

# Interface

Lorain County Computer Users Group  
[LCCUG.com](http://LCCUG.com) (or) [info@LCCUG.com](mailto:info@LCCUG.com)  
Volume 37 Number 4 April 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
The Language of Scams...	Pg.5
Back Up Your Cloud	Pg.7
Remember When	Pg.8
LibreOffice Programming Using ChatGPT	Pg.9
Sharing Locations: a Criminal Roadway to Scams	Pg.10



**Tuesday  
April 14, 2026**

## Tech for Seniors

*Featuring*

**Ron Brown &  
Hewie Poplock**



**Our links can be found at:**

[LCCUG.com/links](http://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 April 14, 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](mailto:info@lccug.com)**

**if you have any questions or concerns!**



# A Word From Our President



How many of our members use a smartphone versus a computer? Of those who use a computer, how many use a laptop versus a desktop? Or a tablet.

It's like more and more of our members are just going to a phone to do their look-ups, check their email, send a text because that has become their primary use for a computer or phone.

But it would be useful to determine this so we would know how to focus our meeting topics in the future. We're going to try to survey members and gather that information among ourselves.

Some research and found this picture of technology use in the United States:

In the United States, smartphones are now the main way many people access the internet, but computers are still widely used, especially for work, school, and more detailed tasks.

Among older adults, the pattern is different: seniors are more likely than younger adults to have lower overall device use, and they are less likely to rely on smartphones as their only way online. Even so, many seniors do use smartphones and computers, especially as more services move online.

The overall picture is that younger adults tend to use both devices heavily, while seniors are more likely to use fewer devices and may prefer computers or limited smartphone use depending on comfort and need.

We have exciting options at this time!

Remember we are back to meeting on the 2nd Tuesday at 10 am in Lorain or on ZOOM. See you then.

**Sandra Ruth**  
**LCCUG President**



## LCCUG Officers For 2026

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

## 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.

Tuesday  
April 14, 2026



# Tech for Seniors

Featuring  
Ron Brown &  
Hewie Poplock



Again we will take a closer look at their website. This Website will help learn how to access their materials on your own, so you can continue learning at your own pace between meetings. This Tech for Seniors has so much to offer the older adults with many videos on how to use your computer.

## Genealogy Tip of the day

Michael John Neill [Rootdig.com](http://Rootdig.com)  
3 April 2026

### For Example: What Is Viz?

*I am always a little hesitant to write about grammar, because it's not really my thing. But we will give it a go here because these words are often used in genealogical materials and legal items.* Their use is much less frequent today, especially in a non-academic setting.

Old newspapers and obituaries often contain the abbreviation *viz.* Some genealogists wonder exactly what *viz.* means, so in this tip we will look at three abbreviations that often are confused. Our discussion of them is not in regards to modern usage because we are generally talking about materials written or published before 1900.

- *e.g.* from *exempli gratia* – “for example” (common usage is that what follows *e.g.* is an example—or more—and not a complete list of items)
- *i.e.* from *id est* – “in other words” (common usage is to clarify or restate something—not to give examples)
- *viz.* from *videlicet* – “that is” (common usage is that what follows is a complete list)

## The reality:

James Jones was born in Harford County, Maryland and his wife was born in Smith County, Ohio. They were married in Smith County, Ohio, in 1830. James and Elizabeth (Smith) Jones had children named Riley, James, John, Martha, Thomas, and Elizabeth. In addition to being a farmer, James was a cooper and also helped make ends meet by fixing wagon gears and wagon wheels.

## The statement in the county history (using *e.g.*, *i.e.*, and *viz.*) :

James and Elizabeth (Smith) Jones came to the county from Coshocton County, Ohio, in 1847. James was born in Harford County, Maryland, and Elizabeth was born in Smith County, Ohio. James and Elizabeth were married in her native county (*i.e.* Smith County) in 1830. James operated a farm after their marriage and also did coopering and other work (*e.g.* wagon fixing and threshing) for nearby farmers. They were the parents of six children, *viz.*: Riley, James, John, Martha, Thomas, and Elizabeth.





## Executive Board Meeting Minutes

**March 3, 2026**

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

The board discussed different activities the members might enjoy outside computer/internet information. Sandee is working on next weeks program of protecting seniors from online scams.

### ATTENTION-ATTENTION

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

**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.**



## General Meeting Minutes

**March 12, 2026**

President Sandee Ruth called the hybrid meeting to order. A motion by Margie Soto-Rivera was made to accept the minutes as shown in the April issue of the *INTERFACE*, seconded by Micky. Motion passed.

Sandee and Micky then presented their program **TECH FOR SENIORS, HUNTINGTON, AND SECURITY, HOW TO PROTECT YOURSELF FROM ONLINE SCAMS.**

They started by telling of the 3 second scam when you receive a telephone call from an unknown number. How to wait, do not say anything and when you do what not to say.

Attendees had many questions which Micky and Sandee answered.



### 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](mailto: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, Alan German, APCUG, Google Images, Microsoft Office art online, AARP

Newsletter is now  
Online at:  
[lccug.com/newsletters](http://lccug.com/newsletters) or [lccug.com](http://lccug.com)

### 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](mailto:secretary@loraincoogs.org)

## The Language of Scams: What We All Need to Know

By Scambuster Elle  
Issue #1,217 – April 8, 2026

Understanding what scam terms really mean and how to protect yourself: Scambusters #1,217

Scammers rely on confusion as much as they do in tricking you. Terms like “phishing,” “spoofing,” and “deepfake scams” are becoming more common, making it hard to keep track of them. Knowing the language of scams is a strong way to protect yourself and others.

### The Language of Scams: What We All Need to Know

Scammers constantly change their tactics, making it hard to keep up with new threats. They find new ways to trick people into giving away personal information or money. Knowing the basic terms related to scams is one of the best ways to protect yourself. When you understand these terms, it becomes easier to spot when something seems wrong.

This article explains common scam terms in a simple way. By learning how these scams operate, you can better recognize red flags in everyday emails, texts, and phone calls. Let's take a moment to review and make sure we have a clear understanding.

### Common Scam Methods

- Phishing – Fake emails or messages designed to trick you into giving personal information Example: You receive an email that seems to be from your bank claiming your account is locked. You click the link, enter your login details, and the scammer steals your credentials.
- Smishing – Scam messages sent through text messages. Example: Your package is delayed and you need to click the link to re-schedule delivery. Be careful, as the link goes to a fake site that requests your credit

card information.

- Vishing – Phone calls used to scam victims. Example: Someone calls and says they are from your bank's fraud department. They ask you to confirm your account number and password.

- Spoofing – Faking a phone number, email, or website to appear legitimate. Example: Your caller ID shows your local police department, but it's really a scammer asking for money because you “missed jury duty.”

- Social Engineering – Manipulating people into giving up confidential information. Example: A scammer pretends to be IT support and persuades an employee to share their login details.

### Modern / Emerging Scam Tactics

- Quishing (QR Code Scam) – Malicious QR codes that lead to fraudulent websites. Example: A QR code on a parking meter can lead you to a fake payment website that steals your credit card information.

- Deepfake Scam – AI-generated video or audio used to impersonate someone. Example: A manager receives a video message that appears to be from the CEO. The message requests an urgent wire transfer.

- AI Voice Cloning Scam – Replicating someone's voice using AI. Example: A grandparent receives a call that sounds just

*(Continued on page 6)*



365-2288 - Elyria 1-800-238-8973 - USA  
591 Cleveland Street Elyria, Ohio 44035

<ul style="list-style-type: none"><li>* COMPUTER REPAIR</li><li>* PRINTERS &amp; SUPPLIES</li><li>* UPGRADES</li><li>* CUSTOM PC'S &amp; LAPTOPS</li><li>* CALL FOR BEST PRICES</li><li>* EDUCATION DISCOUNTS</li><li>* LCD MONITORS &amp; TVS</li></ul>	
--	---

Shop at [www.ROYALBUSINESS.com](http://www.ROYALBUSINESS.com) and save \$\$\$  
Financing Available - 90 days same as cash

like their grandchild asking for money in an emergency.

- SIM Swapping – Taking control of a person's phone number. Example: A scammer tricks your phone carrier into transferring your phone number to their device. Then, they use the text verification codes sent to your phone to reset your banking passwords.
- Account Takeover – Gaining unauthorized access to online accounts. Example: A scammer can use stolen email login information to access your accounts. They can change the passwords for your bank and social media accounts.

### Everyday Scams

- Romance Scam – Building a fake relationship to gain trust and steal money. Example: Someone you meet online builds a relationship with you over several weeks. Then, they ask you for money because of a sudden "emergency."
- Tech Support Scam – Watch out for messages that say your device has a virus. Example: A pop-up may appear on your computer claiming it is infected. It often includes a phone number to call. If you call, the "technician" will ask to access your computer remotely and will request payment.
- Employment Scam – Fake job offers are used to steal money or information. Example: Be careful if a job offer asks you to pay for training or equipment before you start. Also, do not give your Social Security number until you complete the hiring process.
- Rental Scam – Fake property listings used to collect deposits. Example: A scammer posts a rental listing and claims there is a lot of interest. They pressure you to send a deposit before you can see the property.
- Package/Delivery Scam – Fake shipping notifications. Example: You received a message saying your package could not be delivered. The message includes a link that asks you to pay a small fee for redelivery and asks for your payment information.

- Advance Fee Scam – Paying upfront for something you never receive. Example: You are informed that you have won a prize, but you need to pay a fee to claim it. After you pay, the prize never comes.
- Online Marketplace Scam – Fraud involving buying or selling goods online. Example: A buyer sends a fake payment confirmation and asks you to ship the item before you receive the money.

### Psychological Effects

- Urgency Tactic – Creating pressure to act quickly without thinking. Example: You receive a message saying, "Your bank account will be locked in 10 minutes. Click now to verify." The urgency pushes you to act before questioning it.
- Fear Tactics – Using threats or consequences to force action. Example: A person calls and says they are from the IRS. They threaten that you will be arrested if you do not pay them immediately. This can create panic and make you feel like you have to comply.
- Authority Impersonation – Pretending to be someone in power or a trusted position. Example: A scammer pretends to be a police officer or government agent and asks for payment for a fake legal issue.
- Limited Availability – Making something seem limited to rush decisions. Example: An online ad says, "Only 2 spots left. Act now!" It urges you to buy before checking if the offer is real.
- Pretexting – Creating a believable story to gain trust and information. Example: Someone calls you, pretending to be from your bank. They say they need to check for suspicious activity and ask for your account details.
- Trust Building (Grooming) – Gradually building a relationship before exploiting it. Example: A scammer talks to you over several weeks to build trust. Then, they ask for money, claiming it is due to an "emergency."

*(Continued on page 7)*

(Continued from page 6) *The Language of Scams: What We All Need to Know*

## Conclusion

Knowing these terms helps you recognize patterns in scams. Scammers may change their tricks, but their tactics often remain the same. When you understand how scams operate, you are less likely to fall victim to them.

Scammers are always improving their tricks. Their main goal is to steal your money and personal information. You can stay safe by knowing these common tactics and looking for warning signs early.

Always check where unexpected messages come from. Don't click on suspicious links and never send money or personal details to strangers. If an offer sounds too good to be true or a request seems too urgent, take a moment to investigate. Trust your instincts. Education and a healthy dose of skepticism are your best tools for staying safe online.

Remember, Stay Alert and Stay Informed!

*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: Change Your Password and Your Recovery Information

by [Leo A. Notenboom](#)

If you think you've been hacked, changing your password isn't enough.

I have a full article on this topic, but it's important enough to resurface as a tip as well.

If you're able to recover your account after what you suspect is a [hack](#), changing your password is not enough. You must review and possibly change all the recovery information associated with the account. That may include:

- Alternate email addresses.

- Associated phone numbers.
- Two-factor devices and techniques.
- Linked or logged-in devices.

Possibly more, depending on the service in question.

While a [hacker](#) has access to your account, they can set up their own recovery information and hack right back in after you've recovered the account. You need to ensure that anything they've left behind is removed as soon as possible.

Contents Copyright ©

Leo A. Notenboom & Puget Sound Software, LLC.

Ask Leo! is a registered trademark ® of Puget Sound Software, LLC



## Tip of the Day: Back Up Your Cloud

by [Leo A. Notenboom](#)

By itself, cloud storage is not a backup. If your data is only in the cloud, it's not backed up.

Many people are convinced that [cloud](#) storage provides a [backup](#)...

...until their account gets hacked or the provider has a hiccup, and the data they put in the cloud (and kept *only* in the cloud) is lost and gone forever.

The cloud is only one place, and as we all know, **if it's only in one place, it's not backed up.**

However you use your cloud service and whatever service that might be, make sure you keep a separate, additional copy of the data you keep there. Be it on another computer, an [image backup](#) of your computer, or even another cloud service, having that safety net is important for all of the many reasons any backup is important.

Because without one, you could lose it all.

Contents Copyright ©

Leo A. Notenboom & Puget Sound Software, LLC.

Ask Leo! is a registered trademark ® of Puget Sound Software, LLC

## Remember When

Not sure what year this was In the Lorain Journal



Members of the Lorain County Computer Group: left to right, seated: Cathy Ratcliff, and Pam Rihel, standing, Peter Bateman, Lou Koch and Edith Lewandowski.

Picture was taken at the Gould Auditorium,

# LibreOffice Basic Programming using ChatGPT



By Alan German, Treasurer  
Ottawa PC Users' Group, Ontario, Canada  
Published in Ottawa PC News (August 2023)  
<https://opcug.ca>  
[briggittelord@opcug.ca](mailto:briggittelord@opcug.ca)

ChatGPT (<https://chat.openai.com/chat>) is an artificial intelligence (AI) tool that, amongst other things, can create text based on a request from an end user. So, I thought I would use it to write an article for the newsletter by entering "Write an article for OPCUG's newsletter on LibreOffice Basic Programming." Had I gone ahead with this, you would now be reading the following:

*"LibreOffice is a free and open-source productivity suite that provides several applications, including Writer, Calc, Impress, and Base. These applications are designed to provide a comprehensive set of tools to meet the needs of any user. LibreOffice also comes with a built-in programming language called LibreOffice Basic, which allows users to automate tasks and create custom solutions to enhance the functionality of the suite."*

But, first let me explain the scenario. I have a LibreOffice document (ODT file) that contains the lists of topics that have been covered over the past three years in our weekly online Q&A sessions. Each week, I build an agenda for the upcoming session as a simple text file (TXT) that lists the titles of the topics to be discussed next. This text file is used for various purposes, one of which has been manually adding the list of new topics to the main ODT index file. I wanted to automate this latter process by developing a macro that would read the topics from the text file and add them to the end of the ODT file.

I don't know all that much about object-oriented programming, so, when I want to create a macro for a document in LibreOffice Writer, my practice is to use Google to search for code extracts that I can then modify and string together to produce the final product. And, this is precisely what I did to build the required macro

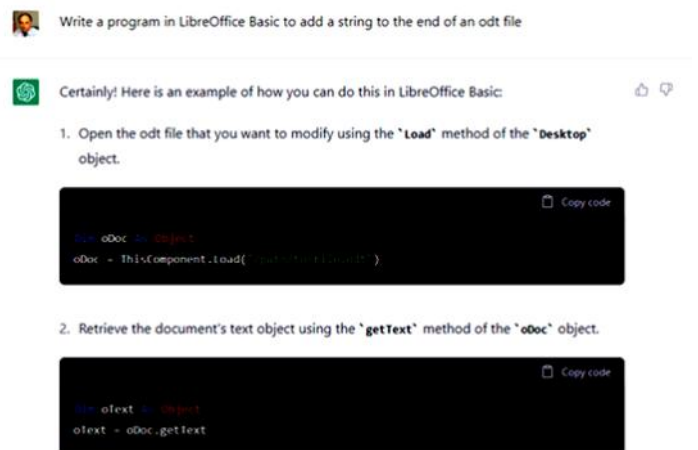
in this case.

But then I saw a YouTube video of an individual using ChatGPT to create computer code in a number of programming languages by simply telling the AI bot what was required. Now, perhaps LibreOffice Basic is a bit of a backwater item in terms of mainstream programming, but I figured that it would be worth a shot to see if I could use ChatGPT to develop the code for my macro.

I know how to read and write lines of text from an ASCII file. My problem is that the ODT file isn't a simple text file. The ODT format is a special type of ZIP file that contains a number of XML and other components. So, the trick is to have the macro open the ODT file, identify the component that contains the body text of the document, add the desired lines at the end, and close the file.

At present, it's possible to use ChatGPT at no cost. All that is required is to create an account on the system or login using an established Google account. Once logged in, one enters a request as a string into a text box. My request was "Write a program in LibreOffice Basic to add a string to the end of an odt file."

*The result was amazing – as shown, in part, by the following screenshot:*



ChatGPT effectively produces a custom tutorial on building the macro. Each required step in the process is explained, and the relevant

*(Continued on page 10)*

code extract displayed. Finally, all the code that has been developed for the requested macro is shown as a complete block:

```
Sub AddStringToODTFile

    Dim oDoc As Object
    Dim oText As Object
    Dim oEnd As Object

    ' Open the document
    oDoc = ThisComponent.Load("/path/to/
file.odt")

    ' Retrieve the text object
    oText = oDoc.getText

    ' Insert the string at the end of the docu-
ment
    oEnd = oText.getEnd
    oText.insertString(oEnd, "This is the
string that will be
    added to the end of the file.", False)

    ' Save the modified document
    oDoc.store

End Sub
```

In essence, this code segment is very close to the macro code that I had produced over some considerable time, having had to research several web postings to identify the required techniques. Clearly, it is very generic code and only covers part of what is required for the final macro. But, it is evident from this simple test that the AI bot is fully capable of generating "modules" of code that can readily be adapted for the desired purpose and that such modules could be quickly consolidated into a fully functional macro.

The other consideration is that the current version of ChatGPT is at an early stage in the development of AI tools. As such applications become more sophisticated and the computer systems running them become more powerful, it is highly likely that their use in computer programming will become ubiquitous.

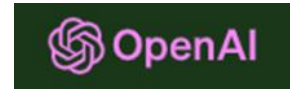
Even now, ChatGPT is perfectly capable of de-

veloping useful code in a number of popular programming languages. For example, in addition to producing macros for LibreOffice Basic, it is just as easy to develop Python scripts. So, ChatGPT is a useful tool for anyone seriously developing programs, macros, and scripts, and is a really interesting option for those who wish to learn the techniques.

## Bottom Line

---

ChatGPT  
(Proprietary, web-  
based system)  
OpenAI  
<https://openai.com>



**Scambusters.org**

## Sharing Locations: A Criminal's Roadmap to Scams

By Scambuster Elle  
Issue #1,216 – April 1, 2026

You check in at a restaurant, post a vacation photo, or share your live location with a friend. It seems simple and safe, right? But what if that same information is being used to track your habits, build a profile of your life, or even target you?

Location sharing has become part of everyday life, but it also creates real risks that many people don't see. Understanding those risks is the first step in protecting both your identity and your personal safety.

### Sharing Locations: A Criminal's Roadmap to Scams

Is sharing your phone's location safe? Most smartphones and apps ask for your location as soon as you open them. You might share your location to find a nearby restaurant, get accurate weather updates, or let friends know where to meet. Sharing your location has become a common feature of modern technology.

However, sharing your exact location can be risky. When you tell people where you are, you also reveal

*(Continued from page 10) Sharing Locations: A Criminal's Roadmap to Scams*

where you are not. This information can fall into the wrong hands, which could lead to serious safety and security issues.

To protect yourself, you need to understand how your location data is collected, who can access it, and how it can be misused.

### **What is Real-Time Location Sharing?**

Real-time location sharing lets your device use GPS, Wi-Fi, and cellular data to share your exact location at any moment. Apps like Google Maps, Life360, and Snapchat use this technology to show where you are on a map in real time. This feature helps with navigation and coordinating with family. However, it also means your device is always sending your location to external servers.

### **How Location Sharing Threatens Your Safety and Identity**

Sharing your real-time location creates a direct link between your digital identity and your physical presence. This overlap creates specific vulnerabilities for both identity theft and personal safety.

#### **Understanding Location Data vs. Personal Info Data**

To understand the risk, you need to know the difference between location data and personal information.

**Location data** – This includes your GPS coordinates, IP addresses, and records of the Wi-Fi networks you join. It tells a system exactly where a device is.

**Personal info data** – This includes your name, email address, phone number, and financial details.

When apps use your location data along with your personal information, they build a detailed profile of you. Scammers and data brokers can then use this combined information to monitor your behavior, confirm your identity, or target you with very specific phishing scams.

### **What is Routine Mapping?**

Routine mapping happens when your phone tracks where you go every day. By looking at your location data, someone, like a stalker, can figure out when you leave for work, which gym you go to, where your kids attend school, and when you get

home. This kind of tracking puts your safety at risk by making your actions predictable.

### **The Risks of Social Media and Photo Sharing**

Social media platforms want you to share your experiences, but how you post is very important for your security.

**Delayed posting vs. real-time posting** – Real-time posting means sharing a photo or status update while you are still at the location. This shows anyone viewing your profile exactly where you are at that moment. It also indicates that your home is empty.

**Delayed posting** means waiting until you have left the venue or returned home before uploading your content. Delayed posting is much safer because it stops anyone from tracking your live movements.

### **Is Tagging Photos Safe?**

Tagging photos with your location is usually not safe. Even if you don't enter your location manually, images often have hidden data called EXIF data (Exchangeable Image File Format). Though this acronym sounds complicated, EXIF records the exact GPS coordinates and the time when the photo was taken. When you upload these images to public sites or unsecured platforms, anyone can access this data and find out where you were.

#### **How Apps Collect and Expose Your Data**

If you keep location services turned on, many apps will track your location. The most common apps that do this include:

- Weather apps – Tracking your city to provide local forecasts.
- Social media apps – Use your location for geofilters and targeted ads.
- Fitness trackers – Planning your running routes.
- Rideshare and delivery apps – Tracking you to coordinate pick-ups and drop-offs.

#### **How to Stop Your Information From Being Collected**

You can take immediate control of your data by adjusting your device settings:

- Turn off global location services – disable GPS tracking in your phone's main settings

*(Continued on page 12)*

when not actively navigating.

- Audit app permissions – Go through your app list and change location permissions from "Always" to "While Using the App" or "Ask Next Time."
- Disable precise location – Many modern smartphones allow you to share an approximate location instead of your exact coordinates. Turn off "Precise Location" for apps that do not strictly need it.

### **The Home Doctor**

#### **The Home Doctor: Practical Medicine for Every Household**

If you want to learn about doctor-approved DIY medical procedures, essential supplies, and self-applied treatments for common health problems and emergencies... you've come to the right place.

This massive 300-page medical guide, with color pictures and complete step-by-step instructions, will help you treat the most common ailments at home or improve your odds while waiting for an ambulance to arrive.

So if you want to manage most health situations at home, especially during crises like blackouts, economic collapse, or natural disasters, then click here for more information.

**Criminals Can Misuse Location Data to Exploit Individuals.**

Criminals actively search for location data to execute targeted crimes. Scammers buy stolen location data on the dark web or gather it from public social media profiles.

They use this information to create believable social engineering scams. For example, a scammer might text you, pretending to be your bank, and mention the exact store you just visited. This makes the fake message seem real.

When your location is exposed, you become vulnerable to several specific crimes:

- Burglary – Criminals monitor real-time vacation posts to rob empty houses.
- Stalking and harassment – Bad actors use routine mapping to follow victims.
- Identity theft – Scammers combine location history with leaked passwords to bypass security

questions and access financial accounts.

### **Populations Most at Risk**

Some groups are at greater risk when they share their location:

- Children and teenagers – Often unaware of the privacy implications of social media, making them targets for predators.
- The elderly – Frequently targeted by localized tech support and grandparent scams.
- Domestic violence abuse – Domestic violence victims are extremely vulnerable to stalkerware and shared family tracking plans.

•

### **Red Flags and How to Protect Yourself**

To protect your personal safety and your data, watch out for these digital red flags:

- Apps asking for unnecessary access – A calculator or flashlight app does not need your GPS coordinates.
- Unexpected battery drain – This often indicates an app is silently tracking your location in the background.
- Unfamiliar login alerts – Notifications from your accounts showing logins from cities you recently visited could mean your data was intercepted on public Wi-Fi.

Check out the YouTube video, *Protect Location Information on Your Phone for Safety Reasons*, that tells how easy your location can be tracked and how to protect your privacy

### **Summary – Take control of your digital footprint**

Sharing your location can put your privacy, safety, and digital identity at risk. By knowing how real-time tracking, mapping, and photo tagging show your daily activities, you can make smarter choices about your device settings. Set your app permissions to "While Using," don't post your location in real time, and check the information you share online regularly. Keeping your location data private is one of the best ways to protect your overall privacy.

*Copyright Audri and Jim Lanford. All rights reserved. Reprinted with permission. Subscribe free to Internet Scambusters at*

<http://www.scambusters.org>