Interface

Lorain County Computer Users Group
LCCUG.com (or) info@LCCUG.com
Volume 36 Number 09 September 2025

scams

2025

Inside This Issue

Tuesday
September 9, 2025
10:00 AM

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
September 9, 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

On Labor Day this month, 6 members of LCCUG met at Sugarcreek Restaurant in Sheffield. A couple of members had to cancel. We really enjoyed each other's company and talked the afternoon away.

This group decided they would like to meet again in December for lunch. Hopefully, more members can join us then. We will announce the date soon, so we can plan.

We will continue to hold our meetings in both Zoom and in-person formats. I hope people will continue to participate in one way or another.

We will keep sharing what is new and happening in the technology world.

New technologies will affect everyone in some way, whether it's through better health, faster internet, or smarter homes. While some may take a bit of time to get used to, they promise to make life easier, safer, and more enjoyable. Don't worry, you won't need to learn all of them at once—but being aware of these advances will help you stay up-to-date with the world around you!

And, as usual, that is what we try to do.

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
September 9, 2025

Join us for our September Meetup!
We will once again discuss various interesting topics, focusing on staying safe from scams and also authentication apps you can use.

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

What's Changed in Your Research?

If you have researched your genealogy for some time, how has your research approach changed? Are you more concerned with citation (you should be—within reason)? Are you more concerned with researching people as completely as you can instead of obtaining as many ancestors and relatives as possible? Are you more concerned about accuracy in your compiled information? Are you more concerned with recording unwritten stories before they are lost? Are you more concerned about preserving information and items past your own worldly existence?

And if your research process has changed over time, have you gone back and looked at work you did early in your research to re-evaluate it?

Executive Board Meeting Minutes

JULY 29, 2025

The August Board meeting was held July 29th at Martinios in Vermilion so the board could rate the restaurant as a place for membership get together. Attending were Sandee, Don, Micky and Pam.

The Board felt the Sugarcreek Restaurant is the best place for lunch, however the decision will be left up to membership.

Sandee and Micky will decide the topics for the membership meeting next month.

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, Chris Taylor, 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

AUGUST 12, 2025

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

Sandee and Micky selected 7 different subjects they felt would be of interest to member starting with "Our Life On a Cruise Ship". This was certainly a different lifestyle of living.
The other 6 topics are available on the club internet page.

Micky moved, Sandee seconded meeting be adjourned..

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

Private Browsing: Is it all it's cracked up to be?

By Chris Taylor, President
Ottawa PC Users' Group, Ontario, Canada
https://opcug.ca
Published in Ottawa PC News (November 2023) Editor: brigittelord@opcug.ca

For well over 10 years, web browsers have offered ***private browsing***, designed to keep your browsing—well—private.

Google Chrome calls it an ***Incognito window***, Firefox, Opera & Brave call it a ***Private window***, and Microsoft Edge calls it an ***InPrivate window***. The easiest way to get there is to right-click the browser's icon on the taskbar and choose the appropriate ***New…*** item from the pop-up context menu.

When in a private browsing window, browsing history, cookies & site data (such as images and contents of webpages), and information entered in forms are not saved to your computer. Other users on your computer will not be able to see your web browsing activities. When browsing, web servers won't automatically recognize you as a returning user, and you won't be automatically signed into websites.

When you close a private browsing window, the browser discards site data and cookies created during that session. Note that you need to close the private browsing window to remove traces. Until you do, a simple click on the back button will return you to the previous page visited in that window.

Private browsing deactivates extensions. You can enable extensions in private browsing windows if you need them. For example, in Google Chrome, click the kebab menu (⋮) at the top-right of the window. Choose ***Settings***. Find the extension you want to allow in Incognito windows and click ***Details*** under that extension. Toggle on ***Allow in Incognito***.

Private browsing is not a panacea
It does not prevent all tracking. While websites do not have the luxury of using cookies to track you, there are many other means of tracking. For example, a web server can know your operating system, browser version, extensions you have loaded, screen resolution, IP address, and more. These data items can be used to fingerprint and track you.

Private browsing does not prevent ads. It does not prevent malware. It does not hide where you are browsing from your ISP or employer.

As Gizmodo reported in October 2022, ***Even Google's Own Staff Thinks 'Incognito Mode' Isn't All It's Cracked Up to Be*** - https://gizmodo.com/google-incognito-mode-google-chrome-1849648071

Where is private browsing useful?
If you are using a computer at a public kiosk, it will prevent the next person using the computer from easily seeing where and what you browsed.

If you use multiple accounts on a single website, a private browsing window can help you keep things separate.

If you are using another person's computer, it can be helpful in making it less likely you leave traces behind.

Strangely, I have encountered shopping sites that required private browsing for the checkout process to work properly. I guess they didn't want to sell things to me all that badly.

For more information about private browsing, see https://en.wikipedia.org/wiki/Private_browsing.

You can always find the latest tips in your ask-leo.com account.

The Ask Leo! Tip of the Day

Tip of the Day: Get a PIN Before You Go

If you live in the United States or Canada (and possibly other countries), you're used to using a PIN for your debit card but not for your credit card. While the traditional swipe-and-sign credit card use is seen less and less in favor of chip readers and tap-to-pay, most people don't need, use, or have a PIN for credit cards.

If you're about to travel — particularly to Europe — check with your credit card provider and see if you can get a PIN for your credit card. Many businesses there are exclusively chip-and-pin. If you can't provide a PIN, you can't use that card. And yes, this is the voice of experience.

I recently returned from a short trip to Europe where I could not use my credit cards at most retail establishments. I had no PIN. I had to use cash or my debit card.

I contacted one of my credit card companies to set a PIN —, which was mailed to my home address. It arrived three days after I returned home.

You'll have greater fraud protection if you're able to use credit cards rather than debit cards, and that could be valuable as you travel. (Also, remember to check your statements and online activity to monitor for unexpected transactions.)

ScamBusters.org

Digital App Wire Transfer Scams: How to Protect Your Money

Instant Money, Instant Mistake: The Hidden Risks of Sending Wire Transfers: Scambusters #1,186

Digital wire scams are quick ways where criminals trick people into sending money online. Once the money is sent, it is often hard to get back. Understanding how these scams work is the first step to protect yourself.

Digital App Wire Transfer Scams: How to Protect Your Money
Digital payment apps have changed how we send and receive money, making transactions faster and easier. However, this convenience has also opened the door for scammers to take advantage of people. Wire transfer scams using digital apps are becoming more common, targeting users of popular platforms like Venmo, Zelle, Cash App, and PayPal.

To protect yourself and your finances, it's important to understand how scams work. Victims often find it hard to get their money back. Once they have sent the money, many digital transfers happen so quickly and cannot be reversed, making these scams especially risky.

What is a Digital App Wire Transfer Scam?
A digital app wire transfer scam happens when criminals trick people into sending money using popular payment apps. Unlike old-fashioned wire transfer scams that require going to a bank, these scams take advantage of how easy and fast mobile payment apps are to use.

Scammers target popular platforms, including:

- Zelle
- Venmo

(Continued on page 7)

(Continued from page 6) Digital App Wire Transfer...

- Cash App
- PayPal
- Apple Pay
- Google Pay

Scammers trick victims into sending them money by pretending these are legitimate transactions. Once the money is sent, it's very hard or even impossible to get it back. This is because most digital payment apps consider these payments as authorized between friends or family.

Digital wire app companies add extra security steps to prevent scams. They verify identities, monitor for fraud, and send alerts about transactions. They warn users before sending money and educate them about common scams. These companies often block suspicious accounts or transfers.

How Scammers Find Their Victims

Scammers use different ways to find and target potential victims:

- **Social Media Research –** Scammers look at social media profiles to gather personal information, learn about people's finances, and find those who might be at risk for specific types of fraud.
- **Data Breaches –** Scammers use personal information from data breaches to create convincing impersonations and targeted approaches.
- **Public Records –** Scammers look for people who may be vulnerable to scams by checking public records, real estate listings, and job postings. They focus on individuals in certain life situations that make them easier targets.
- **Referral Networks –** Some victims accidentally give scammers contact information for their friends and family. This allows scammers to target more people.
- **Random Outreach –** Scammers often try to reach many people by cold calling, texting, or emailing. They hope to find victims who respond among large groups.

The Scammer's Process

Digital wire transfer scams usually follow a clear pattern.

1. **Initial Contact –** The scammer contacts you using one of the methods mentioned above. They often create a sense of urgency or opportunity.
2. **Building Trust –** Scammers work hard to earn your trust. They may show fake credentials, mention shared contacts, or tell made-up personal stories.
3. **Creating Urgency –** The scammer creates a situation that seems urgent and needs quick action. This pressure stops victims from taking the time to check if the request is real. They want you to act quickly on fear.
4. **Requesting Payment –** The scammer asks you to send money using a digital payment app. They often give reasons that seem logical for why this method is needed.
5. **Providing Instructions –** Detailed instructions are given on how to send the money, including specific amounts and recipient information.
6. **Disappearing –** After the scammer receives the money, they may either vanish or keep asking for more.

Red Flags to Watch For

Recognizing these warning signs can help you avoid becoming a victim:

- Requests for immediate payment through digital apps.
- Claims that you've won a prize but need to pay fees upfront.
- Family members are urgently asking for money without checking if the request is real.
- Be cautious of job offers that ask you to receive and send payments.
- People who use dating websites are asked for money.
- Tech support calls asking for payment through apps.
- Do not send money to "verify" your account or identity.

(Continued on page 8)

(Continued from page 7) Digital App Wire Transfer

- Feeling pressured to keep transactions hidden from family or friends.
- Instructions for sending money in small amounts to stay under the radar.

Requests to buy gift cards and share the codes.

Signs You've Been Scammed

If you find yourself in any of these situations, you may be a victim of a digital wire transfer scam:

- Money was sent to someone you don't know.
- The recipient stops responding after getting paid.
- The promised service, product, or help does not appear.
- You find out that the person you sent money to gave you false information.
- You see unauthorized changes to your account in bank or app notifications.
- Friends or family say they are getting suspicious requests that use your name.

Consider this common scenario:

Sarah gets a text message that looks like it's from her nephew. The message claims his phone was stolen and he needs $300 for an emergency. The sender asks her to use Cash App to send the money right away because he fears his parents will find out. Wanting to help, Sarah sends the money without checking if the request is real. Later, she finds out that her nephew didn't lose his phone and never asked for money. The scammer used information from social media to make the request seem real.

Social media has become a hunting ground for finding a quick victim. Scammers are looking for that "easy victim."

What to Do If You Become a Victim

It is important to take immediate action if you believe you've been scammed. The following are resources and steps that can help:

- **Contact Your Payment App –** Report the fraudulent transaction immediately through the app's customer service. While recovery is difficult, some apps may investigate recent transactions.
- **Contact Your Bank –** If your bank account or debit card was linked to the payment app, notify your financial institution immediately.
- **Document Everything –** Save screenshots of conversations, transaction records, and any other relevant information.
- **Monitor Your Accounts –** Check all financial accounts regularly for unauthorized activity and consider placing fraud alerts on your credit reports.
- **Change Passwords –** Update passwords for all financial apps and accounts, especially if you shared login information with the scammer.
- **File Reports –** Submit reports to the Federal Trade Commission (FTC), Internet Crime Complaint Center (IC3), and your local police department.

Conclusion

Wire transfer scams through digital apps are becoming more common. You can protect yourself by following simple security steps. Always check money requests through a different communication method. Don't send money to anyone you haven't met in person, and trust your instincts if something feels wrong.

Real organizations will never ask you to send money using peer-to-peer payment apps. If a family member is in real trouble, you can usually contact them another way. Take a moment to confirm any requests, even if they seem urgent, and don't let pressure push you into a quick decision.

By staying informed about current scams and being cautious with unexpected money requests, you can use digital payment apps safely and avoid fraud.

Remember, Stay Alert and Stay Informed!