Interface

Lorain County Computer Users Group
LCCUG.com (or) info@LCCUG.com
Volume 37 Number 2 February 2026

scams

2026

Inside This Issue

**Thursday
February 12, 2026**

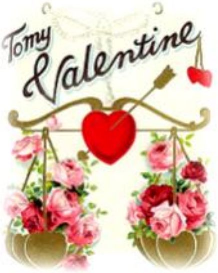
Huntington Bank

Featuring Mel Ellison
and

"Tech for Senior"

Featuring

**Ron Brown &
Hewie Poplock**



Huntington Bank

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
Thursday February 12, 2026 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

I hope you had a nice Groundhog Day!! I hope the message was that there would be an early spring!!!

A reminder that our February and March meetings will be held on the 2nd Thursdays of those months instead of Tuesday. We'll resume Tuesdays on April 14. All these meetings will be held as a hybrid so you can choose to participate on Zoom or in person.

On February 12, we will look at the services offered by the "Tech for Senior" resource. A group of seniors from across North America!! The co-leaders, Ron Brown, is from Western Canada and Hewie Poplock is from near Sarasota, Florida. They have been leading this group for 3 years and have never met!! The group has over 100 members scattered through Canada and the US.

We will look at the benefits of following this group so we can all discover the advantages of being familiar with what they offer. Participating in Tech for Senior doesn't cost anything. Come and discover how to participate.

Although a little belated, at our February meeting, we will ask for nominations from the floor. The current officers would be delighted to have someone step forward to assume one of the roles. Otherwise, the current officers will be presented for voting.

Following our Christmas lunch in December we donated a $200 to Second Harvest Food Bank, like we usually do. We also agreed to donate $100 to Tech for Senior to thank them for being a great resource for us. We often use their short demonstrations during our meetings.

Sandra Ruth
LCCUG President

JOIN US

LCCUG Officers For 2026

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 Education	Neil Higgins education@lccug.com
Statutory Agent	Sandra Ruth statutory_agent@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.

LCCUG
Director of Membership,
membership@lccug.com.

apcug

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

Thursday
February 12, 2025

Huntington Bank **AND**

“Tech for Senior”

Mel Ellison, Huntington Vermilion branch manager, will begin the meeting explaining Huntington's Caregiver Banking option, which can help safeguard your loved one's finances.

Afterwards, we will discuss the Tech for Seniors web site and the information available there.

Genealogy Tip of the day

Michael John Neill , 2 February 2026
Rootdig.com mjnrootdig@gmail.com

The Analysis of Each Statement

Records contain many statements and each of those statements can either be true or false. Analyze each statement separately, thinking about who likely gave the information, how likely they were to actually know the information, and the circumstances under which they were giving the information. It’s also helpful to think about whether the person might have any motivation to give incorrect information and whether there would have been any penalties for giving false information.

It’s also worth considering if more than one person could have been involved in giving the information and how publicly that information was given.

Ask Leo! by Leo Notenboom

Tip of the Day:

Default to Microsoft Office File Types in Open and Libre Office

Setting "save as" preferences in Open Office.
Open Office and Libre Office are two valuable and completely free alternatives to Microsoft Office.

However, even though these alternatives are capable (and did I mention free?), the world still seems to run on Microsoft Office, at least when it comes to file types. Documents are often shared in Microsoft Office file formats — typically one of the "x" formats such as ".docx", ".xlsx", ".pptx" and so on.

Open Office and Libre Office have their own native file formats, but when living in a Microsoft-Office-dominated world, it can be more convenient to configure them to save to the Microsoft Office formats by default. That way, when sharing that document with a Microsoft Office user, there's no question of whether or not they can open it.

Minor formatting and layout differences between the three different packages will remain, but by standardizing the file format, there's one less issue to deal with when exchanging documents.

Bonus Tip: Open Office and Libre Office aren't the only Microsoft Office alternatives. If you're using one of the (many) others, see if you can change the default save-as filetype to be Microsoft Office compatible.

Executive Board Meeting Minutes

DECEMBER 29, 2025

The January officers Zoom meeting was held December 29, 2025 with Sandee Ruth, Don Hall, Micky Knickman, Pam Rihel and Neil Higgins in attendance.

The board discussed the members' reactions to the Christmas luncheon held at Sugarcreek Restaurant in December.

Micky moved, Pam seconded the club donate $200 to Second Harvest. Motion passed.

Sandee proposed she talk about viewing Tech for Seniors at the next meeting.

Don moved, Micky seconded meeting be adjourned.

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

JANUARY 15, 2026

MEETING CANCELED

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/

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

ScamBusters.org
Keeping You Safe from Scams, Fraud and Crime

Fake Apps Are Hiding in Plain Sight

Red flags that signal an app may not be safe: Scambusters #1,208

Many people think that downloading an app from an official app store is safe, but that trust can be wrong. Fake apps are getting through security checks and pretending to be real tools while stealing data, tracking users, or committing fraud. By understanding how these apps get approved and recognizing the warning signs, you can help avoid serious digital and financial harm.

Fake apps are imitation versions of popular applications. They are made to look like real software, using similar logos and designs to trick users into downloading them.

Dangerous Apps (Malware)

Some apps might seem unique or trustworthy, but they can have hidden malware inside them. They are designed to spread harmful software. The function might actually perform the task they advertise (like a flashlight, calculator, or QR scanner) to avoid suspicion. But, in the background, they steal personal data, record keystrokes, hijack banking information, or lock the device.

Where Are These Apps Found?

The most common source of harmful software is third-party app stores. These are unofficial websites or platforms that do not have strong security measures. Downloading an Android Package Kit file from an unknown website is like accepting a package from a stranger in a dark alley.

Users are not completely safe in the "controlled environment" of official platforms. The Google Play Store and Apple App Store have hosted malicious apps by mistake. Even though these companies have strict security standards, their systems are not foolproof.

How Scammers Bypass Official Security

It may seem strange that a huge tech company can be outsmarted by a single hacker, but this happens often. Scammers use advanced techniques to get around the automated checks of Apple and Google.

- **Code Scrambling –** Developers write the code in a confusing way that makes it hard for security scanners to understand what the app really does.
- **The "Dropper" Technique –** The app submitted to the store looks safe and real. After the user downloads it, the app asks for an "important update." This update pulls harmful code directly from the attacker's server, skipping the app store's review process completely.
- **Slow Activation Technique –** Some harmful apps can hide their true intentions after being installed. They act normally for weeks to gain users' trust and receive positive reviews before activating their harmful features.
- **Fake Reviews –** Scammers use bot farms to create thousands of 5-star reviews. This makes the app seem more popular and tricks users into thinking the software is safe.

Why Tech Giants Miss These Threats

The primary reason dangerous apps slip through the cracks is the sheer volume of submissions. Google and Apple review thousands of new apps and updates every single day.

- **Reliance on Automation –** To handle this large volume, companies use automated machine learning algorithms to scan code. While these systems work quickly, they are not perfect and can be fooled by new types of malware that they have not seen before.
- **The Human Factor –** Manual review teams are available, but they can't check every single submission in detail. Scammers take advantage of this by making their apps look as generic and harmless as possible when they submit them.

(Continued on page 6)

(Continued from page 5) ***Fake Apps Are Hiding in Plain Sight***

Removal and Policing of Malicious Apps

When independent cybersecurity researchers find a fake app, Google and Apple respond quickly.

The Removal Process:

- **Delisting –** The app is taken off the store right away to stop new downloads.
- **Banning –** The app's developer account is closed.
- **Remote Deletion –** In serious cases, Google and Apple can turn off or delete apps from users' devices if they are a big security risk. For instance, Google Play Protect regularly checks Android devices and can automatically remove harmful apps.

Identifying the Scammers

Finding the people behind these scams is very difficult. A skilled scammer often leaves a digital trail that leads nowhere.

- **Anonymity –** Scammers create fake identities, use stolen personal information, and set up fake companies to register as developers.
- **Jurisdictional Issues –** Many of these operations take place in countries with weak cybercrime laws or no agreements to send criminals back. A scammer in one part of the world can easily target victims in another, facing little chance of being prosecuted locally.
- **Financial Trails –** Criminals often use cryptocurrencies or money mules to move their profits. This makes it very difficult for law enforcement to trace the money back to a specific person.

Detection Timing – Is it Before or After Damage?

The app store's security filter should catch malware before it goes live. However, many harmful apps were only discovered after they have already been downloaded thousands of times. Detection often comes from:

- **User Reports –** Users noticing strange charges or device behavior.
- **Outside Researchers –** Cybersecurity companies often check popular apps for problems and report any issues they find to Google or Apple.

The Harm Caused by Dangerous Apps

Installing a dangerous app can lead to problems ranging from minor annoyances to serious financial issues.

- **Financial Theft –** “Fleeceware” apps charge very high subscription fees, sometimes hundreds of dollars each week, for basic tasks like photo editing. More harmful banking trojans create fake login screens for real banking apps, stealing your username and password as soon as you enter them.
- **Data Privacy Breaches –** Spyware apps work quietly in the background. They collect contact lists, read SMS messages, track GPS locations, and even access the camera or microphone without permission.
- **Device Performance –** Malicious apps can use your phone's power to mine cryptocurrency or click on hidden ads. This can quickly drain your battery, make your device overheat, and slow down normal operations.
- **Ransomware –** Some harmful software can lock you out of your device or encrypt your files, like photos and documents. It then demands payment to let you back in or to restore your files.

Steps to Take If You Uploaded a Dangerous App

If you suspect an app on your phone is malicious, immediate action is required to minimize damage.

Delete the App Immediately – Don't just delete the shortcut from your home screen. Go to your settings and completely uninstall the application.

Clear Cache and Data – Before uninstalling an app on Android, clear its storage data to make sure no leftover files remain.

Run a Security Scan – Use a trusted mobile antivirus app, like Malwarebytes, Bitdefender,

(Continued on page 7)

(Continued from page 6) ***Fake Apps Are Hiding in Plain Sight***

or Norton, to scan your device for any remaining threats.

Change Passwords – If the app was able to access your device, your accounts may be at risk. Change the passwords for your email, social media, and especially your banking accounts. Do this from a different device.

Monitor Financial Statements – Check your bank and credit card statements regularly for any unfamiliar charges. If you find something suspicious, contact your bank right away to freeze your accounts.

Factory Reset – If your phone is still slow or acting strangely after you uninstall the app, you might need to do a factory reset. Make sure to back up your photos and contacts first because this will erase everything on your device.

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.

(Continued on page 8)

(*Continued from page 7*) *Private Browsing: Is it all it's cracked up to be?*

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.

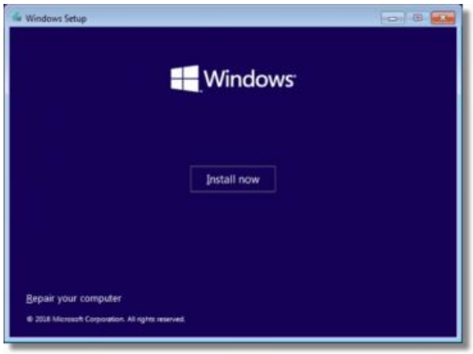
If you use multiple accounts on a single website, a private browsing window can help you keep things separate.

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.

Breaking into an existing Windows installation



Windows installation. (Screenshot: askleo.com)

Breaking into an existing Windows installation is a common topic. Sometimes there is a legitimate need to access information stored on the computer; sometimes it's a not-quite-so-above-board attempt to hack in and steal data.

And sometimes it's nothing more than having picked up a used computer secondhand and wanting to sign in to the already installed copy of Windows.

Don't. Just... don't.

The right solution is to get yourself a copy of Windows (or any other operating system, for that matter) and install it on that previously owned computer *from scratch*, erasing everything currently on the machine. If you're concerned about losing data that's on the machine, there are techniques you can use to back it up first, even if you can't sign in.

Just because it was pre-installed doesn't mean it's legal to include Windows in the sale of the used machine. This varies, of course, with the specific license for the copy of Windows that was included.

At a more practical level, ***you have no idea what's on the machine.*** It could be chock full of malware, or it could just be a bloated install full of things you don't want.

The safest thing to do is to install Windows from scratch. That way, you'll get exactly and only what you need.