

Interface

Lorain County Computer Users Group
LCCUG.com (or) info@LCCUG.com
Volume 37 Number 10 October 2026

scams



2026

Inside This Issue

President's Letter	Pg.2
LCCUG Officers	Pg.2
Program	Pg.3
Genealogy Tip Of The Day	Pg.3
Minutes	Pg.4
How To Avoid Fake Apps	Pg.5
"Save As:" Often	Pg.7
Am I The Only One? Part 2	Pg.8
Add to the Start Menu in Windows 10	Pg.9



**Tuesday
October 13, 2026**



Showing How to Use AI Tools For Both October & November Meetings



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
Back to our regular meeting day & time
Tuesday October 13, 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



Should We Be Afraid of AI?

AI seems to be everywhere online, and we hear more stories about its possible dangers. It's understandable that some people—especially seniors—are choosing to avoid it altogether.

However, many seniors are discovering that AI can be a helpful tool rather than something to fear. It can make everyday tasks easier, help find information, answer questions, and even bring old photos and memories back to life. Like any technology, AI should be used thoughtfully and carefully—but avoiding it completely may mean missing out on some very useful possibilities.

Therefore, our October and November meetings will show examples of these tools as well as other tips and tricks. We are exploring having a restaurant lunch for our December meeting. More information will be coming.

October and November meetings will be on ZOOM and at the usual classroom in Lorain. I hope you can join us.

Sandra Ruth
LCCUG President

LCCUG

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

ROYAL 
business equipment

365-2288 - Elyria

1-800-238-8973 - USA

591 Cleveland Street Elyria, Ohio 44035

- * COMPUTER REPAIR
- * PRINTERS & SUPPLIES
- * UPGRADES
- * CUSTOM PC'S & LAPTOPS
- * CALL FOR BEST PRICES
- * EDUCATION DISCOUNTS
- * LCD MONITORS & TV'S



Shop at **www.ROYALBUSINESS.com** and save \$\$\$

Financing Available - 90 days same as cash

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.

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
October 14, 2026**

Showing How to Use AI Tools For Both October & November Meetings



Michael John Neill [via genealogytipoftheday.com](http://genealogytipoftheday.com)

The Littlest Clue DNA Username Clues, and more

I wrote about these checks from my Grandpa Neill in *Genealogy Tip of the Day* but realized that there's another very small clue in these two checks—one that reminds us of the importance of looking at everything and every detail.

The checks were written in 1941 when my grandparents and their two children were living on a farm a few miles north of Carthage, Hancock County, Illinois. They had lived there since the very late 1930s when they purchased the farm and are enumerated there in the 1940 census.

But why was Grandpa writing checks on a bank in Augusta, Illinois? While located in Hancock County, it's a significant distance from where they lived (approximately 25 miles). Carthage was the county seat. There were banks in Carthage. Ferris, Illinois, was not far away either and also had a bank where Grandpa banked for

some time. But in 1941 my grandparents had not lived on the farm north of Carthage very long.

After their marriage in 1935, my grandparents "took to housekeeping and renting a farm" from my Grandpa's uncle near Plymouth, Illinois. They were living there when the oldest son was born in 1937 and until they moved to the farm near Carthage in the very late 1930s. The likely scenario is that Grandpa still maintained his banking relationship with the bank in Augusta.

At the very least the location of the bank would have been a clue that they had lived in the area if I had not already known that.

December Get Together

The officers would like to have another get together in December. If you are interested in attending please let the officers know. We would like suggestions where you would like to have this luncheon to take place.



Executive Board Meeting Minutes

SEPTEMBER 1, 2026

Officers meeting cancelled.

Cancelled

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, 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

SEPTEMBER 8, 2026

President Sandee Ruth called the Hybrid meeting to order. A motion by Micky was made to accept the minutes as shown in the September issue of the **INTERFACE**, seconded by Ellen Wadge. Motion passed.

Sandee and Micky presented a program, "Interesting Topics & Videos" which were from the 17 they listed on our web page.

Ellen Wadge moved, Nancy Smith seconded the meeting be adjourned.



Member of Association of Personal Computer Users Groups

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

How to Avoid Fake Apps That Want to Steal from You: Scambusters #1,242



Scammers know that seeing a warning about a virus or malware can be frightening. They use fake alerts, pop-ups, and safety apps to make people believe their device is in danger. The goal may be to get you to download an

app, pay for unnecessary services, or give criminals access to your personal information. Knowing what these fake warnings look like can help you avoid becoming the next victim.

Fake Malware and Safety Apps: The Scam Hiding in Plain Sight

Fake apps can be a real concern. They are everywhere. When you look for an app that meets your needs, you may receive many recommendations in your inbox. With so many options available, it can be hard to tell which ones are safe and which ones are not.

Fake antivirus and security apps can trick you into installing harmful software. These scams often show up as pop-up warnings, unsolicited emails, or in third-party app stores. Be cautious of unexpected security alerts, requests for payment or personal information, and apps from untrusted developers. To stay safe, download security software only from *official app stores* and *trusted vendors*.

Cybercriminals know that many people are afraid of malware. This fear helps fake security apps trick users. Instead of protecting your device, these scam apps often install the threats they say they can prevent.

To avoid these scams, you need to understand how they work. This article explains where fake malware apps can be found, who they target, and what you can do to protect your devices and personal information.

Where Do Fake Malware and Security Apps Come From?

Fake malware and security apps usually come from a few common sources:

- ♦ **Pop-up ads** – Scary messages that say "Your device is infected!" and push you to download a fix right away.
- ♦ **Phishing emails** – Messages that pretend to be from real security companies and ask you to install an "urgent update."
- ♦ **Third-party app stores** – Unofficial platforms that do not properly check the apps they offer.
- ♦ **Compromised websites** – Legitimate sites that have been hacked to spread harmful downloads.
- ♦ **Search engine ads** – Paid results that look like real security software but lead to fake downloads.

As usual, scammers use urgency and fear to make you act quickly. When you feel pressured to respond fast, you are more likely to skip the checks that usually keep you safe.

What is Malware and Security Protection?

Malware is harmful software that can damage your device or network, disrupt operations, or steal data without your permission. There are different types of malware, including viruses, ransomware, spyware, and trojans.

Real security software, like antivirus programs and firewalls, helps protect against these threats. It runs in the background to scan files and monitor network activities without needing constant attention or payment.

On the other hand, fake security software often shows false warnings to scare users into buying a "premium" version or giving their payment details.

Who Uses Malware and Security Software?

Many people who use connected devices rely on security software. This software helps protect their devices.

- ♦ **Everyday people** protect their devices from viruses and identity theft.

(Continued on page 6)

- ♦ **Small business owners** keep customer data and financial records safe.
- ♦ **Remote workers** secure company information on their home networks.
- ♦ **Parents** watch their children's online activity and ensure device safety.

This wide range of users makes fake security apps very appealing to scammers. The larger the audience, the more potential victims fall for the scam.

How Is Malware Installed On a Device?

Malware usually gets onto a device through user actions. Common ways it gets installed include:

- ♦ Clicking a harmful link in an email, text message, or pop-up ad.
- ♦ Downloading an app from an unofficial or unverified source.
- ♦ Opening an infected email attachment.
- ♦ Visiting a fake or compromised website that starts a download automatically.
- ♦ Installing a "free" app that comes with hidden malware.

When you see a "free" offer, be cautious. This could be a warning sign. Users often install malware by clicking "Accept" or "Download" without reading the details.

What Are the Red Flags of Fake Malware Apps?

Fake security apps often show these warning signs:

- ♦ **Urgent pop-ups** – These messages say your device is "infected" or "at risk" and often have a countdown timer to cause panic.
- ♦ **Immediate payment requests** – Trustworthy security companies do not ask for instant payments through pop-ups.
- ♦ **Poor grammar or spelling** – Many scam apps have noticeable mistakes that suggest they are not written by native English speakers. But with modern AI, scammers are sounding more professional.
- ♦ **Unverified developer names** – Always check the app publisher's name before downloading.

♦ **Excessive permissions** – Be cautious if a simple app, like a flashlight, asks to access your contacts and messages. Ask yourself, "Why would a 'flashlight' app need access to my contacts?"

♦ **No reviews or suspicious reviews** – A lack of genuine user feedback is a big warning sign.

♦ If an app or alert shows more than one of these signs, treat it as a potential scam.

What if I Visit a Bad Website That Isn't Safe?

If you land on a suspicious or unsafe website, take these steps immediately:

♦ **Close the tab or browser window** without clicking on any pop-ups or download prompts.

♦ **Avoid entering any personal information**, even if the site asks for something as simple as an email address.

♦ **Run a scan** using your device's legitimate, pre-installed security software. Check your malware settings to make sure it runs a scan regularly.

♦ **Clear your browser cache and cookies** to remove any tracking scripts the site may have installed.

♦ **Report the website** to your browser provider or a cybersecurity resource like the Federal Trade Commission (FTC) at <https://www.ftc.gov/>.

♦ If I Click a Link That Leads to Malware, What Should I Do?

♦ Acting quickly can limit the damage. Follow these steps:

♦ **Disconnect from the internet** to prevent the malware from communicating with external servers.

♦ **Run a full system scan** using trusted, verified security software.

♦ **Change your passwords** for sensitive accounts, especially banking and email, from a different, uninfected device.

♦ **Monitor your accounts** for unusual activity over the following weeks.

♦ **Contact your bank** if you entered any financial information after clicking the link.

(Continued on page 7)

(Continued from page 6) *How to Avoid Fake Apps*

- ♦ **Consider a factory reset** if the malware persists after removal attempts.

Do App Stores Protect People From Malware Apps?

Official app stores, like Google Play and the Apple App Store, have processes to check apps for harmful content before they reach users. However, no system is perfect. Sometimes, fake security apps get through these checks, especially if scammers hide malicious code or keep submitting apps under different names.

Official app stores are generally safer than third-party sources, which often have little or no screening. If you want the best protection, choose app stores with good reputations and reporting systems.

How Can I Protect Myself From Dangerous Security Apps?

To protect your devices, follow these simple habits:

- ♦ **Only download apps from official app stores.** Stay away from third-party sites.
- ♦ **Research the developer** before installing any security app. Check their website, read reviews, and look at their history.
- ♦ **Read app permissions carefully.** Question any that seem unrelated to what the app does.
- ♦ **Avoid clicking pop-up security warnings, especially if they demand** immediate payment.
- ♦ **Keep your operating system and apps updated** to fix security issues.
- ♦ **Use a reputable security provider** instead of lesser-known options.

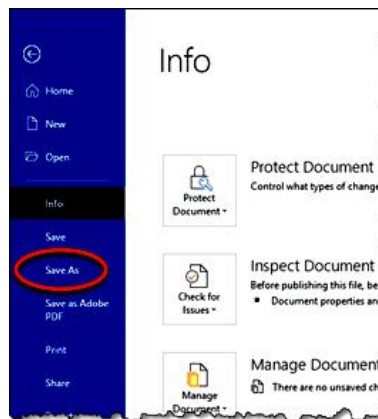
The Bottom Line

Stay one step ahead of fake security scams. Fake malware and security apps can trick people because they prey on a real worry: keeping devices and personal information safe. Watch for warning signs like urgent pop-ups, unverified developers, and requests for immediate payment. These signals can help you avoid scams.

Before downloading any new security app, take a moment to check its source. This small step could protect you from installing the very threat you wanted to avoid.

Copyright Audri and Jim Lanford. All rights reserved. Reprinted with permission. Subscribe free to Internet ScamBusters at <http://www.scambusters.org>

Tip of the Day: "Save As" Often



We often hit "CTRL+S" to save a document we're working on, but that overwrites the previous copy.

An alternative is to use "Save As..." (in the File menu) to give each version a new name as you

Save As in Microsoft Word. (Screenshot: askleo.com)

save. I might save my progress on an important document as a sequence of titles like "Document1.docx", followed by "Document2.docx", "Document3.docx", and so on. When I'm done, I do a final save with its final name, perhaps "Document.docx", and then delete all the intermediate saves.

Why? In case you want to go back to one of the intermediate steps along the way, either to recall what you did or recover what you deleted along the way.

Think of it as a form of manual "undo".

Leo A. Notenboom & Puget Sound Software, LLC.
Ask Leo! is a registered trademark © of Puget Sound Software, LLC

Am I the Only One? Part 2

By Tom Kuklinski, Webmaster at Computer Users of Erie
CUE Newsletter, May 2026
<mailto:Grimcybe@com>

A while back, I shared how I've built up a massive collection of photos over the years and the steps I took to keep them safe. This included a huge batch that I organized in 2014. Since then, I have scanned more and, of course, snapped many more. Yes, massive is well termed. This collection includes 38,265 photos. Today, let's talk about the next big challenge: actually organizing all those digital photos so they're safe, easy to find, and not a complete headache. S

Sounds simple, right? Yeah... it took me many weeks. Many days I did the work across a real mix of devices and operating systems because that's my life: Windows 11 Pro, Linux Mint 22.2, an iPhone, and my Google Pixel 10 Pro XL. I used an old 10-year-old Toshiba 2TB external hard drive, a bunch of USB sticks (more on those later), and Firefox as my main browser.

My Favorite Phone App for Old Paper Photos

One tool that made a huge difference is an app called Photomyme (photomyme.com) on my Pixel smartphone. It's fantastic. You point it at old, printed photos, it scans them, straightens them up, and even fixes crooked or sloppy shots into nice, clean digital versions. You can colorize, crop, and tweak them right there. It also lets you store photos on their site if you want. The app is fast, surprisingly good, and available on both Android and iPhone. Highly recommend it if you have boxes of old family pictures lying around.

Where I Store My Photos

I had spread my collection across a few services:

Google Photos (my main go-to)

Amazon Photos

I tried iCloud but bailed once I saw the paid storage price.

Microsoft OneDrive used to be free-ish, but they tightened things up, and I didn't like how they handled files, so I moved on.

Here's the quick reality check on free storage options:

- Amazon Photos: Unlimited full-resolution photos if you're an Amazon Prime member (videos use a small 5 GB allowance). This is a fantastic perk if you already have Prime.
- Google Photos: 15 GB free (shared with Gmail and Drive). Pretty generous for light users.
- Apple iCloud: 5 GB free — fills up fast.
- Microsoft OneDrive: 5 GB free now.

I ended up buying a paid Google One Plan because it gave me plenty of room plus some nice extras.

Why Google Photos Won for Me

My household is a total mixed bag: my wife lives in the Apple world with her iPhone and iPad, while I bounce between Android, Windows, and Linux. I needed one service that worked smoothly everywhere without constant headaches. After testing everything, Google Photos came out on top for my setup.

Here's why I like it so much:

- It works beautifully on Android (native and seamless).
- The iPhone app is excellent too.
- On Windows and Linux, the web version (photos.google.com) is fast and powerful.
- The AI search is ridiculously good — you can type "beach photos with the kids in 2024," and it actually finds them.
- Automatic face grouping, location tags, and "Memories" make browsing fun instead of frustrating.

For about 50 GB of photos, the 100 GB Google One plan is cheap and gives me breathing room.

The Runners-Up:

- Microsoft OneDrive (through Microsoft 365) is a strong second if you live in Windows and use Office apps. It feels very native on a PC, but the organization tools aren't quite as smart as Google's.

(Continued on page 9)

