2023

Inside This Issue

**Tuesday
November 14, 2023**

Hodgepodge of Topics

Presented by

LCCUG OFFICERS

HAPPY thanksgiving

Using 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 piques your interest.

**LCCUG Meetings will be happening on ZOOM
& in Person at the LCCC Learning Center, 201 W. Erie Ave., Lorain, OH**

from 10 am. - Noon

Problem Solving/Electronics Workshop will be held after the meeting starting at Noon if there is any interest.

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

A Word From Our President

I invited a guest speaker to share with us their thoughts on what technology trends we need to keep up with. Below is their response:

In today's fast-paced digital age, senior citizens must stay attuned to various technology trends to remain connected, informed, and engaged in the modern world. One critical trend is the proliferation of smartphones and mobile applications. These devices are not only communication tools but also gateways to a wealth of information and services. Seniors can benefit from learning how to use smartphones for video calls with loved ones, accessing health-related apps, or even managing their finances. Staying proficient in smartphone technology empowers seniors to maintain their independence and stay connected with their families, all while enjoying the convenience of mobile applications designed to make their lives easier.

Moreover, the internet has become an essential resource for information and social interaction. Seniors need to adapt to online platforms, as they provide access to a wide range of resources, from online shopping and virtual support groups to educational courses and social networking. Seniors who embrace the internet can overcome isolation, find like-minded communities, and pursue lifelong learning. They must also be aware of digital literacy and online safety to protect themselves from potential risks and scams.

Lastly, the field of telehealth has gained tremendous importance, especially in the wake of the COVID-19 pandemic. Senior citizens should become acquainted with telemedicine technology, allowing them to consult with healthcare professionals remotely. This trend not only enhances access to medical care but also provides a safer and more convenient option for routine check-ups, reducing the need for frequent in-person doctor visits. By keeping up with telehealth innovations, seniors can take better control of their health and well-being while adapting to the changing landscape of healthcare delivery.

Thank you, Chat GPT 3.5

Watch your email for information on our December meeting. We are planning to go to Golden Corral for a lunch meeting!! It should be the second week of December. Have a good Thanksgiving!

Sandra Ruth

LCCUG President

Hodgepodge of Topics

Presented by

LCCUG OFFICERS

Our November meeting will be another hodgepodge of topics. We will be looking at more examples of Artificial Intelligence and some tips helpful in using Windows. We will also look at a couple of favorite apps for your smartphone and remind everyone about the Eclipse coming next April 8.

If you have questions on any of these subjects please write them down or email them to the LCCUG officers at: lccugboard@lccug.com.You can click on this link to send your questions.

We hope you can make it to our meeting and bring a friend.

Executive Board Meeting Minutes

OCTOBER 3, 2023

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

The board agreed next week's program will be Sandee giving "TIPS and TRICKS" using your computer.

Glenn Pubal is not available for the November meeting and has been rescheduled for the January 2024 meeting.

Sandee will check out our using Golden Coral for the December meeting.

Don moved, Pam 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
secretary@loraincoogs.org

General Meeting Minutes

OCTOBER 10, 2023

President Sandee Ruth called the hybrid meeting to order. A motion to accept the minutes as shown in the October issue of the *INTERFACE* was made by Micky Knickman and seconded by Nancy Smith. Motion passed by voice vote.

Sandee pointed out the October issue of the *INTERFACE* was available online.

Sandee and Micky presented a program "TIPS and TRICKS" covering many things going on in the online computer world.

MEMBERSHIP WITH LCCUG:

Yearly dues are now $15.00 For 3 years. For more information contact:
LCCUG
Director of Membership,
membership@lccug.com.

Meeting Information:
time: from 10 am. - noon
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 - 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, 2023 - Cookin! Home Automation for your Kitchen! Judy Taylour from APCG

October 10, 2023 - Tricks, Tips & much more by LCCUG officers and the Geek Squad

November 13, 2023 - Hodgepodge of Topics by LCCUG officers

December 12, 2023 - We are planning on having our Christmas Bruch at Golden Coral again this year. 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

michaeljohnneill, 25 Oct 07:10 PM

Who Is Your Brother?

Keep in mind that there are some relationships stated in records that, after some research is conducted, are not as clear as we would like them to be.

"Brothers" could be full brothers or half-brothers. One of the siblings could have been an adopted sibling.

They could also be step-brothers or brothers-in-law.

A Map as a Research Log

24 Oct 09:51 AM

When a manual search of census records is necessary, use a map.

A map will help you keep a geographic perspective when searching and help guide you in knowing where to search if your ancestors are not initially where they are expected to be. The map can also be used to keep track of where searches have been conducted.

The ideal map to use would be one that shows the same enumeration regions that were used in the census. For censuses taken 1880 and after, these enumeration districts had maps created for the sole purpose of census enumeration and sometimes those districts had boundaries that followed civil government boundaries. These enumeration district maps are online at the National Archives and Records Administration website. For enumerations before 1880, enumeration regions also often followed governmental boundaries and contemporary maps are helpful for those searches as well.

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– November 14, 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 - November 14, 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

Tip of the Day: Make Your Passwords Longer

Animation: askleo.com, via https://bitwarden.com/password-strength/

Whenever I recommend that people create complex passwords, I get pushback because complex passwords are too difficult to remember or type.

Even though I recommend them strongly, not everyone wants to use a password manager. Nor is a password manager a solution in every situation.

Today's tip is this: length adds complexity. A longer, simpler password is more "complex" than a shorter combination of random characters.

When in doubt, make your password longer.
One approach I use for passwords I have to type in (as opposed to using my password manager) is to memorize a common phrase and use it (or subsets of it) as my password. For example, you might memorize "mary had a little lamb its fleece was white as snow."

For one site, you might use "mary had a little lamb" as the password. It's nice and long (22 characters), but perhaps a little too obvious. So drop the first word and add the next: "had a little lamb its" is a fine 21-character password. By almost all measures, it's more secure than any eight-character password, even with numbers and symbols, and potentially more secure than even 12 or 16 character passwords.
And it's a lot easier to type.

For another site, you might drop another a word: "a little lamb its fleece" is a fine 24-character password. For another, slide over another word: "little lamb its fleece was". You get the idea. As long as it's easy to remember and you recall which variant goes where, it's safe and secure.

To make things even more secure, choose a phrase that is unique and meaningful to you rather than a common nursery rhyme.

Naturally, this requires that wherever you're setting the passwords accepts passwords of enough length and allows spaces. More and more sites are doing just that in the name of improved security.

Tip of the Day: Send Links Instead of Attachments
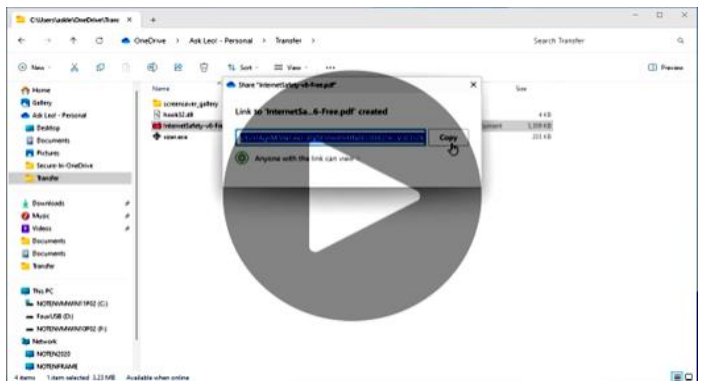
Email attachments — particularly large ones — slow email delivery and are more likely to be flagged as spam. Email with attachments stand a slightly higher-than-average chance of not being delivered at all.

This effective solution takes two steps:

1. Make the file you would otherwise attach visible on the internet somehow.

2. Send a link to that file instead.

It used to be that #1 was out of the realm of possibility for anyone except folks who ran servers on the internet, but that's no longer the case. With the proliferation of cloud storage services like Dropbox, OneDrive, and others, up#1

Send Links Instead of Attachments

loading the file somewhere on the internet is trivial.

Of course, you can use these services to share files and folders with others who have the programs installed as well, but that's not necessary. For example, you can share a link to any file in your OneDrive with anyone whether they use OneDrive themselves or not.

For example, I've placed a file into a folder in my OneDrive. Right-clicking on that file within my OneDrive folder displays a Share option. Within that option, I can choose what kind of a link to share: one that allows the recipient to edit the file — great for collaboration — or one that allows them only to view it.

Copying that link to the clipboard allows you to paste it into your email.

https://1drv.ms/b/s!AgsM3hkLexJ-i8V9H8mlHrHN8EU80Q?e=V3CHZK

Click on that link, and you'll be taken to that file, ready to be viewed or downloaded from

OneDrive.com.

Document shared in and linked to OneDrive. Click for larger image. (Screenshot: ask-leo.com)

The email you send containing a link to a document like this is smaller, delivers faster, and is in fact more likely to be delivered than including the file as an attachment.

PENNY STOCK SCAMS: HOW THEY WORK AND HOW TO AVOID THEM

 There's big money to be made from trading penny stocks. But a lot of it is by scammers. And there's no shortage of potential victims.

Every year, investors hunting get-rich-quick opportunities, lose millions of dollars buying and selling penny stocks - actually called micro-cap stocks and referring to equities selling for under $5 apiece.

They're risky at the best of times but the lure can be overwhelming. Why? Simply because if you bought one for literally one cent and the price went up to two cents, you made 100 percent profit.

The bad news is that this rarely happens. And if it does, it was likely a scammer who paid the one cent and you, the investor, who paid two. That may be okay if you only bought a few, but gullible investors may buy many, many thousands after being tricked into thinking the price would continue to rise.

And when they try to bail out, to cut their losses, they usually can't find anyone who wants to buy them. So, they end up losing every single cent they plowed in.

The root of the trouble is that trading these cheap equities on what are known as over-the-counter (OTC) markets is not nearly as tightly controlled as regular stocks are on the likes of NASDAQ and the New York Stock exchange.

That leaves the way open for a variety of schemes, mostly lies or lack of information about the activities of the companies behind the stocks.

For example, Cynk Technology was a penny stock that soared over 25,000% in 2014 despite having no assets, revenues, or operations. The

lack of financial information on the company made it impossible for investors to know whether the price was justified. The stock eventually crashed back down over 99% from its peak.

Then, there was the famous case of Jordan Belfort, on whom the movie *Wolf of Wall Street* was based, which cost investors $194 million.

COMMON PENNY STOCK SCAMS The two most common scams relating to penny stocks are:

1. Lack of financial information, as in the Cynk Technology case we just mentioned. Unlike larger, publicly-traded companies, penny stock companies are not required to file detailed financial statements with securities regulators.

2. Price manipulation, more commonly known as pump and dump schemes. As we know, fake news is easier than ever to create and spread. Scammers repeatedly talk up the prospects for a company after buying its stocks from the bottom of the price barrel. Investors pile in as the price soars, then the crooks sell their holding.

Often, fraudsters use high-pressure sales tactics, calling potential victims and spinning a web of lies to try to talk them into buying. These characters operate from offices termed "boiler rooms," repeatedly calling their targets and implying they'd be stupid not to buy their stocks. They also spam their potential victims, sending out multiple emails every day. Or they may issue legitimate looking newsletters and posts on social media.

Large-scale scammers even employ and pay people to spread their lies.

HOW TO AVOID PENNY STOCK SCAMS It's probably fair to say that the lower the price of a penny stock, the greater the potential for a big fat profit - but more likely a big fat loss.

Don't let that happen to you by taking the following steps:

• Thoroughly research any company you're thinking of investing in. If big chunks of information are missing, that's a red flag. Check for proper licenses/registrations and look on consumer protection websites for alerts. Verify growth claims.

• Another red flag: promises of guaranteed high returns with little or no risk. All investments carry risk.

• Only invest in companies with audited financial statements from reputable firms. Be wary of one-person audit shops.

• Ignore paid stock ads and sponsored content. Focus investment decisions on company fundamentals rather than ads.

• Hang up on boiler room operators. You'll know them when you hear them, they make unsolicited calls to push specific stocks and often claim they have valuable inside information.

• Be skeptical of unconfirmed news reports of market-moving activities. Be especially wary of newly launched financial websites.

• Don't be influenced by "friends," message board acquaintances, and family members claiming they're in on a good penny stock deal. Still do your research.

• Don't provide any personal financial information to someone you don't know and don't fully trust.

• Beware of statements saying a stock has been checked and approved by the US Financial Industry Regulatory Authority (FINRA). They don't do that.

• Learn more by visiting their website, which also has a searchable database of legitimate stockbrokers.

Finally, and importantly, take advice from a trusted financial professional before making any investment decisions. Scambusters does not provide financial advice. The less you know about a stock, the higher the risk you'll lose money. Most likely, professional advisers will steer you away from penny stocks.

Modern-Day Bonnie and Clydes Are Trying to Steal Your Identity and Your Money

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

I've written in the past that if Bonnie and Clyde were alive today, they definitely wouldn't waste time robbing banks. If you're not familiar with the couple, they were ruthless gangsters who robbed banks, stores, and other places of business and killed lawmen, shopkeepers, and owners of cars they were stealing in at least four states.

They were, perhaps, best known for robbing more than a dozen banks– some of the same banks twice–over a four-year period, primarily in Missouri, Oklahoma, New Mexico, and Texas. Back in their heyday, they also targeted stores in small towns and funeral homes located in rural areas. Make no mistake about it. They were dangerous lawbreakers. That was how it was in the Depression-era 1930s.

Fast forward to today. Modern Bonnie and Clydes don't rob banks. It's too much work. Instead, they steal personal data from computers, phones, and tablets. They're called hackers. One of their main goals in this life is to steal, rob, and gain access to your hard-earned dollars. Their goal is to grab your money and run; your goal is to keep that from happening. So, whether you're tech-savvy or not, how in the world are you supposed to keep this from happening? There are simple steps you can take.

1. When someone calls you on the phone from an unknown number, DO NOT answer the phone; wait for a voicemail message. Microsoft, Apple, etc., will not call you. These thugs want to get their hands inside your computer or other device to steal your passwords or personal information. If you answer the phone, your number may be sold for more money.

2. Don't open emails from unknown sources. Don't open attachments from unknown senders. Don't respond to schemes alerting you that a friend has been hurt in London, Paris, Sydney, or some other location. Could you send money to help them? Your friend is in the hospital and needs your financial help. Their wallet's been stolen. Their purse has been snatched. And I'm the king of Spain.

Please don't fall for it. Don't click on links in an email from someone you don't usually hear from, urging you to view these great photos. There are no photos. Once you click on the link, malware infects your Windows PC and sends emails to everyone in your address book with the same message, urging them to click on a link to view photos. Phishing is the most successful cybercrime in America.

There were nearly 324,000 victims last year alone. (Phishing refers to an email that appears to be from a legitimate company or organization. There's often a threat – your account will be closed, or the sheriff will come to your house unless you respond. It's all bogus. But plenty of Americans fall for it.) Ever gotten an email that you owe $500 for Norton 360 (virus and malware protection software) that you never even purchased? You'd be surprised by how many folks respond to the email and even pay for the software they don't own. The thugs sending the email are not from Norton. Most junk email trying to get into your wallet originates in Russia, Germany, the U.S., and China.

3. Yes, it's a pain. But what tech folks call two-factor authentication can save your bacon. Turn it on. You'll be blocked if you decide to change your Gmail password, Facebook log-in, iCloud username or password, or some other account, you'll be blocked. You must enter a code you receive in a text message, an email, or even using the Gmail app on your smartphone to get permission to change your password. Yes, as I said, it's a pain. But it's preventing crooks from gaining access to your

account. So instead of just changing your passwords, you must first receive a code and enter it into a website or Gmail app. That proves you are who you say you are.

4. Run antivirus software.

For Windows PCs:
Safety Detectives: The Best Windows Antivirus
https://www.safetydetectives.com/

PC Mag: The Best Antivirus Software for 2023
https://www.pcmag.com/picks/the-best-antivirus-protection

For Macs:
Safety Detectives: Ten Best Antiviruses for Mac in 2023
https://www.safetydetectives.com/best-antivirus/mac/

Macworld: Best Mac Antivirus Software 2023
https://www.macworld.com/article/668850/best-mac-antivirus-software.html

For Linux:
Safety Detectives: Five Best Antiviruses for Linux in 2023
https://www.safetydetectives.com/best-antivirus/linux/

Ubuntu Pit: Top 15 Best Linux Antivirus Programs in 2023
https://www.ubuntupit.com/best-linux-antivirus-top-reviewed-compared/

5. Don't go on a fishing expedition on the Web. The World Wide Web is remarkable. It's the best library in the world. There are an estimated 1.6 to 1.9 BILLION websites currently accessible. Less than 400 million are currently active. More than 51% of all people in the world are online. Asia accounts for half the Internet traffic worldwide. Talk about diversity. Websites appear in more than 200 languages. But watch your step. Don't put your foot into horse dung. Make sure the website you visit starts with https. No, this is not always possible.

Some websites refuse to use the "https:" system. The "s" stands for secure. You're accessing a secure website. Don't randomly visit online gambling websites, sites with outdated addresses, websites with shortened addresses, sites ending in .onion, torrent websites (file sharing sites), porn sites and others.

Google constantly scans websites, looking for legitimate websites that have been compromised, unsafe sites, or other questionable pages. If you wonder whether a website is safe or not, visit the web address below and paste your website into Google's Safe Browsing website:
https://transparencyreport.google.com/safe-browsing/search

It will tell you whether it's safe to proceed or not.

5. Use a well-regarded virtual private network (VPN).

This tool sends your Internet signal through a tunnel so that hackers and other thieves cannot access the web pages you visit, your email, your passwords, or additional private information. Do your homework. Find a good VPN you can afford.

Steer away from free VPNs because many sell your data online, bombard you with ads, and some even use your computer's processing power.

For Windows PCs:
Privacy Savvy: Five Best VPNs for Privacy
https://privacysavvy.com/vpn/best/windows/

VPN Reports: Best of the Best VPNs
https://www.vpnreports.com/best-vpn/windows/

For Macs:
VPN Reports: Best VPNs for Mac in 2023
https://www.vpnreports.com/best-vpn/mac/

Safety Detectives: Ten Best VPNs For Mac
https://www.safetydetectives.com/best-vpns/mac/

For Linux PCs:
Safety Detectives: Five Best Linux VPNs
https://www.safetydetectives.com/blog/best-linux-vpns/

Pro Privacy: Ten Best VPNs for Linux
https://propriACvacy.com/vpn/comparison/best-linux-vpn

6. Use a password manager to track your passwords and log in to many websites requiring a username and password automatically. Experts say this is smarter than allowing your browser to remember your passwords. Unfortunately, web browsers are not really safe to keep that sort of information. As Tom's Guide writes, "That's because desktop web browsers, despite their best efforts, tend to do a lousy job of safeguarding your passwords, credit card numbers, and personal details, such as your name and address. As a result, web browsers are fairly easy to break into, and lots of malware, browser extensions, and even honest software can extract sensitive information from them."

Here are websites where you can read about the best password managers and pick one that works for you:

PC Mag: https://www.pcmag.com/picks/the-best-password-managers

Tom's Guide: https://www.tomsguide.com/us/best-password-managers,review-3785.html

How To Geek: https://www.howtogeek.com/780233/best-password-manager/

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

Kretchmar's Korner
A Mighty Mite External SSD

David Kretchmar, Hardware Technician
Sun City Summerlin Computer Club
https://www.scscc.club
dkretch ** gmail.com

A mystery package addressed to me appeared at our front door a few months ago. This is not an uncommon occurrence at our home; at least once a month, I forget I have ordered an item, and its arrival is a pleasant surprise. I have no idea what was in the package until I opened it, and fortunately, I still remember ordering the item.

Something different happened to me this time. I excitedly cut open the mystery padded envelope and found a wee SanDisk USB 3.2 Gen2 portable SSD. I was further delighted when I noticed the drive had a one Terabyte capacity.

It was 1/3 the size and a fraction of the weight of a mechanical external USB drive thanks to its M.2 SSD. Cool, I thought – this is something I can use. I guessed I might have ordered this late at night, maybe after a couple of sips of wine, and forgotten about it.

I soon realized my mystery package was the SanDisk SSD external drive I had volunteered to test for Newegg.com, an online reseller. YES! A free useful item is an even better deal than the drive costs at online sellers.

I plugged the SSD into my tower using the cable provided: USB-C (external drive end) to the USB Type-A (backward compatible with any standard USB port). It was instantly recognized.

Real-world speed

The drive is advertised as having a READ speed of up to M.2 SSD 520 Mb/second. I copied a 2 Gb file from my tower's internal M.2 SSD to the SanDisk external drive to test the real-world speed of the drive. It transferred data at about 120 MB per second, 3X faster than copying the same data to my older external mechanical Samsung external drive. This was a little slower than I anticipated since SSDs generally run from 4 to 10 times faster than a mechanical drive.

My tower's USB is mostly the older and slower 3.1 version, which I'm sure was the factor in the drive's lack of speed. I am disappointed with the data transfer speed because of the USB 3.1 and maybe the USB C to USB A cable. My tower, which is just a few months old, does have one Type-C USB port, but since I do not have a newer USB C to USB C cable, I could not test that transfer speed. This cable costs about $10 - $20 at Amazon or Newegg.

The Vault

The Samsung external SSD M.2 drive comes with an ingenious encryption scheme they call PrivateAccess with the encrypting software installed on the drive itself. This software will ONLY run off the external drive, further increasing the device's security. Transferring data to the external drive vault is a drag-and-drop procedure using the drive's built-in encryption software. There is no back door into the vault. As you would expect, if you forget your password, the data in the vault is gone forever. This drive will dedicate only the amount of space required for encrypted data, so the balance of storage space is available for nonencrypted storage.

The curse and blessing of backward compatibility

The drive would be much faster on newer computers if it included a USB C to USB C cable

and a USB C to USB A cable. Other external SSDs I have seen advertised come with the USB C to USB C cable. Obviously, the USB C - USB A cable is required for backward compatibility and is the most useful connection today. Still, any new computer you buy now should include a USB-C outlet. If you are offered a computer without a USB Type-C port, you know that system is likely old stock, and you should make your buying decision accordingly.

The USB cable furnished with this drive is only one foot long. This is adequate for functionality but too short for real-world usage. As a result, I prefer the external drive sitting on top of my tower rather than dangling at its side.

Conclusions

This is a remarkable amount of fast external storage for the money. A USB Type-C to USB Type-C is necessary if your computer has a USB Type-C outlet. At the risk of boring repetition, a computer user who does not back up important files will very possibly lose those files due to a hardware failure or mischief caused by a ransomware infection.

The Vault feature of this drive is an outstanding personal privacy consideration. It would also be impossible for any ransomware software to corrupt files stored in the Vault.

Interesting Internet Finds by Steve Costello

scostello ** sefcug.com

While going through more than 300 RSS feeds, I often encounter things that might interest other user group members.

The following are some items I found interesting in February.

Num Lock Will Ruin Your Day

https://cynmackley.com/2023/02/12/num-lock-will-ruin-your-day/

It is simple things like the Num Lock Key that can be frustrating. If you are like me, sometimes you try to use the number keypad and can't get numbers entered. Usually, I use the numbers on the upper row of the keyboard until I remember to check if the Num Lock Key is the problem.

Do You Really Need To Have Your VPN On All The Time?

https://www.howtogeek.com/866500/do-you-really-need-to-have-your-vpn-on-all-the-time/

This question comes up fairly often. This post gives pros and cons so you can decide about leaving the VPN on all the time. (Note: I keep the VPN on all the time on devices when I am traveling, while only when doing sensitive things like shopping or banking at home.)

Have You Made These Identity Theft Mistakes?

https://askbobrankin.com/have_you_made_these_identity_theft_mistakes.html

Bob Rankin goes over some common Identity Theft mistakes in this post. I read these posts to remind myself of best practices concerning Identity Theft prevention to ensure I am as safe as possible.

Which Should You Use On Your Smartphone?

https://www.online-tech-tips.com/smartphones/cellular-data-or-wi-fi-which-should-you-use-on-your-smartphone/

There is no best answer to this question, so I advise reading this article and making the best decision after having the facts. (Note: For me, it depends on the situation and the available speed.)

How Do I Keep My Email Address When I Change My ISP?

https://askleo.com/is_there_a_way_to_keep_my_email_address_when_i_change_my_isp/

Leo Notenboom explains ways to keep the same email address when changing ISPs. Unfortunately, there is not usually a way to do so if you use the ISP's issued email address, so things need to be set up beforehand.

Is Facial Recognition And Fingerprint ID Safe?

https://askleo.com/is-facial-recognition-and-fingerprint-id-safe/

Leo Notenboom gives his take on this question. If you watch a lot of TV and movies, you might think these options are easily bypassed. If that is the case, check out Leo's post.

How To Find The Right Kindle For Your Reading Needs

https://www.reviewgeek.com/144298/how-to-find-the-right-kindle-for-your-reading-needs/

Are you Thinking about buying a Kindle? If so, check out this Review Geek post outlining the different options and why each is best for different needs.