Interface

Lorain County Computer Users Group
LCCUG.com (or) info@LCCUG.com
Volume 34 Number 04 April 2023

2023

Inside This Issue

President's Letter Pg.2
LCCUG Officers Pg.2
Program Pg.3
Minutes Pg.4
LCC-OGS Pg.4
Genealogy Tip Pg.5
Calendar of Events Pg.5
Get a Portable E-mail Address………….. .. Pg.5
Workshops Pg.6
Genealogy Tip Pg.2 & Pg.13
I asked Chat GPT….Pg.7
Your Key Weapon Against Biometric Data Theft Pg.7
Is Windows 10 Going Away? Pg.9
Interesting Finds Pg.10
Most of Us Get It Wrong Pg.11
QR Code Scams Pg.12

Thursday
April 13, 2023

The Amazon Warehouse and Digital Payments: Google Pay Apple Pay, PayPal, etc.

Presented by

LCCUG

In-Person & Zoom Meeting

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

LCCUG Meetings will be happening on ZOOM & in Person

At our new time: from 10 am. - noon

Workshop will be held after the meeting starting at Noon

Please Email: troubleshooting@lccug.com if you have any questions or concerns!

A Word From Our President

We have one more meeting on Thursday morning. Starting in May we will return to Tuesday's morning meetings. We will continue with hybrid meetings indefinitely.

We will also continue to offer troubleshooting and problem solving immediately after our meeting. If you would like to take advantage of this, please email **troubleshooting@lccug.com** so we will know to expect you.

During our Thursday club meeting on April 13, we will have our hybrid meeting at 10 am. We will learn about the option to shop at the Amazon Warehouse. We will learn how to get deals through their Deals warehouse. We can discover whether the Amazon warehouse is cheaper than Amazon outlet.

While Amazon Outlet sells overstock and clearance items, Amazon Warehouse sells open-box items, refurbished items, and returned items. **Amazon Warehouse items are typically priced the most competitively since they are used**. (Nov 28, 2022)

We will also take a quick look inside an Amazon fulfillment center.

We will also look at how to use a digital wallet such as Apple Pay, Google Pay, Samsung Pay, etc., looking specifically at Google Wallet. Is this digital wallet on your phone and/or smartphone safe? Is it convenient? We will use recordings from Ron Brown of Tech for Seniors to look at this.

Sandra Ruth
LCCUG President

Newsletter Editor: Pam Rihel using Microsoft Publisher, 2016

This Month's contributors: Micky Knickman, Sandra Ruth, Pam Rihel, Don Hall, Neil Higgins, Michael John Neill, Scambusters, Ask Leo, Steve Costello, Kurt Jefferson, Phil Sorrento, APCUG, Google images, Microsoft Office art online,

Newsletter is now
Online at:

lccug.com/newsletters or **lccug.com**

LCCUG Officers For 2023

President	Sandee Ruth president@lccug.com
Vice President	**Vacant** vp-programs@lccug.com
Secretary	Don Hall secretary@lccug.com
Treasurer	Micky Knickman treasurer@lccug.com
Newsletter Editor	Pam Rihel newsletter@lccug.com
Web Page Editor	Richard Barnett webpage@lccug.com
Statutory Agent	Sandra Ruth statutory_agent@lccug.com
Director of Membership	**Vacant** membership@lccug.com
Director of Advertising	Richard Barnett advertising@lccug.com
Director of Education	Neil Higgins education@lccug.com

Genealogy Tip of the Day

michaeljohnneill,
Rootdig.com mjnrootdig@gmail.com
michaeljohnneill, 01 Apr 04:08 PM

Not Just One and Only?

If the dates allow, always consider that both members of a couple may have had a prior marriage that resulted in one or more children.

That could explain why certain children are left out of a parent's or grandparent's estate, why it looks like the first child was born before the marriage, or people are marrying individuals who appear to be relatives (but are actually step-siblings).

Thursday
April 13 2023

The Amazon Warehouse and Digital Payments: Google Pay Apple Pay, PayPal, etc.

Presented by

LCCUG Officers

This presentation will explain how to shop and purchase products in the Amazon Warehouse, (usually with a discount). We will also explain the various payment options available.

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

Woohoo!

Membership Dues

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.

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

FEBRUARY 28, 2023

The board Zoom video meeting for March was held February 28 and attended by Sandee Ruth, Don Hall, Micky Knickman, Pam Rihel, Richard Barnett and Neil Higgins.

The March 9 hybrid meeting will about VPN, virtual private network.

The April program will cover Amazon Warehouse and Google Pay.

In May, C-Cleaner and Malwarebytes are being considered.

The board discussed a possible summer picnic or social gathering.

Neil proposed, Richard seconded the meeting be adjourned.

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 using bluejeans.com.

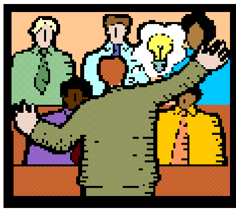
To join the meeting on a computer or mobile phone:

https://bluejeans.com/5006724159?src=calendarLink

Also a link will be sent to you before the meeting.

North Ridgeville Library, 35700 Bainbridge Rd. North Ridgeville, Ohio. Meetings are free and open to the public. Social time is at 6:30 PM and the program begins at 7:00 PM. Canceled Until further notice due to Covid-19

John Kolb



General Meeting Minutes

MARCH 9, 2023

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

Sandee announced next months program will be Tech for Seniors and Ron Brown's Amazon Warehouse Deals.

In May we will be back to Tuesdays for members meetings.

The program "Virtual Private Network", VPN, showed 5 different free providers.

Micky recommended you use VPN when you are in the public domain,

Lata Arora moved, Margie Soto-Rivera seconded the meeting be adjourned. Motion approved by voice vote.

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.

Lorain County Computer Users Group

2023 Calendar of Events

http://lccug.com
email: info@lccug.com

Using Zoom & In Person

Meeting & program starts at 10 am

2nd Thursday of each month. Changes are announced on the webpage and the newsletter.
All meetings are open to the public

January 11, 2023 - QR Code 101 ZOOM ONLY

February 9, 2023 - Artificial Intelligence

March 9, 2023 - Google Voice, VPNs

April 13, 2023 - Amazon Warehouse & Digital Payments

May 9, 2023… to be determined ...

December 12, 2023—Please check our website LCCUG.com for more updates. If you have anything you would like to know about, PLEASE let up know. We would really like your input.

LCCUG

Genealogy Tip of the Day

***michaeljohnneill,* Genealogy tip of the day March 6, 2023**

Rootdig.com   mjnrootdig@gmail.com

Read the Whole Thing

michaeljohnneill, 28 Feb 10:06 AM

This may seem obvious and it is but based on my emails and personal experience, it bears repeating.

Reading an entire document, record, article, etc. before jumping to conclusions, researching, or commenting is advised. This cuts down on research mistakes, creating brick walls where none existed, and making comments that make no sense.

Also giving yourself time to let information digest before moving forward on it is advised as well. Slow down. Your deceased relatives are not going anywhere, but haste in your research may make you look for them in the wrong place.

Search NewsBank’s GenealogyBank for your ancestors.

The Ask Leo! Tip of the Day

Get A Portable Email Address Before You Need It

In a recent article, How Do I Keep My Email Address When I Change My ISP?, I discussed the pitfalls of having an ISP-issued email address when it comes time to leave that ISP's service area.

The same concept applies to email addresses issued by your school or your place of work. When you leave, those email addresses will likely no longer work.

Get that portable email address — be it a free email account such as Gmail or your own domain — now, before you need it, and start using it for your non-school or work related email. You'll be significantly less inconvenienced when the time comes to leave school and/or work behind.

Visit Tip of the Day: Get A Portable Email Address Before You Need It for moderated comments, related links, and updates.

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/.

NEED HELP?

Here's Who to Contact:

Neil Higgins
440-985-8507 - **higgins.neil@gmail.com**
Evenings 6 p.m. -10 p.m. + Weekends
Hardware, Linux & Windows Operating Systems,
Chromebooks, Tweaking your system

Micky Knickman
440-967-3118 - **micky@knickman.com**
Daily 5:00 am to 3:00 pm. Leave message if no answer.
General Software Configuration, Hardware Installation, Basic to Advanced Windows

Richard Barnett
440-365-9442 - **Richard216@aol.com**
Evenings & Weekends
General Software Configuration, Hardware Installation, Basic to Advanced Windows & Web Page Design

Sandee Ruth
440-984-2692 - **sandee29@gmail.com**
Basic Word Processing, Windows, & Web Design
Advanced Internet

Pam Casper Rihel
440-277-6076 or 440-308-8196
6:00 p.m. to 9:00 pm Monday thru Thursday
Genealogy help
prihel1947@gmail.com

Denny Smith Unavailable at this time
440-355-6218 - **dennis.smith@windstream.net**
Microsoft EXCEL
Leave message on machine if no answer

If any of our members are interested in helping other users with what programs you are adept at, please contact any of our officers with you name, what program or programs you would be willing to give help with, you email address and or phone number and when you would like to have them call you. Thanks

LCCUG ONGOING WORKSHOPS

ALL ARE FREE AND SOME ARE OPEN TO THE PUBLIC

Problem Solving Workshop

Date: Thursday- April 13, 2023
Time: 12PM –Please show up by 12:30 Instructor: Micky Knickman
Place: LCCC @ 201 W. Erie Ave., Lorain, OH

Learn how to repair or update your computer by changing hard drives, memory, CD ROMs, etc.

This workshop is limited to LCCUG members in good standing.

The Problem Solving Workshop is being held at our new building, LCCC, 201 W. Erie Ave. Lorain, Ohio

You are asked to bring in your computer, laptop and other electronics that you need help with unless the problem/question can be replicated on any device.

Learning About Electronics

Date: Thursday - April 13, 2023
Time: 12PM –Please show up by 12:30
Instructor: Sandee Ruth
Place: LCCC @ 201 W. Erie Ave., Lorain, OH
Learn how use you electronic devices.

Members are encouraged to bring their tablets, iPod, kindles, etc. for assistance from Sandee and any other knowledgeable members. The public is welcome to sit in on these sessions.

IMPORTANT NOTICE

Changes to the day of our meetings

**Our meetings will now be held on the 2nd Thursday of the month
From January 2023 to May 2023.
The times will be the same.
Workshop is also on Thursday after the meeting.**

Here is a story I asked ChatGPT to write for us.

I asked it to write "a cheery newsletter story for a group of senior citizens about keep up with technology in a fast changing world. "

Hello LCCUG members,
I hope this newsletter finds you in good health and spirits. Today, I want to share a cheerful story about the importance of keeping up with technology in a fast-changing world.

Meet Martha, a 70-year-old retiree who recently decided to take a computer class at her local community college. She was initially hesitant to try something new, but with encouragement from her family and friends, she decided to give it a go.

At first, Martha struggled with using a mouse and navigating the computer screen. But with the help of her patient instructor and a lot of practice, she started to get the hang of it. She learned how to send emails, browse the internet, and even video chat with her grandchildren who live across the country.

As Martha continued her computer class, she began to realize just how much technology had changed since she was in the workforce. She saw how technology had revolutionized the way we communicate, access information, and even shop for groceries. And she knew that if she wanted to keep up with the world around her, she needed to keep learning.

So Martha started to explore other technology resources available to her, like YouTube tutorials and online forums. She even joined a seniors' technology club at her local library, where she could learn from others and share her own experiences.

Now, a year later, Martha is proud to say that she's become quite tech-savvy. She's comfortable using her computer, smartphone, and even her smartwatch. She's able to stay in touch with family and friends more easily, and she's discovered new hobbies and interests through online communities.

Martha's story shows us that it's never too late to learn something new. Embracing technology can be intimidating, but it can also open up a world of possibilities. Whether it's taking a computer class, watching online tutorials, or joining a seniors' tech club, there are many resources available to help us keep up with the fast-changing world around us.

So, let's all follow Martha's lead and keep learning and growing. Who knows what new adventures await us in the exciting world of technology?

Best regards,
Chat GPT and Sandee Ruth **What do you think??**

ScamBusters.org

YOUR KEY WEAPON AGAINST BIOMETRIC DATA THEFT

Security pros keep telling us that the age of the cumbersome use of passwords is nearly over and we'll all be using fingerprints, facial, eye-iris, voice recognition, and other forms of biometrics, even DNA, in their place.

But the bad news is that scammers and hackers have developed software and theft techniques so they can use biometrics and pretend they're you.

And the really bad news is that millions of public biometric records are already for sale on the Dark Web for as little as $5. In fact, according to a biometric specialist in Dubai, hackers who stole a billion records in India have offered access to their database for just $8.

In another famous case, in 2019, fingerprint and facial records were stolen from a security firm's database. Almost 28 million records subsequently appeared on the Dark Web – the Internet area that's not indexed by search engines and where criminal activities are rife.

But hold on. We don't want to panic you – yet. Yes, biometric hacking, as the crime is called, is here, but it's still not widespread in the public domain.

However, it's expected to spread rapidly as the technology is increasingly adopted by businesses and government organizations, but there are two very important things you can do to protect yourself. We'll get to that shortly.

HOW IS BIOMETRIC DATA STOLEN?

The biggest haul of stolen fingerprint, voice, and facial records comes from hacking the systems that store them. It's already happened a few times, going back to 2015 when the US Office of Personnel Management was hacked, giving access to fingerprint data of 5.6 million people.

(Continued on page 8)

(Continued from page 7) Your Key Weapon Against Biometric Data Theft

Of course, there's not a lot that we consumers can do about that sort of crime, apart from being wary about who we give this precious inmation to.

More worrying from a public perspective is the amount of biometric information we give away freely on social media - from high resolution photos and videos on Facebook to pictures of eye makeup that users posted on TikTok. Experts have shown that these images can be used to trick scanners.

Another worry - though it's something for the future rather than today - is that we leave our fingerprints all over the place. Just waiting to be copied. And, as many scanners only use a tiny part of a fingerprint, it's relatively easy to reproduce enough to trick our devices.

Last October, leading security software firm Trend Micro published a 75-page report on the dangers we all face through biometric hacking.

"By publicly sharing certain kinds of content on social media, we give malicious actors the opportunity to source our biometrics," the report says. "By posting our voice messages, we expose voice patterns. By posting photo and video content, we expose our faces, retina, iris, ear shape patterns, and in some cases, palms and fingerprints."

THE MOST IMPORTANT ACTION YOU CAN TAKE

It's important to be aware of this and to exercise extreme caution when posting images on social media sites, especially in groups, public or private, where crooks may hang out. Keep your personal stuff for your own, privacy-protected page. And remember, your personal profile photo is usually available to anyone and everyone, so use a low-resolution image.

But the number one thing you can do to safeguard yourself is to use two-factor or multi-factor authentication (2FA and MFA) on every site that allows you to.

We've written about this several times in the past in the context of password security (see How to Easily Enhance Your Password Security, for example). But it also applies to biometrics. Very simply, 2FA involves having to input an additional code or password to verify who you are. That means that someone who has you biometric data still won't be able to access your accounts and devices unless they also know the relevant code.

Other things you can do to reduce the risk of being victimized by the hackers and tricksters include:

- Thinking twice before you provide your biometrics to anyone. Why do they need it? How do they secure it? Note: This is quite different from providing fingerprint or facial images on a mobile device. This data is stored securely on the device, not on a hackable server somewhere else.
- Protecting the sources of biometric data you carry around with you, like passports, driver's licenses, and Green Cards.
- Monitoring all your accounts, credit scores, and records for evidence of unusual activity. Since biometric hacking, just like password stealing, is mainly used for identity theft, at least you'll know sooner and act faster if you regularly check these.

Using a Dark Web monitoring service to see if your ID information, including email addresses, passwords, and biometrics, have been exposed. Some Internet security software includes this as part of or as an add-on to their services. You can check right now, for free, if your details have been compromised on the Dark Web, using security firm Aura's email scanner. Note that the provider, security firm Aura, offers a paid monitoring service but you don't need to sign up for this.

YOU CAN'T CHANGE IT

Security firms are working flat-out to counter the risks to our biometric data. This includes complex algorithms, artificial intelligence, and

(Continued on page 9)

(Continued from page 8) Your Key Weapon Against Biometric Data Theft

other checks for what's called "liveness" - that the person providing the data is alive!

So, expect to see more and more organizations using the technology for security. It's convenient to use and, at least for now, harder to spoof than guessing passwords. But it's not foolproof.

And here's the thing: Unlike passwords, you can't change your biometric data if it gets stolen. If that happens, it could affect you for the rest of your life.

THIS WEEK'S ALERTS

Distressing AI: The grandparent - or person in distress - scam is alive and well thanks to developments in artificial intelligence (AI). Tech site Ars Technica reports that crooks now need only a few seconds of someone's voice to create a perfect imitation. They can even inject some emotion into calls pretending to come from a friend or relative in trouble and in urgent need of money. If you get a distress call, no matter how convincing, check on the true whereabouts of the person involved.

It's Legit (Probably): The US Census Bureau is currently collecting information from 3.5 million households for its American Community Survey (ACS). But the bureau is worried that people - chosen at random - might think it's a scam. It's not, but that may not prevent scammers from picking up on the survey and trying to trick people. If you get a request and feel uncertain, ask your regional census office to confirm. Check out the interactive map of offices to find yours.

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

Ask Leo! by Leo Notenboom

Is Windows 10 Going Away?

All good things come to an end. Or do they?

by Leo A. Notenboom

Windows 10 going away?

Windows 10 is going away in the sense that you'll no longer be able to purchase it and it will stop being updated at the end of 2025. Windows 10 isn't going away in the sense that it'll keep working after the end-of-support date. With a little common sense, you'll be able to continue to use it for a long time.

Windows 10 is and is not going away. It depends on your perspective.

Applies to Windows: **10**

So, is Windows 10 going away or what? If so, when? And what should I do about it?

Yes, it is…

And yet it's not.

It's complicated.

Microsoft has a vested interest in the "Yes it is" answer, and that's what they promote. However, reality is a little more complicated than that.

Windows 10 going away?

Windows 10 is going away in the sense that you'll no longer be able to purchase it and it will stop being updated at the end of 2025. Windows 10 isn't going away in the sense that it'll keep working after the end-of-support date. With a little common sense, you'll be able to continue to use it for a long time.

The article, How Long Will Windows 10 Be Supported? has more details on the scheduled demise of Windows 10.

(Continued on page 10)

(Continued from page 9) Is Windows 10 Going Away

Yes, Windows 10 is going away

Microsoft announced a **formal end-of-support date for Windows 10 Home and Pro editions: October 14, 2025**. After that date, there will be no further updates to the operating system.

Inferring from the documentation, at this writing it's likely there will be only one more "major" update: 23H2, in the second half of 2023. There will presumably be bug fixes and security updates until the end-of-support date.

In a sense, Windows 10 is already going away. It's difficult to find copies to purchase legitimately,[1] and new machines generally come with Windows 11 pre-installed.

It's safe to assume it'll be more and more difficult to find Windows 10 for new installations over time.

It's going away.

The article, What Happens at Windows 10 End of Support? goes into more detail about how Windows 10 will slowly die.

No, Windows 10 is not going away

Nothing magical happens on October 14, 2025.

Computers running Windows 10 will continue to operate just fine.

Microsoft will not force you to upgrade or take any other action. They may pester you about upgrading, as they've done before, but there's no requirement that you do so.

Your copy of Windows 10 will simply stop getting updates. Some components — like the Windows Security database (likely, but not guaranteed) and Microsoft applications installed on the system — will continue to be updated.

Related

We've been here before.

Will Windows XP Keep Working after Support Ends?

Will Windows 7 Keep Working After Support Ends?

There are people who continue to run Windows 7, and even Windows XP and Vista, *years* after their end of support. While theoretically they're at somewhat higher risk of security issues, there haven't been mass exploitation events when the final date passed. Used with common sense and perhaps third-party tools to increase security, they continue to be used safely and effectively.

It's not going away any time soon.

Yes, Windows 10 is going away… eventually

A more practical cause of Windows 10's demise has nothing to do with Windows 10 itself, but rather the other software you run on it.

Over time, vendors will remove support for Windows 10.

This means that if you want to upgrade/update some package you've been using on Windows 10, at some point you won't be able to. You'll have to choose to live with whatever version you're left with, find an alternate tool that still works on Windows 10, or upgrade to whatever newer version of Windows is available at the time.

There's no predicting when this will happen, other than to say that it'll be a while, and it depends a lot on what tools you use.

Let's face it, some software you purchase today will still run in Windows XP.

Windows 95 compatibility, however, is rare. Someday, that'll be true for Windows 10 as well.

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/.

Interesting Internet Finds August 2022

by Steve Costello
scostello@ sefcug.com

Android Cellular Data Not Working? 8 Ways To Fix
https://helpdeskgeek.com/help-desk/android-cellular-data-not-working-8-ways-to-fix/

It is not a question of if, but when your android cellular data will stop working. When it does, refer to this post for cures most likely to work. (Note: I lose my android cellular data at least once a month for some reason but usually get it back in minutes using one of these fixes.)

Is It Dangerous To Use Free Stock Photo Websites?
https://www.plagiarismtoday.com/2022/05/18/is-it-dangerous-to-use-free-stock-photo-websites/

This is an interesting article for the editors and bloggers that use photos from stock photo websites. Just because it is free from a stock photo website does not mean it is safe to use. Check out the advice in this post before using just any stock photo website photo.

Most of Us Get It Wrong: Not Just Teenagers Depend Upon the Internet

By Kurt Jefferson, Editor, Central Kentucky Computer Society
https://ckcs.org/ lextown2@gmail.com

70% of seniors are now online and using technology, reports the World Economic Forum in July 2019. When it comes to the Internet, the website claims it's – No Longer Just For the Young.

"Young people may roll their eyes at older people who can't use technology as fast as they do, but it's wrong to say that older Americans can't use technology. Remember, a baby boomer, Tim Berners-Lee, invented the World Wide Web, so why should we be surprised that they continue to create, adapt, and use new technology?" reports the World Economic Forum.

In January 2022, Pew Research revealed its latest technology poll results. It discovered: "When it comes to internet use, virtually all adults ages 18 to 29 now say they use the Internet (99%). A similar share of those 30 to 49 (98%) say the same. And 96% of those 50 to 64 use the Internet, compared with 75% of those 65 and older who report being internet users."

So, if you're over 50 and depend on the Internet, how do you protect yourself against the onslaught of cybercriminals who want your money? Let's start with good advice from Reviews.org.

First off, don't share your information online. I'm amazed at the number of folks who scream to the world on Facebook or Instagram that their baby is due on a specific date. Isn't that an invitation to a burglary? I mean, mom and dad are obviously at the hospital. Who's at home watching the turf? Just don't make major personal announcements on social media. You're visiting New Zealand over the summer? Keep it to yourself. Why in the world would you list your departure and return dates online? Talk about an opportunity for burglars.

Before clicking on a web link, hover your cursor over it. You should see where the link takes you in your browser's status bar. This prevents you from visiting a rogue website disguised as a legitimate one.

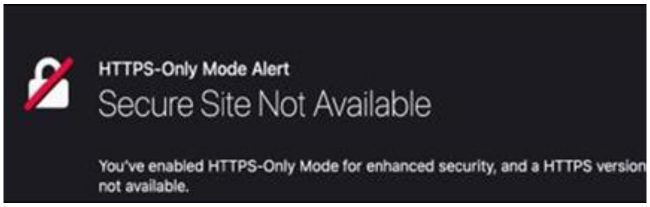
Use only secure public websites and a trusted VPN (virtual public network.) Logging onto unsecured Wi-Fi at a motel, restaurant, library, or airport is just crazy. If you must log onto an open wireless network, ensure your VPN is up and running. (I use a VPN even when a Wi-Fi password is required.)

Experts say you should only log onto websites that begin with https:, but this isn't always possible. For example, if I visit a specific school from the home page of the largest school district in central Kentucky, the page won't automatically load on my version of Firefox. I have a Firefox add-on installed called HTTPS Everywhere, which blocks the page and tells me it's not secure.

A button allows me to continue to the http-only site, but the browser add-on is a red flag alerting me to a possible security problem.

There are plenty more basic security tips on the Reviews.org page. Check them out if you want more security suggestions.

Just because you're over 50 doesn't mean you have to fall for traps designed to steal your money. Be smart. Be safe. Be vigilant. Scammers are out there, even if you cannot see them.



HTTPS-Only Mode Alert

Secure Site Not Available

You've enabled HTTPS-Only Mode for enhanced security, and a HTTPS version
not available.

QR Code Scams – Be careful where you point that smartphone

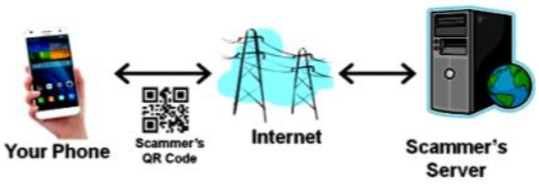
By Phil Sorrentino, Secretary and APCUG Rep, Sun City Center Computer Club
https://scccomputerclub.org/ philsorr@yahoo.com

QR Codes seem to be everywhere today. You'll find them anywhere someone wants to give you more information than is possible by other means, like a sheet of paper or a machine-readable standard bar code. Initially, QR codes were created to track manufacturing processes where barcodes couldn't store enough information. However, a bar code has one dimension. A QR code is 2-dimensional and can store significantly more data than a bar code. Roughly speaking, a QR code may contain as many as 7,000 characters as opposed to a bar code that may contain up to around 40 characters. That's over 170 times the amount of data. This increased amount of information makes the QR code so worthwhile.

QR codes were invented in Japan in the 1990s. They were first used by the automotive industry to manage production but have spread everywhere. There are even websites and apps that let you make your own. A QR code is a machine-readable, 2-dimension matrix of black and white squares. A QR code may represent many different data types, such as text, a hyperlink to a website, a telephone number, an email address, or a text or email message. QR codes, like billboards, clothing labels, walls, TVs, and even tattoos, can be placed on almost anything. QR stands for Quick Response. Quick Response comes from the manufacturing industry and deals with how fast a product can be replaced on the seller's shelves. Quick Response is *"the rapid replenishment of a customer's stock by a supplier with direct access to data from the customer's point of sale." A QR code is merely a data storage representation of some information using the binary code. (For example, the letter A is represented by "01000001") The little squares and patterns of the QR code represent the binary information. The actual QR code is read-only, so it cannot record or steal any personal information on its own. Nowadays, the smartphone's camera app can scan the QR code when the camera is directed at it. (Most smartphones no longer have to download a separate app from the App store for reading QR codes.)*

A QR code with an embedded hyperlink to a website can connect you to a specific website quickly and easily using your smartphone. There is very little one needs to know to take advantage of a QR code. But a lot of the latest technology is being used to accomplish the task. The three major technology components are your smartphone, the internet, and a server (on the internet, or "in the cloud"). This collection of technologies goes by the name "Client-Server Technology," and all three components have been developed to work together. For example, your smartphone has a camera App that connects the smartphone, as the client, to the server website whose URL was embedded in the QR code. (URL is the Universal Resource Locator, the term for a web address on the internet.) This allows the provider of the QR code the ability to connect your phone with the QR code provider's server when you scan the QR code. Once connected to the server, the smartphone can access all the information that the server can provide.

QR codes take people from the physical world to the online (cyber) world. They let smartphones connect to an enormous world of information quickly and easily, but unfortunately, they also allow smartphones to connect quickly and easily to a scammer's website. This is why scammers have started using QR codes in attempting to get in touch with potential victims. It gets people online with the scammer's server. It is similar to "phishing" emails and telephone calls. QR codes are another way for scammers to get in touch with potential victims.



(Continued on page 13)

(Continued from page 12) QR Code Scams

Many scammers (aka cybercriminals) have started to exploit the technology's convenience. Scammers create malicious QR codes to connect unwitting consumers to the scammer's server and dupe them into divulging their personal information. Anytime new technology comes out, cybercriminals attempt to find a way to exploit it. This is especially true with technology like QR codes. It seems like most people can figure out how to use them, but they probably don't really know how they work, and it's always easier to manipulate people when they don't understand their technology. Scanning the scammer's QR codes won't do anything malicious to your smartphone, such as installing malware. Still, it probably will take you to a website designed to try to get personal or financial information from you.

Like any other phishing scheme, it's impossible to know precisely how often QR codes are used for malicious purposes. Experts say they still represent a small percentage of overall phishing, but numerous QR code scams have been reported to the Better Business Bureau. As a result, many people know they need to be on the lookout for phishing links and questionable attachments in emails that purport to be from your bank. But thinking twice about scanning a QR code with your smartphone camera isn't second nature for most people yet.

Recently a QR code scam was uncovered in a Texas city. Drivers were led to a scammer's website after scanning a QR code sticker on a parking meter. Eventually, around 30 such stickers were found. The QR code was supposed to help the motorist pay for online parking. However, instead of being taken to the city's authorized website, the motorist who scanned the fake stickers was led to a fake website that collected their credit card information. With a warning of the parking meter scam, officials in another city issued a warning to motorists after spotting similar stickers on parking meters.

Fake QR codes have even shown up in emails. Scammers may like using QR codes in phishing emails because they often aren't picked up by security software, giving them a better chance than attachments or bad links to reach their intended targets. It boils down to QR codes being just one more way for cybercriminals to get what they want and yet another threat for people to be on the lookout for.

So be careful when scanning QR codes. Here are some tips from security experts. Think before you scan.

Be especially wary of codes posted in public places. Take a good look and determine if the sticker is part of the sign or display. If the code doesn't look like it fits in with the background, it may have been put there by a scammer. Be suspicious of any QR code that comes in an email. If you scan a QR code, look at the website it led you to and determine if it looks like what you expected. If it doesn't look appropriate, then leave the website. If it asks for personal information you don't think is appropriate, don't provide it. And, in the words of one of the Computer Club's past presidents, Matt Batt, "Be careful out there!"

If they are “Divorced”

michaeljohnneill, 31 Mar 02:24 PM

If your relative indicated they were divorced, make certain that you have searched for:

- Records of all local courts that may have heard a divorce case.
- Look for a separate maintenance case as well–there might have been no legal divorce, just a separation.
- Look for land records on the couple for any property they owned.
- Look for any property settlements (even of personal or chattel property) in the local land records.
- Consider the fact that the couple was not legally divorced.