# Interface

Lorain County Computer Users Group
LCCUG.com (or) info@LCCUG.com
Volume 34 Number 08 August 2023

2023

Inside This Issue

**Tuesday**
**August 8, 2023**

## What is Another Name for the Library of Things?

Libraries Are for Everyone

Presented By

LCCUG President
Sandra Ruth

## Zoom & In Person 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**

**From 10 am. - noon**

**Workshop will be held after the meeting starting at Noon**

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

**We are back on the 2nd Tuesday of the month**

# A Word From Our President

**How can we be looking at August already? This is crazy!!**

During our July meeting we looked at some useful tools in our technology world – on our phone or tablet or PC.  Starting with easy access to a Google Solitaire game, Google Keep for notes, lists and memos and so on.

In August I will be talking about free public library resources.  It's been several years since I've done this.  After reviewing some of the great online databases and resources available from our libraries, I will introduce the **Library of Things** that all libraries are participating in, to various degrees.

The idea behind the Library of Things is to promote the sharing economy and reduce wasteful consumption. Many people find that they occasionally require specialized tools, equipment, or appliances for projects, events, or other purposes, but purchasing these items for one-time use can be expensive and environmentally unfriendly. The Library of Things addresses this issue by providing access to a variety of items that people can borrow for short periods, thus encouraging the community to share resources and reduce unnecessary production and waste.

We will look at the libraries in Lorain County and see what their resources are.  Each one has something different!  I will remind you how to get a library card to have access everywhere.

So please attend and be prepared to be surprised and impressed with what you will learn.

We will stay after the meeting for a while to help members with their computer questions.  Let us know that you want to do this so we can be ready. Contact us at troubleshooting@lccug.com.

Be sure to mark your calendar for August 8th at 10 AM and join us at 201 W, Erie, Lorain, or log in via Zoom for an enlightening discussion on the Library of Things and its impact on our community. Looking forward to seeing you there!

**Sandra Ruth**

***LCCUG President***

# *LCCUG Officers For 2023*

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

## 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.

**Tuesday**
**August 8, 2023**

# What is Another Name for the Library of Things?

## Presented By

## LCCUG President Sandra Ruth

Formerly known as Realia, a Library of Things (LoT) is a fascinating collection of items available for loan, expanding the boundaries of traditionally defined library materials.

The concept of the "Library of Things" has emerged in response to the growing interest in sustainable and collaborative consumption models. Similar to a traditional lending library for books, the Library of Things offers a diverse range of items and tools for borrowing. This innovative approach allows people to access items they may need only temporarily or infrequently, promoting a more sustainable lifestyle.

During the meeting, we will explore the various libraries in Lorain County and discover the unique resources they offer. Each library has something different to offer, and you'll be amazed at the possibilities! Additionally, we'll provide a reminder on how to obtain a library card, granting you access to these valuable resources across all participating libraries.

Be sure to mark your calendar for August 8th at 10 AM and join us at 201 W, Erie, Lorain, or log in via Zoom for an enlightening discussion on the Library of Things and its impact on our community. Looking forward to seeing you there!

## 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.

# Executive Board Meeting Minutes

**JULY 4, 2023**

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

Micky reported completing our statement of non-profit to the state of Ohio.

Various programs were discussed for future meetings. Next week's program will be TIPS & TRICKS by Sandee and Micky.

Neil moved, Don seconded the meeting be adjourned.

LCCUG

## 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
secretary@loraincoogs.org

# General Meeting Minutes

**JULY 11, 2023**

President Sandee Ruth called the hybrid meeting to order in a different room at the LCCC building. This room does not require Micky to climb up on tables to adjust the electronics.

A motion to accept the minutes as shown in the July issue of the ***INTERFACE*** was made by Micky and seconded by Cliff Salisbury. Motion passed by voice vote.

Sandee informed members that next months program will be on things available at your local library beyond just books.

Sandee and Micky presented a program showing us some of the many tips and tricks from the various internet sites they are familiar with. Very informative.

## 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

**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, Phil Sorrentino, Jim Cherny, Steve Costello, Scambusters, Ask Leo, APCUG, Google images, Microsoft Office art online, AARP

Newsletter is now
Online at:

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

# 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 - Cellphones, Learning Tips and Tricks**

**June 13, 2023 - Cybercriminals are out to get Us-Senior Scams**

**July 11, 2023 - Useful Tips & Tricks, by LCCUG Officers**

**August 8, 2023 - What is Another Name for the Library of Things**

**September 12, 2023TBA**

**October 10, 2023 TBA**

**November 13, 2023 TBA**

**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.**

## Genealogy Tip of the Day

Rootdig.com mjnrootdig@gmail.com

### Appraised vs. Sale Values

michaeljohnneill, 21 Jul 09:53 AM

If your ancestor's chattel goods were sold at auction after their death, is there also a valuation of the specific property? Comparing the appraised value of items to the sale value can be interesting.

Actual prices can vary quite a bit, depending on the item, who is bidding on it, and how badly they want to purchase it. What's more interesting is to see how the values of items purchased by close family members compare to the appraised value. I've seen a few cases where the prices paid by the widow were a fraction of the appraised value and items purchased by others were closer to the appraised value.

The sale of items may have been a legal necessity, but in some locations, neighbors may have avoided serious bidding if a member of the family was trying to purchase something.

### Do You Have a Space Name?

michaeljohnneill, 19 Jul 09:28 AM

De Moss, Van Hoorebeke, Van De Walle, and similar names with "de," "van," and "van de," have spaces between the prefix and the rest of the name.

The problem is that sometimes they don't have a space between the "van," "van de," or "de" and are all run together. When querying any electronic database for these names, make certain to search for DeMoss, De Moss, and maybe even just "Moss," Different sites handle these names differently and what worked to locate the name on one site may not work on another.

Occasionally Van De gets morphed into "Vander."

# 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:Tuesday– August 8, 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:Tuesday - August 8, 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.

**Member of Association of Personal Computer Users Groups**

ScamBusters.org

# DON'T GET SCAMMED BY DIGITAL E-SIGNATURE CROOKS

If you've ever had to sign a document electronically by pasting your signature or a code into a digital file, you'll know how much time, cost, and hassle the process saves you.

But the growing popularity of e-signatures, as they're called, has also made them a target for scammers, despite stringent security by companies providing the service.

E-signing is widely used in business but it's also increasingly common for consumers - for example, when signing mortgage agreements, tax forms, and many other types of legal documents. But if you get caught out by the scammers, it could cost you a fortune.

The surge in digitally signing a document is a hangover from the Covid pandemic when face-to-face contact was discouraged or downright forbidden.

Since companies and individuals discovered how convenient e-signing is, it's taken off, generating a market worth more than $4 billion a year. As we get used to it, that number is forecast to rocket in the next few years.

As it is, an estimated 95 percent of organizations say they use or plan to use e-signatures in the future.

## HOW E-SIGNATURES WORK

Although, on the face of it, e-signing sounds risky it's possibly more secure than old-style ink signatures - mainly because of the number of security and verification measures service providers have built in and a big reduction in mistakes.

In very simple terms, an individual or company receives a notification that there's a document awaiting their signature. They log onto the website where the document is stored, check it, paste in or even finger-sign their moniker and they're done. The result is a legally enforceable document.

Backstage, there's a lot more to it in security terms but it's really that straightforward. No wonder users prefer it to a time-consuming office meet-up. And businesses save a lot, both in costs and time.

The biggest name in the business is DocuSign. If you haven't already used them, you almost certainly will in the not-too-distant future.

## COMMON E-SIGNATURE SCAMS

Crooks abuse the e-signing process mostly for phishing - trying to steal people's sign-on credentials and other confidential information. Their tactics include:

- Fake notifications that seem to come from a provider like DocuSign, asking users to sign into their account via a bogus imitation login page. Sometimes, they include an attachment that appears to be the specified document but is primed to install malware. Other times, they warn the user that their account has been suspended unless they click a bogus link and enter their login.
- Imposters using forged documents that victims are asked to sign and to add confidential information. The crooks call or use messaging services pretending to be from the e-signature provider or someone else involved in a transaction.
- Doctored docs, when fraudsters intercept legitimate documents after they've been signed and alter them, perhaps adding or removing sections or changing terms and conditions.
- Account takeover. Often the outcome of a phishing attack, crooks gain access to legitimate e-doc accounts, enabling them to forge signatures or redirect payments.

## HOW TO SPOT AND AVOID AN E-SIGNATURE SCAM

There are a number of red flags that signal a potential e-signature scam. Here are some

*(Continued on page 8)*

(Continued from page 7) Don't Get Scammed ...

to look out for:

- An unexpected notification that you have a document to sign when you haven't asked for one.
- You don't know the sender. If you don't recognize the name of whoever sent you a notification, it's likely a scam.
- The link to review the document takes you somewhere unexpected, often with a name that's very similar to a genuine e-sign provider. In the case of DocuSign, messages should come only from docusign.com or docusign.net, not any variation of these names.
- The message contains an attachment. DocuSign, which controls more than 80 percent of the electronic signature market, says it never uses attachments. Users have to visit its website to review documents.
- You get a pop-up box after opening an email. Again, the company says it never uses pop-up boxes because they're not secure.
- The message uses an impersonal greeting like "Dear DocuSign Customer" instead of the recipient's name.
- Poor grammar and spelling. Although less common these days (thanks to artificial intelligence) some scammers still give themselves away with awkward sentence construction and spelling mistakes.
- Asking you to act urgently by claiming your account has been compromised or setting an imminent deadline for a response.

The web page address (URL) you're directed to uses an insecure "http" instead of "https."

### GET MORE HELP

DocuSign has further guidance, including information about what to do if you think you've fallen victim to an e-signature scam. See How DocuSign Users Can Spot, Avoid and Report Fraud.

Ask Leo!®
by Leo Notenboom

### Tip of the Day:

## Comments on Facebook are a Mess

Facebook comment display options:

I'm not talking about the content of the comments; I'm talking about just finding them.

Facebook tries to be "helpful" (I assume that's their intent) by defaulting to showing you only the "most relevant" comments on any Facebook post you might view. Relevance is in the eye of the beholder, and Facebook and I often don't see eye-to-eye. I'm sure the same is true for you.

There are other options if you click on the "most relevant" at the lower right of a post.

"Newest" sorts by most recent, but notice that it also says "Some comments are filtered out". Why? What comments? What triggers filtering? We have no idea.

"All comments" would seem to be the most complete, but even then I find that I have to go in and expand replies, click on "more comments", and more. In even a moderately busy comment section, that gets really annoying really quickly, and it's still easy to miss or overlook comments.

I have no solution other than this: be aware. If you want to see everything, use "All comments" and be prepared to expand replies frequently.

PS: In the example above, "hidden" is shown only to page owners who want to more actively manage comments on their page. I don't think I've ever used it, preferring instead to delete and/or block troublesome individuals.

Ask Leo! by Leo Notenboom

# Dealing with Proprietary Backup Formats

***Will you be able to read them two decades from now? Will you want to?***

by Leo A. Notenboom

If your backup program writes to a proprietary format, you may not be able to access it decades from now. I'll discuss how to prepare.

Locked Hard drive

(Image: canva.com)

How does making image backups relate to the issue with long-term storage that you made a video about a while back? What I mean is a proprietary image format that you may not be able to read in 10 years. What is your strategy with making temporary image backups and long -term backups without proprietary format?

Long-term viability of proprietary formats is an issue that transcends the subjects of backing up and even file formats. As hardware evolves, we run into it frequently. As one simple example, I have floppy disks in my basement that I currently have no way to read.

The concern is that the same thing will happen in software, and specifically back-up software. Will there be software a decade or two from now that will be able to access and read the backup images you've created today?

### Proprietary backup formats

Most good backup tools use proprietary data formats to efficiently back up while simultaneously providing the features of the tool. That's fine for backing up, where the need to access the file decreases rapidly over time. For longer-term archival, using different, simpler tools is a hedge against proprietary formats going away.

### Proprietary

Proprietary simply means that the format of data stored within a file is not public or openly available, and perhaps even considered corporate intellectual property. A backup image made with tool X can be read only by tool X, or, presumably, its subsequent versions. If the company goes out of business or stops producing software that understands that particular backup format, you may be left with no current software capable of understanding and/or accessing it.

Most of the time, this is fine. The companies whose software we choose to use typically outlast our personal use of their tools (Admittedly, not always) or our personal need for the information created using their tools.

Backups are an interesting conundrum, since they are often a convenient way to not only back up something short term, but keep things longer as well. That puts us at interesting risk.

### Open

One common solution is to avoid proprietary formats completely. This can be difficult, as not all the tools we might want to use support open formats.

And sometimes things change. ZIP used to be a proprietary format. PDF was as well. Now they're present in a wide variety of tools from any number of vendors and even in the operating system itself. They're formats that, for a variety of reasons, will be around for a very, very long time. I have no doubt that a PDF of a document I create today will be readable 50 years from now.

Other common formats are likely to either be open, become open, or become so ubiquitous and important that one way or another, there will always be a way to understand them. Microsoft Excel's XLSX format is one such candidate. Regardless of where it is on the spectrum, I'm equally convinced that the spreadsheet I create today will be accessible long after I, Windows, and even Excel itself have passed on. Backup formats may not fall into that category. I'd be surprised if the backup

*(Continued on page 10)*

(*Continued from page 9) Dealing with Proprietary Backup Formats*

image I create today will be easily accessible 50 years from now.

If that's a goal, then a slight change in thinking is called for.

### Backups: short term

Backups — specifically image backups — are most useful for decreasing short-term risk. By short term, I mean days, weeks, or months. (See How Long Should I Keep Backups? for specific advice on how long to keep 'em.)

Backups decrease risks including malware, accidental data loss, hardware failure, data corruption, failed updates, and more. These all fall into the category of things you'll notice and/or fix pretty quickly.

Image backups are also comprehensive in that they contain everything: the operating system, installed programs, settings, and, of course, your data.

Longer term, however, you may not need or even want all of that data. That's where I take a slightly different approach.

### Archives: for the long term

I don't expect to need my current version of Windows, my settings, or even my installed programs several years from now. What I do want to have on hand, however, is my data: things like my documents, my photos, my videos, and whatever else makes sense for my world. Perhaps the installation programs for some of the software I use. That's what matters, long term.

So I take a different approach. I don't use a backup program and its proprietary format for long-term archives at all. I just copy files. In some cases, I might collect them into a .zip file, but as I said above, that's a format I expect to be around a lot longer than I will.

Note this is for data I want to keep in readable form for years — think decades. I'm not suggesting this method for backing up, because you won't have all the information you need to recover from the risks listed above.

I happen to have the process automated with scripts running nightly, but honestly, all it really takes for a more normal person would be to periodically copy all files of import to a different location, such as an external drive. Even putting them online in the cloud might suffice. That's where my terabyte of photos live, and as a side effect are also replicated to several other machines.

The late Karen Kenworthy also had a popular program — Karen's Replicator — that could perhaps more easily automate the process. There are also many alternatives.

The key here is that archiving uses simpler tools and techniques than backing up, thus protecting you from possible loss of access due to a proprietary tool.

### Hardware longevity

Whenever I talk about archiving or keeping data long term, the issue of hardware longevity and eventual incompatibility comes up. Indeed, What's the Best Long-Term Storage Media? **Tips to Avoid Losing Data in Your Lifetime** is one of my most popular YouTube videos. (Its companion article is **here**.)

As I said earlier, hardware we might have used for what we expected to be long-term storage may no longer be available in the years and decades ahead.

My approach and my advice is to not assume anything. Put another way, assume that whatever you're using today will be inaccessible 20 years from now. Instead, routinely migrate forward.

I had all my data on CDs. I "migrated forward" by copying them to hard disks.

As I got newer, larger, hard disks, I "migrated forward" by copying from the old disks to new.

As I get new technology in the future, I'll "migrate forward" to whatever the current ubiquitous standard happens to be.

I'll repeat the cycle as long as I can. Usually

*(Continued on page 11)*

*(Continued from page 10)* ***Dealing with Proprietary Backup Formats***

every few years.

Interestingly, this is exactly what cloud service providers are doing transparently behind the scenes. You can bet that Dropbox, OneDrive, and others, are constantly, slowly, rolling their hardware forward with new technology. The hard disks they used even just 10 years ago are likely nowhere to be found.

This will make sure the files you care about will be available long into the future.

**Do this**

There is no perfect solution, but understanding the issues ahead of time can dramatically reduce the risk of long-term loss.

The key takeaway here is to think about long-term storage differently. Don't think of it as backups, but instead as archives with a different set of requirements, risks, and approaches.

And yes, regardless of where your archives are stored, make sure they're backed up. If it's in only one location, then it's not backed up.

Subscribe to Confident Computing! It's a hedge against even more risks! Less frustration and more confidence, solutions, answers, and tips in your inbox every week.

**ScamBusters.org**

## THIS WEEK'S ALERTS

**Cheating cheats:** How much do you trust your partner/spouse - enough to shrug off a letter claiming they're having an affair? Scammers in Texas have been sending out personally-addressed letters telling recipients they have hard evidence their partner is involved in an illicit relationship. And they say they'll send you the proof, including photos, if you send them money. Of course, they want you to pay with untraceable cryptocurrency. Trash it.

# Beware of Auto-Pays

Jim Cerny, 1st VP, Education Chair, and Forums Coordinator Sarasota Technology Users Group
https://thestug.org/
jimcerny123 ** gmail.com

It sounds great, doesn't it? Don't bother sending us a check every month – put us on "auto-pay"! We will charge your credit card or get a payment from your bank account every month, so you don't have to do anything. If you make automatic payments, you can forget about paying us! And that's what they hope you do – forget that you ARE paying them every month!

Autopay is a convenient way to allow a company to receive regular payments from you without you having to do anything. Some examples of convenient auto-pay billing are for your internet services, TV cable providers, utility services, entertainment video providers, lawn maintenance, car insurance, home, and appliance insurance, tollway payments, and many others. In fact, almost ANY company would love to have you use autopay to pay them! And why not? If you owned a company, wouldn't you like all your customers to use autopay?

There is nothing wrong with the convenience of autopay, but it is often TOO convenient!

With autopay, you are giving a company permission to get their payment directly from your charge card or checking account. Doesn't this sound like a rather dangerous open-door policy? So here are my tips on the things to be careful about autopay:

1. ALWAYS check your charge card and bank statements CAREFULLY every month and make sure ALL charges are correct!!!

*(Continued from page 11) Beware of Auto-Pays*

2. A company may be able to increase your auto-payment without notifying you. Does your contract with the company clearly state the regular payment amount?

3. If you lose your credit card or have a serious problem with your bank account, you may be given a new credit card or account number. Unfortunately, you must change all your auto-pays to the new account. This can be very troublesome, especially if a company tries to get payment from a closed account – they may cancel their service.

4. There is the danger of over-drafting your account or going over your charge account limit when paying your bills automatically. Therefore, you must ensure all your bills are always paid from accounts with sufficient funds.

5. You need to CANCEL any services you are no longer using. People have begun paying for a new service and forget to cancel the payments to the discontinued service they no longer need or want. Check your statements to ensure you are using what you are paying for.

6. Some companies may add additional charges for services or products, even if you did not order them.

Be careful to understand the advantages and dangers of using automatic payments. My bottom line: Carefully check your payments (checks, credit cards, etc.) every month to make sure your billing amounts and your payments are correct, and try not to use auto-pay unless you really need to.

ScamBusters.org

# WILL SECURITY KEYS SPELL THE END OF PASSWORDS?

Thousands of data breaches and millions of individually hacked accounts and computers remind us of something most of us probably already know - passwords are past their sell-by date.

They're no longer enough to protect us from online scammers and hackers. So, over the past few years, security experts have been coming up with new ideas to protect us from the online baddies.

First, there were password managers helping us to create unique and complex strings of characters that crooks find tough to crack or reuse.

Then there is multi-factor authentication (MFA), which effectively requires a second code, either sent to the user via an SMS text message or generated by an authenticator app on your phone.

Next, we got biometrics - things like fingerprint scanners and facial recognition devices.

We've discussed all of these many times in the past. (Search the Scambusters site for the relevant issues.)

But each of them has weaknesses, We've seen password manager databases hacked, MFA codes intercepted, and facial recognition technology tricked by photographs - though they're all still safer than not using them at all.

More Scam Reports: **Wondering About a Car Scam? 10 More Tricks and Tips You Need to Know About**

What's next?

Two hopeful solutions have shown up on the horizon - USB security keys and passkeys. Let's take a quick look at both. And we prom-

*(Continued on page 13)*

ise not to get too technical!

## SECURITY KEYS

These are usually plug-in USBs that establish a unique relationship with your computer or mobile device. One key can be used on multiple devices but each one has a separate relationship with the key that's established when you set it up.

In simple terms, they check in with each other like all good partners do. If an app or online account doesn't recognize the key or if the key is plugged into an unpaired device, you won't get access.

So, a fraudster would need to have both the device and the security key to cause trouble. Even then, in some cases you might be able to password-protect the key.

Backstage, a lot of technical stuff goes on to encrypt or jumble up the relationship, but you don't need to know about that. Otherwise, setting up is quite easy and straightforward.

Of course, there are downsides, notably the risk of losing the key, which you wouldn't want to keep permanently plugged in for the reason stated above. You'll need a backup solution, available from many providers.

Also, for now, not all devices and online service providers have a security key option. Plus, there are several different types of formats or protocols that work with some devices but not others.

So, before you go down this route, you need to check compatibility - like the right USB connection, the right protocol, and the availability of security key authentication. Most of the big online players like Google, Amazon, and Facebook use them in the same way as multi-factor authentication.

In fact, Facebook has a good page explaining how their security keys work.

Another risk is the possibility of unwary consumers buying doctored security keys from unreliable sources, which then transmit data to scammers.

Bottom line: Used properly, security keys lock out the crooks, even if they know your sign-on details and other authentication codes. Lookalike phishing sites won't work either. It's likely the way forward but you need to spend a little time getting to understand and use them. And always buy from a trusted, reliable source.

## PASSKEYS

Microsoft is betting on this technology as a security solution to replace regular passwords without needing hardware like security keys. Yet, it's still a password of sorts.

Sometimes known as a passphrase, a passkey usually uses a much longer string of easy-to-remember words than conventional passwords - a line from a song for example - that converts in your device to a jumble of unrecognizable numbers.

The string is stored on your computer and the user can then either key it in or use a biometric technique to pair themselves with the device. If they don't match, you don't get in.

The increased length of the passkey and its encrypted storage make it virtually impossible for fraudsters and hackers to identify. It verifies the identity of the user to allow them to access their computer system.

Of course, as with regular passwords, the security of passkeys is only as good as the words and characters the user selects. But because no USB hardware is required (unless you're using biometrics), you're at less risk of being locked out of your device.

On balance, we think security keys point the way forward, but it's perfectly possible to combine the two technologies to make your computer or mobile device security water-tight. Until the crooks find a way of circumventing them too!

# Interesting Internet Finds

by Steve Costello<br>
scostello ** sefcug.com

In the course of going through the more than 300 RSS feeds, I often run across things that I think might be of interest to other user group members. The following are some items I found interesting during April 2023.

New Privacy Tool: Mullvad Browser

https://firewallsdontstopdragons.com/new-privacy-tool-mullvad-browser/

I currently use Google Chrome, Firefox, Tor, and Vivaldi browsers, depending upon the level of privacy and identity hiding needed. Still, I found this post about the Mullvad browser interesting.

Still Using Windows 10 21H2? Time To Upgrade

https://www.computerworld.com/article/3692869/still-using-windows-10-21h2-time-to-upgrade.html

For those using Windows 10, this is a must-read article. It gives the reasons you should upgrade to 22H2 and some reasons you might not have already. (Note: Both my Windows 10 machines are using 22H2.)

Top 10 Ways To Turn Flashlight On And Off In Android

https://www.online-tech-tips.com/smartphones/top-10-ways-to-turn-flashlight-on-and-off-in-android/

Just the day after I read this post, my wife asked me if there was a way to get a shortcut to turn the flashlight on and off for her Samsung Galaxy S3. Luckily, I remembered reading this, and now she has a flashlight shortcut on her lock screen. If you use an Android phone or tab let, check out this post.

What Can You Do With The USB Port On Your Router?

https://www.howtogeek.com/791384/what-can-you-do-with-the-usb-port-on-your-router/

I had never thought about the USB port on a router until I read this post. Unfortunately, my router does not even have a USB port. But I have a neighbor with a 2 TB drive setup on his router for sharing files and backing up his travel laptop.

What's My IP Address And How To Find It

https://www.thewindowsclub.com/whats-my-ip-address-and-how-to-find-it

You might not know your IP address or even need to know right now. Even if that is the case, you should know how to find it, so this post might come in handy someday.

What's The (Number) Added To Some Of My Downloads?

https://askleo.com/whats-the-number-added-to-some-of-my-downloads/

This is one of those things that come up from time to time. When it happens to me, I usually know what it is and why it happens, but not everyone knows about this. If you are one of those that don't know, check out this post.

**How To Make Sure Your VPN Is Working and Protecting Your Privacy**

https://helpdeskgeek.com/how-to/how-to-make-sure-your-vpn-is-working-and-protecting-your-privacy/

Do you use a VPN? If yes, do you know how to ensure it works correctly? Check out this post to learn how to check your VPN for various issues.

**********