Interface

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

scams

2026

Inside This Issue

Tuesday
June 9, 2026

Security, AI & other topics continued

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 June 9, 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

Almost halfway through the year! How fast things are changing in the technology world!!

We thought about electric cars last month.

Now digital glasses have my curiosity:

“Digital glasses, also known as smart glasses, are wearable computers that merge the physical world with digital information. Depending on the model, they can display floating notifications, record video, translate languages, or provide virtual multi-screen workspaces, all while looking like traditional eyewear. “

Like most new technology there will be features that are super cool and generally a lot of issues with our security and privacy. Which will win out?

We are continuing to look at short videos about new features on the computer/phone world.

We are exploring options for a summer lunch. Please send your ideas!

Sandra Ruth

LCCUG President

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

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 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

ATTENTION-ATTENTION

The Board would like to have another get together at a restaurant, maybe in this month.

If you are interested in this get together, please let one of the officers know, so we can get a rough count.

Not sure what restaurant, until we know who is interested.

We really would like it if you would contact Sandee and let her know how many are going to be joining us.

We had a good time at the last luncheon that it would be really nice if we could do it again.

Sandee Ruth
president@lccug.com

Tuesday
June 9, 2026

Security, AI & other topics

Again we will take a look at various fun & informative videos, articles and discussions about safety, security, artificial intelligence, and other topics.

Genealogy Tip of the day

Michael John Neill Rootdig.com
Genealogy Tip of the Day
June 2026

How Many Times Have I Been to the Cemetery?

The author's shadow graces a tombstone in a late afternoon photo taken at the West Point, Illinois, cemetery.

I'm not a big fan of any sort of meme or "busywork" activity, but as I looked at the panoramic picture I took at the West Point Cemetery, I got to wondering "how many times I have been here other than for genealogical research? Had I ever been at the cemetery without writing down an inscription or taking a picture.

Had I ever been there for an actual funeral?

And I could only think of once: my grandmother's funeral in 1994. For some reason I have the vague memory of attending another funeral there and interacting with certain relatives, but I cannot think of who it would be. I must be remembering a different funeral involving my paternal family or have convinced myself that the interaction did not take place at Grandma's funeral. It's just some additional evidence that memory is a fickle thing.

My grandfather died in 1968 and at six months of age, I was too young to attend the funeral. I'm not certain where I was, but I think my great-grandma Ufkes probably watched me while my parents were at the funeral. My great-grandma Ufkes always seemed so old and ancient to me, but when she babysat me she would have been in her early seventies, the same age my mother was when she died. Somehow that does not seem as old now as it did then.

Other members of my paternal family who died after I was old enough to attend funerals were not buried in West Point. My grandpa Neill's siblings are all buried elsewhere as are my grandma Neill's. Grandma is the only member of her family buried at West Point—it's a Neill cemetery and many of my grandfather's relatives are buried there.

And now I am off to think about the other funerals I have attended and where the internment was afterwards and how many times I had been to those cemeteries.

"When did you attend funerals at a specific cemetery?" might be a really good question to ask that family member you are interviewing.

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 & TVs

intel Channel Partner Premier Member 2006

Shop at www.ROYALBUSINESS.com and save $$$
Financing Available - 90 days same as cash

Executive Board Meeting Minutes

MAY 5, 2026

There was no officers meeting for May.

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, Greg Skalka, 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

MAY 12, 2026

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

Sandee and Micky Presented a program, "More Fun & Interesting Videos & Web Sites" which covered electric cars, starting over to Reboot , Pay Pal invoices scam and other videos from Tech For Seniors.

There was talk again of luncheon possibilities.

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

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

Free Wi-Fi or Fake Wi-Fi?

By Scambuster Elle
Issue #1,225 – June 3, 2026
The Dangers in Connecting to Free Wi-Fi: Scambusters #1,225

Public Wi-Fi might be handy, but not all networks are safe. Some criminals set up fake Wi-Fi hotspots to trick people into connecting their devices. If you connect, they could access your personal information, passwords, and online activity without you knowing. By learning how to recognize fake Wi-Fi, you can help keep your identity and personal safety protected.

Free Wi-Fi or Fake Wi-Fi?

Fake Wi-Fi networks are dangerous hotspots set up by scammers to steal your personal data, passwords, and financial information. These scammers make their networks look like real public Wi-Fi. You can protect yourself by using a Virtual Private Network (VPN), turning off auto-connect, and checking network names with staff.

Free Wi-Fi is common in coffee shops, airports, and hotels. People use these public networks to check emails, do work, and browse the internet when they are away from home. Since these networks are open to everyone, they do not have the strong security that private home networks have. Scammers exploit this weakness by creating their own fake networks. When users accidentally connect to these hotspots, hackers can watch their online activity and steal sensitive information.

What Is the Difference Between Free Wi-Fi and Fake Wi-Fi?

Free Wi-Fi is a public wireless network provided by businesses or local governments, like coffee shops and libraries. These places offer free Wi-Fi as a service to their customers. While this type of Wi-Fi is usually not secured and may have security risks, it is intended for people to access the internet.

Fake Wi-Fi, on the other hand, is a network set up by criminals. They want to trick users into connecting to their network instead of the real one. Once someone connects, the criminal can steal information that the user sends online.

Scammers often use open, unprotected networks to target victims. Since these networks do not need a password, it is easy for users to connect, which increases the number of potential victims for the hacker.

How Do Scammers Create and Operate a Fake Wi-Fi Network?

Creating a fake Wi-Fi network is easy and doesn't require much technical skill or expensive equipment. A scammer only needs a portable router or a smartphone that can create a hotspot.

To set up the fake network, the scammer simply makes their device broadcast a Wi-Fi signal. They change the network name, called the Service Set Identifier (SSID), to look like a real business.

For example, if a scammer is at a Starbucks, they might name their fake network "Starbucks_Guest_Free" or "Starbucks-WiFi." Because this name looks legitimate and doesn't need a password, many unsuspecting customers will connect to it from their devices. The scammer's device then acts as a bridge, sending the victim's internet traffic to the real internet while secretly capturing all the data that flows through it.

Can You Check for New Wi-Fi Connections to Verify If They Are Real?

There isn't a public registry that checks new Wi-Fi networks to see if they are real or fake. Wi-Fi works on open radio frequencies, so anyone can create a signal at any time. To verify a network, users should ask the business staff for the official network name and password.

What Are the Common Risks of Connecting to

(Continued on page 6)

(Continued from page 5) Free WI-FI oe Fake WI-FI

a Fake Wi-Fi Network?

Connecting to a fake network puts your device and data in serious danger. The main risks include:

Data Theft – Scammers can steal your login details, credit card numbers, and personal email addresses while you type them.

Malware Distribution – Hackers can install harmful software, like ransomware or spyware, on your connected device.

Session Hijacking – Scammers can take control of your active login sessions. This allows them to access your social media or bank accounts without needing your password.

Discover how to transform everyday waste into beautiful home decor — without spending a fortune! From Trash to Treasure: The Ultimate Guide to Creative Upcycling provides a step-by-step guide to teach you sustainable DIY projects, saving you money and the planet as well.

Start your upcycling journey today with The Ultimate Guide to Creative Upcycling.

Are There Red Flags to Help Recognize a Fraudulent Wi-Fi Network?

You can spot a bad Wi-Fi network by watching for certain signs. Be careful if you notice these warning signs:

Slight misspellings in the network name – Scammers often use typos (e.g., "Airprt_Free_WiFi" instead of "Airport_Free_WiFi").

No password required – If a typically secure location, like a hotel, suddenly has a completely open network with no login page, it may be a trap.

Incredibly slow speeds – Because the scammer's device is routing your traffic through another connection, the internet speed is often noticeably sluggish.

Multiple networks with the same name – If you see two networks called "Cafe_Guest," one of them is likely a fake.

What Is an "Evil Twin" Attack?

An "evil twin" attack is a scam where a hacker creates a fake Wi-Fi network that looks just like a real one. The goal is to trick people into connecting to the fake network instead of the legitimate one.

A real-world example of an evil twin attack can be:

Imagine you're at a busy airport. The airport's official Wi-Fi network is called "Airport_Free_WiFi." A scammer sets up their own portable Wi-Fi router with the same name: "Airport_Free_WiFi." They make their signal stronger than the airport's. When a traveler's phone looks for networks, it connects to the scammer's stronger signal, thinking it's the real airport network. The traveler then checks their banking app. The scammer captures their login details and empties their bank account.

How Can You Protect Yourself from Connecting to a Bad Wi-Fi Network?

To protect your data, take steps to secure your devices when you are in public places. Follow these guidelines:

Use a Virtual Private Network (VPN) – A VPN hides your internet activity. If a scammer tries to steal your data on a fake Wi-Fi network, they will only see scrambled code.

Turn off auto-connect – Turn off the setting on your phone or laptop that automatically connects to Wi-Fi networks you have used before or to open networks.

Verify the network name – Always ask an employee for the exact name of the official Wi-Fi network for the business.

Use cellular data for sensitive transactions – When you check your bank account or enter a credit card number, turn off Wi-Fi. Use your cellular data (4G/5G) instead.

What Should You Do If Your Personal Information Is Compromised on Public Wi-Fi?

If you think you have connected to a fake Wi-Fi network and your personal data may be at risk, act right away to protect yourself.

(Continued on page 7)

(Continued from page 6) Free WI-FI oe Fake WI-FI

Disconnect immediately – Turn off your Wi-Fi to stop the data transfer.

Change your passwords – Use a safe and private network, like your cellular data, to change the passwords for your email, bank, and social media accounts. Also, turn on two-factor authentication (2FA) for extra security.

Contact your bank – Contact your bank or credit card company right away if you think there has been a breach. They can check your accounts for any unauthorized charges or issue you new cards.

Contact law enforcement – Contact your local police and file a formal report.

Monitor your credit – To prevent scammers from opening accounts in your name, place a fraud alert on your credit file. You can do this by contacting the main credit bureaus: Transunion.com, Experian.com, Equifax.com.

Frequently Asked Questions About Fake Wi-Fi

How much does a VPN cost to protect against fake Wi-Fi?

Most trusted VPN services cost between $3 and $10 each month. While free VPNs are available, they often have limits on data, slower speeds, or may not protect your privacy. Paying for a VPN is the best way to keep your public Wi-Fi traffic secure.

How long does it take for a scammer to steal data on fake Wi-Fi?

Data theft can happen very quickly. When you connect to a fake Wi-Fi network and enter your information, like logging into a website or sending an email, the scammer can capture that data right away.

What is the best alternative to using public Wi-Fi?

The safest way to connect to the internet instead of public Wi-Fi is to use your smartphone's cellular data. You can create a personal hotspot on your phone. This lets you securely connect your laptop or tablet to the internet without using risky public networks.

The Bottom Line

Fake Wi-Fi networks are traps set by scammers to steal your personal data, passwords, and financial information. These networks pretend to be real public Wi-Fi by using similar names, tricking you into connecting. Once connected, scammers can hijack your data, spread malware, or take over your sessions.

Look out for red flags like misspelled network names, no password needed, slow internet speeds, or duplicate network names. To stay safe, use a VPN, turn off auto-connect, check network names with staff, and use cellular data for sensitive activities. If you think you've connected to a fake network, disconnect right away, change your passwords, notify your bank, and keep an eye on your credit.

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

There's more to life than new computers.

You're backing up regularly. Yay! But when you try to restore an image backup to a brand new PC, it doesn't go as planned. Image backups are good for many things, but not that.

Question: I'm a good little backup-er. I follow all of your instructions and happily use Macrium for regular image and file folder backups. Recently, the video system on my aging PC died, and I decided to buy a new PC. I thought I could easily restore the image backup to my new PC, thereby saving me hours of reinstalling my software. But no, I can only restore an image to the same sort of hard disk on the same PC. What a waste! Surely most people will want to replace their whole PC when they have a failure that requires them to think about restoring an image. How many people, and in what circumstances, find an image backup has been a lifesaver?

I understand your frustration, but restoring an old backup to a new computer is not what image backups are for.

(Continued from page 7) There's More to Life than a a new Computer

It's also not why you back up.

An image backup includes the detailed settings and configuration information for the specific hardware being backed up. When restored to a new/different machine, those settings no longer apply. The backup can still be useful, but not for what you're trying to do.

So, when is an image backup useful? Let's look at a couple of scenarios.

Image backups are great, but they're primarily for your current computer, not a new one. If your hard drive dies, swap in a new drive and restore your backup. Fighting malware? A backup wipes the slate clean. Moving to a new PC? Start fresh with a clean install, and restore your data from that backup.

When your hard disk fails

If your hard disk fails, you don't need to replace your entire computer. Just get a replacement hard drive (perhaps a bigger one, to increase capacity, while you're at it) and swap out the old drive for the new.

That's a perfect scenario for an image backup.

You restore the backup image to the new hard disk, reboot, and it's as if nothing happened. (If the new disk is larger, you might need to fire up the disk manager tool to extend the partition and use the additional space.)

When malware strikes

You can try to disinfect and remove malware, but once you're infected, you've basically lost control of your computer. You may have clean scans, but you never really know all the malware is gone unless you restore to a backup image taken before the infection.

This is one of the more common uses for image backups.

There's nothing as reassuring as being able to say, "Oh, well, darn, my machine's been infected! I'll just restore to last night's backup", and poof, the computer is clean, and life goes on.

When you want to copy or restore some files

The reason images are so wonderful is that they contain everything. You don't have to rely on figuring out what needs to be backed up beforehand, so you don't have to worry that you missed something.

However, you don't need to restore an entire image. You can pick and choose what you want to restore to your computer or copy to a new one.

If I delete a file today that I later find out I needed to keep, I can go to the image backup I took last night and restore the file. Similarly, your image backup makes a handy way to transfer data files when you move to a new machine.

When you move from one computer to another

It is sometimes physically possible to do what you ask: you can restore an image to a different device, reboot, and hope it works. Windows will do its best to reconfigure itself on the fly to what it sees as a massive hardware change.

While I admit it's gotten better over the years, it's not something I would rely on. Remember, the image contains Windows as configured for the old computer's hardware. Booting it up onto a different computer is a kind of digital culture shock; everything Windows knew about the hardware is instantly and massively wrong.

Often, your computer will not boot, or will run with many problems quickly apparent. Even if things look fine, you can never be sure some configuration problem isn't hiding, waiting to cause you grief.

Some backup programs attempt to address this issue; they try to reconfigure an image tak-

(Continued on page 9)

(Continued from page 8) There's More to Life than a a new Computer

en from one computer and “restore” it to new hardware. Macrium Reflect includes this feature, called “ReDeploy”, in its Professional version. I have used it at least once1, and it did okay. There remained a few issues, but it served my needs at the time. If this is a direction you must go, using a tool like ReDeploy would be my recommendation.

Do this

Image backups are valuable and useful for many different scenarios. Their primary purpose is to back up your existing computer, not set up a new one.

When you move to a new computer, the best solution — for many, many different reasons — is a fresh start with a clean install.

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

Tip of the Day:

That Simple Feature Isn't So Simple

"But it would be so easy for the programmers to do!"

As you can imagine, I get that kind of comment from time to time when I tell people that, no, a feature to do X doesn't exist, and, in fact, there's no realistic way to do X.

The specific scenario that prompted this tip related to the ability to back up and restore a specific subset of autocomplete information in an email program. It seems straightforward: keep a list somewhere. Back that file up, and you have it; replace that file, and you've restored it.

An idea like this is a great example of how mind-blowingly amazing it is that any software works at all.

Here are some of the issues that come up.

- The feature needs to be localized into all the languages supported by the program. Even if there's no actual display text in normal usage, error messages need to make sense, and the feature itself (an autocomplete backup file, in this example) must support all possible languages and character sets.

- The feature needs to be tested in all possible configurations, including all those languages and whatever OS or program variations might impact it.

- The feature needs to be hardened. Maybe this feature has an exploitable vulnerability that can be used to gain unauthorized access to your email or even to the operating system itself. This must be considered, designed for, and tested for.

- The feature needs to be documented. Someone needs to write instructions on how to use the feature; otherwise, it's as if the feature doesn't exist.

The documentation for the feature needs to be localized into all the languages supported by the program.

There's more, but you get the idea.

While you might disagree with the features and functionality software vendors choose to spend time on, you can see that even so-called simple features have dramatic and easily overlooked costs.

This work by Ask Leo! is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. Additional information is available at https://askleo.com/creative-commons-license/.