation, and even social connections, making life more convenient but also raising important questions about privacy, ethics, and what it means to be "human" in an age of smart machines. The key will be staying flexible, learning continuously, and remembering that technology is a tool—how we use it will determine whether the next five years are exciting, overwhelming, or both.

Sandra Ruth

LCCUG President

LCCUG Officers For 2025

President	Sandee Ruth president@lccug.com
Secretary	Don Hall secretary@lccug.com
Treasurer	Micky Knickman treasurer@lccug.com
Newsletter Editor	Pam Rihel newsletter@lccug.com
Director of Membership	Neil Higgins education@lccug.com
Statutory Agent	Sandra Ruth statutory_agent@lccug.com

LCCUG

Member of Association of Personal Computer Users Groups

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

Tuesday
August 12, 2025

Living on a Cruise Ship
&
More Topics that are Interesting.

featuring

Geeks on Tour

The LCCUG officers will be on hand to field any questions concerning the topics presented or other questions from the audience, so join us for an informative presentation.

Click on link below to attend via Zoom:
https://us02web.zoom.us/j/89987212300?pwd=Y0QxRE00UXVMMUh6T0d4dm9nWmxSUT09

Genealogy Tip of the day

Michael John Neill , 2025
Rootdig.com mjnrootdig@gmail.com

August 8, 2025

There's a never a guarantee that you'll get an answer to every genealogy question you have. Sometimes that's just the way life is. You may also get an incomplete answer or one that raises more unanswered questions. There are things you can do to maximize the chance you do find that answer.

Constantly learn about new sources and finding aids for those sources. Make certain you are familiar with records for the area at all geographic levels. Do not just focus on online or easy-to-access sources. Consider the fact that some of your information or assumptions about a person are wrong. Make certain you understand the local geography, history, and culture. Double and triple check every detail. Consider asking someone with specific knowledge in the area and time period for help.

That can be a tall order, but performing all those tasks can reduce the chance the answer eludes.

However, at the end of the pedigree chart there are no guarantees and only blanks to be filled.

Executive Board Meeting Minutes

JULY 1, 2025

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

The board again discussed what they felt the members wanted in programs. The program for next week will be more on AI.

Discussion was held on possible places for a meal get together since Golden Corral has closed.

AARP Fraud Watch Network

Did you know that AARP makes available free articles on preventing scams & fraud? Visit this site for more information:

https://www.aarp.org/membership/benefits/finance/fraud-watch-network/

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, Kurt Jefferson, Lynda Burske, Jim Cerny, Adobe Stock, Scambusters, Ask Leo, APCUG, Google Images, Microsoft Office art online, AARP

Newsletter is now
Online at:
lccug.com/newsletters or **lccug.com**

General Meeting Minutes

JULY 8, 2025

President Sandee Ruth called the hybrid meeting to order. A motion to accept the minutes as shown in the July issue of the ***INTERFACE*** was made by Micky and seconded by Elaine D'Andrea. Motion passed by voice vote.

Sandee and Micky continued showing the various programs they found interesting on the Internet regarding AI. Micky explained how you can see them all on our web page. They started with "What Are Passkeys?" followed by "How To Use AI Safely".

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.

LCCUG
Director of Membership,
membership@lccug.com.

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

Burned By Another Security Breach?

By Kurt Jefferson, Editor, Central Kentucky Computer Society
https://newsite.ckcs.org/
lextown77@mymetronet.net

If you're reading this, there's a fair chance your personal data has been compromised. *Stolen.* As Malwarebytes Labs reports, "Earlier this week, the data of over 70 million people was posted for sale on an online cybercrime forum. The person selling the data claims it stems from a 2021 breach at AT&T."

If you think you might be a victim, you can type the email address connected to your AT&T account here on the Malwarebytes website. (Malwarebytes is a well-known company that produces anti-virus software and similar products.)

This security breach is especially troubling because, as Bleeping Computer notes, "AT&T says a massive trove of data impacting 71 million people did not originate from its systems after a hacker leaked it on a cybercrime forum and claimed it was stolen in a 2021 breach of the company." The stolen personal data is from an alleged 2021 AT&T breach that hackers calling themselves ShinyHunters attempted to sell on the dark web.

Search tools like Google, Yahoo!, or DuckDuckGo cannot reach the dark web. It's comprised of websites where everything from drugs to guns to personal information is sold for the right price. Whether or not the stolen data came from AT&T, the wireless giant says it has started notifying millions of customers about the data thefts.

AT&T says it has already reset the passwords of current customers and will be contacting others whose passwords, Social Security numbers, and possibly email and street addresses were compromised.

Prosecutors in New York are opening an investigation into the breach.

Numerous tech websites are urging AT&T's current and former customers to freeze their credit accounts at the big three credit agencies–TransUnion, Experian, and Equifax. In addition, sign up for two-factor notification on their AT&T accounts and change your AT&T password if it hasn't already been changed. Also, monitor your credit reports.

This isn't the first time the phone company has had problems. In a major AT&T outage in March, the company apologized for the disruption and offered a $5 credit to customers.

ScamBusters.org

Your Favorite Streaming Service is Being Hijacked

Warning: Look-Alike Streaming Sites are Stealing Logins and More: Scambusters #1,182

Scammers are using your favorite streaming platform to steal your money. Read on for more details!

Your Favorite Streaming Service is Being Hijacked

As streaming services like Netflix, Hulu, Disney+, and Spotify become more popular, scammers are finding ways to exploit them. Streaming scams are becoming more common. These scams trick users with fake login pages, phishing emails, and false subscription offers. They can lead to stolen personal information, unauthorized charges, or malware infections. To protect yourself and your digital life, it's important to know how these scams work.

Common Types of Streaming Scams

(Continued on page 6)

(Continued from page 5) Your Favorite Streaming Service….

Streaming scammers trick people by pretending to be real services. They use convincing methods to deceive their victims.

Knowing where these criminals work can help you spot and avoid their traps.

- **Social Media Platforms –** Scammers make fake profiles and pages on popular social media platforms to advertise streaming deals that seem too good to be true. They often use stolen logos and branding to appear real, targeting users who engage with entertainment content.
- **Email Campaigns –** Scammers buy email lists or use automated tools to send mass emails promoting fake streaming offers. These emails often avoid spam filters by using senders that look legitimate and have professional formatting.
- **Search Engine Results –** Scammers make fake websites that show up in search results when people look for streaming deals or account help. These sites use techniques to improve their position in search results for relevant keywords.
- **Text Message Campaigns –** Scammers send SMS messages pretending to be from streaming services. They often target phone numbers linked to existing accounts, using information from data breaches or purchased contact lists.

Impact on Legitimate Streaming Companies

These scams significantly affect legitimate streaming services and their customers.

- Streaming companies work hard to fight fraud and help consumers recognize scams. They regularly check for fake websites that use their name and team up with law enforcement to close down fraudulent activities.
- Customer trust is a major issue because scammers can pretend to be real services. This makes people cautious about online streaming offers, leading them to sign up for fewer subscriptions, even for legitimate ones.
- Streaming companies face more costs than just direct losses. They need to spend money on better security, customer support, and legal actions against scammers. These costs can increase the prices of their services and leave less money available for development.

The Streaming Service Scammer's Process

Understanding how criminals execute these schemes reveals their methodical approach to fraud.

- **Target Identification –** Scammers look for popular streaming services and current market trends to decide which platforms to imitate. They usually target services that have many users or new platforms that are becoming popular.
- **Website Creation –** Scammers create fake websites that look like real streaming services by using stolen logos, images, and content. These sites also have working payment systems to gather information from victims.
- **Marketing Campaign –** Scammers share fake offers through social media ads, emails, and search engines. They often create a sense of urgency with phrases like "limited time offers" to push people into making quick decisions.
- **Information Collection –** When victims visit these sites and share their personal and payment information, scammers often charge their credit cards immediately or sell the information to other criminals.
- **Disappearance –** After scammers collect enough information or money, they often close their fake websites. Then, they create new ones to avoid being caught and continue their scams.

A Fictional Streaming Scam Example

Sarah received an email that appeared to be from a service called "NetStream." She had never heard of this service, but it looked similar to a popular streaming platform. The email offered a premium subscription for only $2.99 per

(Continued on page 7)

month, while her current Netflix bill was $15.99.

The email looked professional, with logos and a link to sign up right away. Excited about the savings, Sarah clicked the link and found a website that seemed real, showing movie trailers and subscription options.

She entered her credit card information and personal details to create an account. A few hours later, she noticed unauthorized charges on her credit card totaling over $300.

When she tried to visit the NetStream website again, it had disappeared. Sarah realized she had been scammed. The criminals used her information to make fraudulent purchases and may have sold her data to others.

Take Action If You Become a Victim of a Streaming Scam

If you think you might fall for a streaming scam, act fast to limit any harm.

- **Contact Your Bank –** If you spot any fraudulent charges on your credit card, call your credit card company or bank immediately. Request a new card. Most banks have a fraud hotline that you can reach at any time.
- **Document Everything –** Take screenshots of the fake website, emails, and any messages from the scammers. Record all unauthorized transactions and make notes about your communication with your bank.
- **Change Passwords –** Change the passwords for all your streaming accounts and any other online services that use the same login. Make sure to use strong and unique passwords for each account.
- **Monitor Your Accounts –** Check your bank and credit card statements every month for several months after the incident. Set up alerts for your accounts to let you know if there is any unusual activity.
- **Report the Scam –** Report incidents to the right authorities. This can help prevent others from becoming victims and may help you recover your losses.

Resources for Streaming Scam Victims

Several organizations provide assistance and support for scam victims.

File a complaint at ReportFraud.ftc.gov to help law enforcement track scam patterns and potentially shut down fraudulent operations.

An FBI-operated website, Internet Crime Complaint Center (IC3) accepts online crime reports and coordinates with law enforcement agencies to investigate internet fraud.

Check out the video BBB Warns of Streaming Service Scams.

Conclusion

Always check streaming offers by visiting the official company website. Avoid clicking links in emails or looking for deals that seem too good to be true. Legitimate streaming services usually have subscription rates close to their standard prices.

Be cautious of unexpected messages about urgent account issues. Real streaming companies send account notifications through their official apps or known email addresses. Before sharing your payment information, research any unfamiliar streaming services. Look for online reviews, check if they are registered as a business, and find their customer service contact details to confirm they are real.

Keep your devices and browsers updated with the latest security patches, and use reliable antivirus software with web protection.

Streaming scams often take advantage of our desire for cheap entertainment. Staying informed can help you avoid becoming a victim. Always verify offers through official channels, be skeptical of suspicious deals, and act quickly if you suspect you've been targeted. Stay cautious to enjoy your favorite shows and movies safely.

Remember, Stay Alert and Stay Informed!

Tip of the Day: Plan for the Worst

This is a thought exercise I go through when I'm about to go on a business trip.

What would happen if I lost everything I had with me? I mean *everything*: technology, wallet, perhaps even clothing.

How would I start over while on that trip? Sure, after seeing to my physical safety, I might borrow a computer — but then what? My digital world is locked down so tight that it would be

Tip of the Day: Plan for the Worst

This is a thought exercise I go through when I'm about to go on a business trip.

What would happen if I lost everything I had with me? I mean *everything*: technology, wallet, perhaps even clothing.

How would I start over while on that trip? Sure, after seeing to my physical safety, I might borrow a computer — but then what? My digital world is locked down so tight that it would be

difficult for me to gain access without my second factor (as used for two-factor authentication), or my mobile phone (often used for the same thing), not to mention my password vault, since the vast majority of my passwords are beyond memorization.

How would I bootstrap my digital life?

By bootstrap, I mean to gain access to one key piece of information (perhaps a one-time passcode in a safe location secured by a very strong yet still memorable passphrase) that would allow me to bypass a two-factor authentication requirement and gain access to the next level (perhaps a password vault, at which point I could access my critical accounts).

To be clear, I'm *not* suggesting you weaken your security for this "just in case" scenario. For example, don't turn off two-factor; just make plans for how you might *securely* bypass it in an emergency.

Pack your bags!

By Lynda Buske
Published in Ottawa PC News (June 2023)
Ottawa PC Users' Group, Ontario, Canada (https://opcug.ca)
Editor: brigittelord@opcug.ca

As you already know, one of my interests is travel photography, and we are entering the season when many of us travel far (or near) to experience and photograph new locations. A stay at an area B&B or a friend's cottage can provide ample opportunity to enjoy a different life from your normal routine. Perhaps you have time to notice nature's beauty when the pace is slower and your schedule is not so packed. Maybe you also have the chance to view familiar things from a different perspective. Finding beauty that others walk by is a comment I often hear with respect to my photos.

I have often written about travel photography, so here are some links to past articles you may find useful.

Tips for travel photography. Review my five tips for better travel photos.

https://opcug.ca/Photography/TipsForTravelPhotography.pdf

Rainy day photos. Don't spend vacation days inside when rainy days offer enticing photographic opportunities.

https://opcug.ca/Photography/RainyDayPhotos.pdf

Shooting near water. Canadians have abundant opportunities to visit lakes and seasides, so review these tips before heading to the beach!

https://opcug.ca/Photography/ShootingNearWater.pdf

(Continued on page 9)

(Continued from page 8) Pack Your Bags

Don't miss the road shots! Don't miss photo opportunities from the passenger seat or on a bus.

https://opcug.ca/Photography/RoadShots.pdf

What to do with all those travel photos? How to organize your pics once you are home. Please note that the article refers to Shutterfly.com. As of March 2023, setting up a personalized site for sharing on Shutterfly is no longer an option. I would suggest trying a site like Flickr, where you can post 1000 free photos and provide links to friends.

https://opcug.ca/Photography/WhatToDoWithAllThoseTavelPhotos.pdf

Happy travels!

Apps You Run on Your Computer Are ".exe" files

By Jim Cerny, 1st Vice President
Sarasota Technology Users Group
https://thestug.org/
JimCerny@gmail.com

Your device (Windows or Apple computer, iPhone, iPad, or whatever) runs "apps," which is a term short for "applications". An app is a program or a set of instructions for the computer to execute or "run." They are why you have your device. Although apps can run on any device, to keep it simple, let's look at how an "app" runs on a Windows computer (almost the same on any device).

When you purchase your device (Windows computer), it comes with many apps that have already been installed and are ready to go. Some very helpful apps with Windows are WordPad, Paint, Calculator, and many others, such as some games, utility apps, and more. You are probably unaware of all the apps that come with Windows that have already been installed. If you want an app you do not have, like a game, Microsoft Word, or Firefox, you must DOWNLOAD and INSTALL it on your device. You are downloading and installing an EXECUTABLE computer file; that is, it can "run" on your device. This file type has a name that ends with ".exe," meaning "executable."

You are probably already aware of a "file" on your Windows computer. A file can be a text document, a photo, or a spreadsheet. If you wanted to create or write a new app from scratch, you would write the app using computer language and write it in a file, too. But what you are doing by writing an app is you are giving commands or instructions for the computer to follow. Suppose you were writing a game app to play tic-tac-toe on your computer; you would have to write instructions for the computer to recognize where each X or O is on the grid and where to place the next move. So this app is written as a file just like any other file except the name of this kind of file ends with ".exe." If you have downloaded (that is, copied a file from somewhere else, like a website, for example), you probably have noticed that the name of the file you downloaded ends with ".exe." In Windows, one way to run such a file is to click your mouse on the file name – your computer sees it as an executable file and runs it.

It is the same if you double-click an app icon on your desktop; you tell the computer to run that app.

Maybe you get notices that there is an update to an app you already have. If you download the update, it is an executable file (a ".exe" file) that you click on to run the update.

Exe files are not for you to open and look at or change. They are in computer or machine" language that you would not be able to understand. But they ARE just files stored on your computer in a program or apps folder. To remove an app from your device, you must UNINSTALL it using a Windows or other utility app to do that. Please do NOT attempt to find the executable file yourself and delete it.

If you want to learn more about executable files or apps, ask Google and watch a short video or two about it. But most of us want the app to run so we can use our device how we want.