The Rochester Computer Society, Inc.

a computer/tech club open to everyone

MONITOR

Vol. 42, No.8 web: www.rcsi.org Rochester, NY August 2023

Member of apcug An International Association of Technology & Computer User Groups

Our Club

RCSI is a nonprofit 501(c)(3) group open for membership to anyone interested in computers and new technology. Established in 1981, our aim is to provide an exchange of information between users of digital devices. We are not in any way affiliated with any computer manufacturer or software company, and ***we do not sell your data or email address***.

Program Meetings

No admission fee for non-members*. *Everyone is welcome! Second Tuesday of every month, ***except July and August***, from 6:30pm-8:30pm.

Help's Half Hour (Q & A) 6:30pm – 7:00pm. *Members and Guests are welcome to attend and bring their computer related questions with them to get answered.* **Yes, you may bring the problem computer with you.**

7:00 – 7:15, Club Business

7:15 – 8:30+, Main Presentation Come and join in the fun and enjoy a snack! **You are welcome to bring a guest.**

Become a Member

The club would like to have you as a member, and your subscription will help to keep us going. Go to our website, www.rcsi.org, and download a printed form for use by the Post Office mail, **or** enter your info online and pay with a credit card or PayPal, **or** attend a meeting.

*** * July and August, summer hiatus – No Meetings * ***

In This Issue

Internet Security – Once over easy, with Hash

By Phil Sorrentino, Secretary, and APCUG Rep

The Internet is essential to so many things we do, like shopping, investing, and banking, that you may have wondered how secure the Internet is. And additionally, how secure is my private information during an Internet transaction? And now that we're thinking about it, how is the Internet made secure? If knowing a little about how the Internet is kept secure is interesting, read on; if not, jump to the next article.

The Internet provides essential communications between tens of millions of people and has become an essential tool for commerce; therefore, security has become a tremendously important issue. Internet security has many facets, ranging from keeping communications private to protecting passwords and guaranteeing

"Your Computer User Group of the Air", Saturdays from 12:00 pm to 2:00 pm, with Nick Francesco, Dave Enright, and Steve Rae. Broadcasting on JAZZ 90.1 FM (WGMC) from Rochester, NY. Call 966-JAZZ (585-966-5299) or 800-790-0415, **www.jazz901.org**

Sound Bytes is the longest running computer call-in show in the known universe.

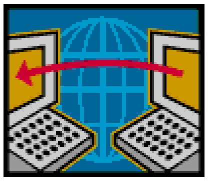
We have stopped printing the Monitor newsletter. Digital copies can be emailed or obtained from **www.rcsi.org** or my **Pcloud** storage at **https://tinyurl.com/tonydel-rcsi** (***this link works in PDF version only***). Also includes presentation slides, **past newsletters dating back to 1996** and articles too large for this newsletter.

Some Past Presentations:

Autonomous Cars and Robots
Open Source and Free Software
Protecting Your Identity
Tablets, the Programs and Uses
Personal Finance Software
Amazing Browser Tips
Linux is Like Cars
Drones and Their Many Uses
Gifts and Gadgets for the Holidays
Cut the Cord, Streaming Services
3D Printing, ENABLE project
Features, Mac OS X & Windows
The New Space Race, 2021
Tech of South America
Internet Security and Privacy
AI and Digital Assistants
Emerging Technologies
My Favorite Android Apps

secure commerce transactions and payments.

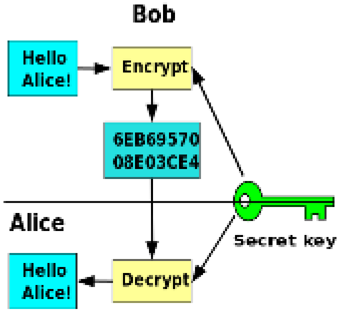
Computers are an integral part of the Internet, and when it comes to computers, security is a concern on many different levels. There is physical security that keeps your computer hardware from being stolen. There is software security that keeps people out of our private files. There is "malware" security that keeps your computer software from being infected with viruses, spyware, worms, and the like. And finally, there is "network" security that keeps private data protected as it goes from one computer (or client) to another computer (or server) on the Internet. These security concerns are important, but the subject here is network security. Network Security is implemented by applying cryptography to messages sent on the Internet.



Remember the "s" in "https://" and the little lock icon on the browser when you go to a "secure" website? Well, cryptography is behind all that security. Cryptography is used to secure telephone, Internet, and email communications (as well as to protect software and other digital property). Cryptography is nearly as old as written language itself. It was invented to address the age-old question: How can I communicate with my friend so that no one else listening will know what was shared? Cryptography becomes necessary when communicating private information over a public or "un-trusted" medium, such as the Internet. Typically, you can be sure that the message you send over the Internet will get to the destination you expect, but you cannot guarantee that intermediaries (computers along the way) will not be able to see and/or read your message if it is not protected. With a collection of not-so-expensive equipment and a good deal of knowledge, a message on the Internet can be intercepted (sniffed), and if it is "plain text," it can be read. For mundane email messages, this is not much of a concern; for messages that contain private information, such as personal information such as bank account or social security numbers, this could be an invitation for Identity Theft.

To get a bit technical here (here's the once over, with hash), we need to address the following four security concerns to guarantee messages are secure on the Internet. 1) *Privacy:* Ensuring that no one can read the message except the intended receiver. 2) *Integrity:* Assuring the receiving party that the received message has not been altered from the original. 3) *Authentication:* The process of proving one's identity. 4) *Non-repudiation:* A mechanism to prove that the expected sender sent this message.

There are, in general, three types of cryptographic schemes typically used to accomplish these goals: Secret-key cryptography, Public-key cryptography, and Hash functions, each of which can be researched in great detail by doing a Google search on the subject and settling in for some rigorous mathematics and explanations.



Secret-key Cryptography

However, here is a brief summary.

APCUG, An International Association of Technology and Computer User Groups

https://apcug2.org/

Saturday Safaris

Exploring Technology in Depth
Saturdays:
12 pm – 2 pm EST

https://apcug2.org/saturday-safaris/

Tech for Seniors

https://www.techforsenior.com

hosted by Ron Brown
and Hewie Poplock
Every Monday from 9-10 AM PT,
(12-1 PM ET)
Broadcast with Zoom
The meeting ID is **526-610-331** (there is no password) and you'll be placed in a waiting room and then admitted.

# # #

APCUG Website Help

Windows & Android Tips:

By Judy Taylour

https://apcug2.org/jerestips/

Apple Tech Tips:

https://apcug2.org/50-best-mac-tips-tricks-timesavers/

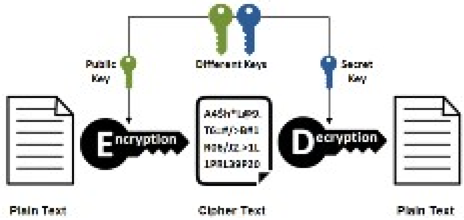
Penguin Platform (Linux):

https://apcug2.org/penguin-platform/

Chromebook Tips And Tricks:

https://apcug2.org/chromebook-tips-and-tricks/

Secret-key cryptography, sometimes called symmetric cryptography because the sender and receiver use the same key, is the more traditional form of cryptography where the (same) key is used to encrypt and decrypt a message.



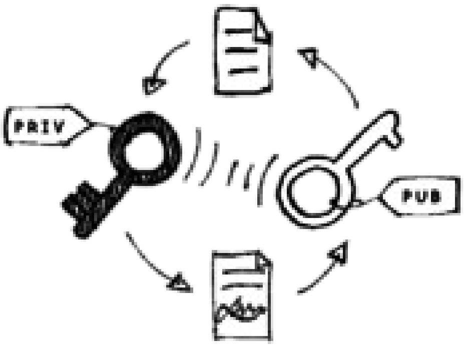
Public-key cryptography

On the other hand, public-key cryptography uses algorithms to create two asymmetric keys, a public, and a private key. (Unlike secret-key cryptography, it does not require a secure initial exchange of secret keys to both sender and receiver.) The asymmetric keys are a mathematically related key pair: a secret private key and a published public key. These keys protect a message by creating an encrypted message using the public key, which can be decrypted only by using the private key, providing "privacy," the first security concern.

Hash functions are mathematical transformations used to irreversibly encrypt data, meaning that the Hash results cannot be reversed to recover the original message. Hash functions are well-suited for ensuring data "integrity," the second security concern, because any change made to the contents of a message will result in the receiver calculating a different hash value than the one sent by the sender. Since it is doubtful that two different messages will yield the same hash value, data *integrity* is ensured to a high degree of confidence.

"Authentication," the third security concern, is accomplished in nearly all modern computer systems using passwords that authenticate users attempting to access computer resources. For security reasons, passwords are not typically kept on a server in plaintext. Hash functions are commonly used to convert passwords to an irreversible data pattern. When you type in your password, a Hash function converts it to a data pattern and compares it to the data pattern previously stored for your password. Your password is never stored on your machine or your server's machine; only the hash function results are stored. There is no way of going backward from the Hash function data pattern to the password (remember, the Hash function is irreversible). *So now you know how the passwords are protected and why when you forget a password, the server can't tell you what it was; they can only reset it to a new password.*

Digital Signature



The fourth security concern, "non-repudiation, " ensures the message was sent from the expected sender. This is accomplished by a digital signature which ensures that the sender cannot deny the authenticity of its signature or later deny sending the message. A digital signature is created using the private key of an asymmetric

RCSI Board Members

President:
Mark S. Lawson . . 544-5377
mslawson51@peoplepc.com

Treasurer:
Jerry Seward . . . .
jerry@jerryseward.com

Members-At-Large:

Bob Avery 385-4491
Webmaster
webmaster@rcsi.org, 9/24

Jan Rothfuss 347-6020
Membership & Help's Half Hour
jan_rothfuss@hotmail.com, 9/23

Tony Dellelo 734-6149
Programs & Monitor editor
tonydel@techie.com, 9/25

Got Questions?:

Windows: . . . . . Arpad Kovacs
podcomputer@gmail.com
Linux & some Mac: . . . .
Carl Schmidtmann
unixgeek@faultline.com

Planning Meeting

Held on 1st Tuesday of each month at 7 pm, * * ONLINE * *. We will be using Jitsi Meet. ANY CLUB MEMBER MAY ATTEND.

Monitor Newsletter

The Monitor is published monthly by members of RCSI. Articles by our members may be reprinted by other user groups or nonprofits, without special permission. A courtesy copy may be emailed to the author or Monitor editor. Limited copies (probably in black and white) will be printed and available at our meetings.

Club Mailing Address

Rochester Computer Society, Inc
PO Box 18516
Rochester, NY 14618

key pair. The signature can be verified by the corresponding public key of the asymmetric key pair, thus proving that the document was "electronically signed" by the private key owner, thus guaranteeing the message's source. So with all of these four concerns met my take, it looks like the Internet is pretty secure.

Reprinted from Sun City Center Computer Club, FL, https://www.scccomputerclub.org/ , philsorr@yahoo.com.

So I Just Googled Myself...

By Bob Rankin
a Translator for the Technology Impaired
offering Free Tech Support

Have you ever used Google or Bing to search your own name, address or phone number? In an age of powerful search engines, social media, artificial intelligence, and changing attitudes about privacy, you might be shocked to see what a casual searcher can learn about you. If you're okay with that level of transparency, then fine. If not, read on for some tips on what you can do about it....

Removing Personal Information From Google

If you search for yourself on Google, you may be surprised by the results. Things you posted on social media without thinking twice; blog posts or news reports that mention you in an unflattering or libelous manner; an embarrassing photo; even your home address or phone number... all of these are examples things you'd probably wish you could remove from Google.

Recently I saw an example of a well-meaning person who saw a neighbor dumping trash. He posted a photo on social media of the man's truck, along with his name, license plate number and home address. Thankfully, several people warned that this could put both the poster and the bad neighbor in danger, and the personal information was removed. But that doesn't always happen.

It's not easy to remove information from Google (or any other search engine), once it gets found and indexed. Google's business is indexing Internet content so that people can search it. Since Google does not control what is published on the Web, you have to start with the person who did publish what you want removed.

If you published something you regret, delete it. If the offending info is on someone else's site, ask the poster, publisher or site administrator to delete it. Then, when Google's Web-crawler indexes the site again, it will delete Google's cached copy of the now-missing content, and it will no longer appear in search results. But that may take a while, depending on how often Google indexes that particular website. To speed up the process, you can file a remove outdated content request with Google. But first, you must be sure that the content you want removed from Google search results has been removed from the Web.

If you can't get the content owner to remove the offending content, there are some special cases in which Google will intervene. On the Remove your personal information from Google help page, Google

Tidbits of probably useless information

I did not verify any of these.

Did you know:

New York's Central Park was opened in 1876.

Hawaii officially became a part of the US in 1900.

Plastic bottles were first used for soft drinks in 1970.

The tea bag was invented in 1908.

The doorbell was invented in 1831.

The electric toothbrush was invented in 1939.

The naming of tropical storms and hurricanes officially began in 1953.

Instant coffee was invented in 1901.

In 1878, the first telephone book made contained only 50 names.

The first Burger King was opened in Florida Miami in 1954.

Halley's comet passes the Earth every 76 years (the next time it will return will be 2062).

The Olympic flag was designed in 1913.

The first dictionary of the English language, sometimes published as Johnson's Dictionary, was published on 15 April, 1755 and written by Samuel Johnson.

The $ sign was introduced in 1788.

lists things such as "non-consensual explicit or intimate personal images," "financial, medical and national ID information," and cases where “doxxing” (exposing information with an intent to harm) is involved. Google won't help you remove the offending information from the page where it exists but they will expunge it from their search engine database so it is not easily found.

Dealing with other people who control content you don't want online requires diplomacy, lawyers, or both. It's always best to start with a polite approach: "Hi, sorry to bother you but I have a problem with this content... would you please delete it?" You'd be surprised by how cooperative neutral strangers can be.

More Removal Tools

Google has another tool for requesting removal of content from sites it owns, including Google Search, YouTube, Google Maps, and others. Requests for removal through this tool must rely on legal issues, i.e., violation of copyright, privacy, or child p**nography laws.

My article Breaking Up With the Internet (is hard to do) discusses your options for removing personal data from social media, online phone directories and other places.

The best way to keep unflattering information about yourself out of Google is to keep it off the public Internet. That means tightening up the privacy controls of all your online hangouts: Facebook, Twitter, Instagram, TikTok, Linkedin, etc., etc. Also, watch what you say in web forums, which are also indexed by Google unless the administrator has added a "do not index" tag to his forum. Be careful what you post on your own website, Facebook page, or blog.

You can use Google Alerts to monitor what's being said about you or your business online. There are also very expensive services like Reputation Defender that will fight on your behalf to remove offensive or incorrect content.

Of course, if it's someone who has a grudge against you, you may need to decide whether getting the offending content removed is worth the cost of these services, or even legal fees. But there's always the bluff. Sometimes sending a threatening letter spiced with a bit of legalese will do the trick.

If you are content creator, such as a musician, writer or digital artist, you may find that someone else has used your music, article or artwork without permission. This has become a bigger problem with the recent advent of "generative AI" tools that create content by imitating or taking portions of copyrighted materials, combining it with other content, and passing it off as something new and original. Some of these tools can write articles or term papers, create works of art, or write music. One recent example is the song "Heart on My Sleeve" which was created by AI software. It appears to be a collaboration between musicians Drake and The Weeknd, but it's an AI fabrication. In such cases, you can initiate a DMCA Takedown request to have the offending content removed.

But Wait, There's More...

Of course, Google is not the only search engine in town. Although it has a smaller reach, you should search for yourself on Microsoft's Bing search engine as well. If you find something that's troubling, use the Report a Concern to Bing page. You can report broken links or

Windows & Android Tips

Judy Taylour

HOW TO STOP APPS FROM USING MOBILE DATA ON ANDROID – Mobile data is a precious resource. It's one part of many phone contracts that's still subject to limitations and can get pretty costly if it's not monitored and kept in check. A vital way of controlling mobile data is to get an idea of how much data each app uses, then find ways to curtail their data use. There are various ways to do this, as you'll see in this guide, that shows how you how to stop apps from using your mobile data on Android. Read more at https://tinyurl.com/n9xx36tp

HOW TO RESET ALL AUDIO SETTINGS IN WINDOWS – The audio settings in Windows automatically adjust with your app requirements and system updates. If you're not getting the desired sound quality, or when there is no sound at all, you can reset your current audio settings to resolve the problem. Find out all the different ways to reset your diverse audio settings in Windows here. https://tinyurl.com/mr26nx6m

HOW TO DISABLE STARTUP APPS ON WINDOWS 11 – Here are four ways to prevent apps from running automatically on startup on Windows 11. How to disable startup apps on Windows 11 – Pureinfotech

outdated pages, unauthorized use of intellectual property, child p**nography, offensive material, exposure of private information or images, or malicious pages.

In addition to searching for your personal info on Google or Bing, there's one more place you might want to look. The Internet Archive is a collection of over 600 billion Web pages, captured over the past 25 years. You can use it to see what a Web page looked like in the past. The point here is that something pertaining to you might have been removed from a given website years ago, but still lives on in this archive. See how to remove something from the Internet Archive.

From the website of
https://askbobrankin.com/so_i_just_googled_myself.html.

FREE!
e-RECYCLING EVENT
08 · 19 · 23
8:30am - 2:00pm
Xerox Corporation
Panama Rd. (Bldg. 147)
Webster, NY 14580
*Ticket is REQUIRED for entry

Sunnking, https://www.sunnking.com/events/webster-08-19-23

* * Registration is Required * *

* * * * * SOFTWARE and HARDWARE * * * * *

So Long LastPass - Hello NordPass

By Bob Woods, Co-Webmaster
Under the Computer Hood User Group

For several years, I used LastPass as my password manager. The free version allowed my PC and Android devices to use the same encrypted vault. In 2021 there was a change. Only paid accounts could have PC and Android using a shared vault. The free version no longer did. This required one vault for the PC and another for Android devices.

Because of this, a few UCHUG members changed to the free open-source BitWarden for their multi-platform password management, which uses the same vault across all platforms. I tried BitWarden and did not care for the interface. LastPass either auto-filled or only required a single mouse click to fill in the login information. BitWarden usually needed two or three clicks. But it may have just been me or an incorrect setting. At any rate, I didn't want to change. So, I created an account for my Android devices and exported the PC vault. I also had different master passwords for each version. It required me to sync the two different vaults manually, but I was willing to accept this inconvenience for free.

Then, last year one of the LastPass backup servers was breached, and some user information was stolen. LastPass Corporate informed their users and assured everyone that sensitive data (usernames,

Scams

https://www.usatoday.com/story/money/taxes/2023/07/05/irs-tax-refund-scam-warning/70383512007/

You may soon get an IRS letter promising unclaimed tax refunds. It's a scam.

This summer, don't overreact if a cardboard envelope shows up from a delivery service and the letter inside implies the IRS is reaching out to help you snag a tax refund. The letter uses an IRS masthead but don't be fooled: The agency is not sending out individual notices alerting taxpayers to an “unclaimed refund.”

Like many scams, this one appears pegged to legitimate news. The IRS has said taxpayers must file a 2019 tax return by July 17, if they've not done so already, to get their hands on an unclaimed refund. We are talking about some cool cash, too, maybe $800 or $900 in unclaimed refunds for some people. But again, no one is sending out letters demanding key information from you.

Don't send scammers a picture of your driver's license.

The new scam letter goes so far as to request that you send detailed pictures of your driver's license. Identity thieves use such details to try to open new credit cards in your name or fill out a fake tax return to steal a refund. Your driver's license contains information, such as your birthdate and home address.

passwords, credit card information, etc.) was encrypted and safe. This prompted me to re-evaluate password managers. After online reviews of password managers, I decided to give NordPass a try.

My reasons to try were:
1. They are highly rated in many password manager reviews.

2. They recently had and passed an independent security audit.

3. They have never been breached. LastPass has. In 2022, LastPass suffered significant security incidents. User data, billing information, and vaults (with some fields encrypted and others not) were breached, leading many security professionals to call for users to change all their passwords and switch to other password managers.

4. NordPass is based in Panama, which has no mandatory data retention laws and does not participate in the Five Eyes or Fourteen Eyes alliances. This means that the company isn't required by law to keep logs or share them with governments.

5. Your NordPass vault is encrypted with the XChaCha20 encryption algorithm. XChaCha20 is more modern and faster than AES 256-bit. For an explanation, go to XChaCha20 Encryption vs. AES-256:What's the Difference? | NordPass

6. They have a family plan that allows up to 6 independent accounts. You can also share your vault with a family member. For example, this will allow me and my wife to have a synced vault.

7. The software is multi-platform. Even the free version can be used on all my devices using the same vault. After loading the NordPass free version, it asked for some account setup info: username, password, and Master Password. You should make it different from your account password, as it will be the magic key to decrypting your vault. I used a phrase that would be easy to remember containing the normal mix of upper/lower case, symbols, and numbers. You will use this key on all your devices to decrypt the vault. DO NOT FORGET WHAT THE MASTER PASSWORD IS! You are the only one that knows what it is. NordPass support cannot help if you forget it. There is one thing that may help. When you create your master password, you will receive a 24-character alphanumeric recovery code. The recovery code will allow you to create a new master password. You should lock this code away in a safe place. During the Windows setup process, you will be prompted to install the browser extension for whatever browsers you have installed. Setup will help you get and install the extension as needed.

After the setup, I exported my password vault from LastPass and imported it into NordPass. Everything went in without a hitch. Next, I went into settings, turned off launching at startup, and set the auto-lock to four hours. That way NordPass will only launch if I needed it, as there are times I am not doing anything that would require a login.

Virtual Tours

The Vatican, Italy
Vatican City is the headquarters of the Roman Catholic Church and the seat of government. More than 5 million people come to Rome every year to feast their eyes on the prized paintings and sculptures of the Vatican and to experience the most religious and cultural site in the world. Check out www.youvisit.com/tour/vatican for the tour.

Reichstag Parliamentary Building, Berlin
The Reichstag is one of the most important buildings in Berlin today. Built to symbolise the reunification of Germany. It's one of the few parliamentary buildings in the world that allows the public to watch over government processions. Similar to the White House, it's free to visit but you have to book months in advance for a tour. Wait no more as this virtual tour of the Reichstag is pretty awesome.

Palace of Versailles, France
Did you know that the Palace of Versailles was a mere hunting lodge before it became the world's largest palace? It's one of the most important landmarks in French history because it symbolises the power and downfall of the French monarchy.

Explore its opulent, regal interior and admire its intricate details on this Palace of Versailles virtual tour.

Also, the four-hour timeout will keep NordPass from requiring a re-login unless I go over four hours or shut down.

I set the password generator for upper/lower case numbers and symbols. I also set it for 16 characters. Next was to install NordPass on my Android phone and tablet (both Samsung). The app is available in the play store and can be installed easily. The app also installs into your browsers, so there isn't a separate extension installation that I had on the Windows PC. You can launch the NordPass app on Android devices, but I find that just going to a site requiring a login will bring up NordPass as a selection for a spelling selection atop the onscreen keyboard. You select NordPass, which will open the window to input the Master Password. Then you can populate the login info for the site you are accessing.

On my phone, I left auto lock at five minutes as a trial time. If I go to another location requiring login info within five minutes, I do not need to input the Master Password again. Better to be more careful with the phone auto lock settings than the PC on my desk at home. After using NordPass for a few days, I liked how it worked. Since I wanted to have NordPass available to my wife and share the vault with her, I opted for the family plan. The cost for the two-year plan is $68.00. But with six separate accounts available, I can offer an account to both my wife and my son. Also, the paid plan offers a weak and reused password check and a data breach scanner to scan the web for data breaches. I spent some time doing some cleanup. When checking for weak passwords, a change password button will launch a browser to the site needing a password change. Unless you want to create a new password, NordPass will manually offer to autofill the new password per your password settings and save it to the vault.

I am happy and comfortable with NordPass. However, if you have never used a password manager or are looking for an alternative to one you may be using, go to https://nordpass.com/ and check the personal free version.

Reprinted from https://www.uchug.org/ ,
Webmasters@uchug.org .

The **APCUG Wednesday Workshops** (WW) presentations have received high praise from attendees and presenters. Both have enjoyed the Zoom meeting format instead of the VTC Webinar presentations. With the WWs, cameras are an option for everyone. The presenters like seeing the many people attending the workshop and having more time to answer Chatbox questions since more questions can be answered live without a time limit. WWs have either an in-depth two-hour presentation by a single presenter, a panel of presenters, or two presentations with open mic Q&A following the presentations. Everyone likes the biggest feature where the mics are open for general questions, comments, and sometimes socializing. We have people that attend just about every workshop, even from Australia. We've become a Wednesday family. **9 am PT, 10 am MT, 11 am CT, 12 noon ET** Typically, the 2nd and 4th Wednesdays are for Windows or ??? workshops, and the Linux workshop is the 3rd Wednesday of the month.

Interesting Internet Finds

by Steve Costello
scostello@sefcug.com

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.)

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.

A Mighty Mite External SSD

David Kretchmar, Hardware Technician
Sun City Summerlin Computer Club

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

* * Jokes & Quotes Stolen from Everywhere * *

Last month I typed in the words horse jokes. This time I typed the words ‘cat jokes’.

What sports do cats play? **Hairball**!

What types of cats purr the best? **Purrr-sians**!

Where do cats always fly out of when they travel? **Kitty Hawk**!

How does a cat sing scales? **Do-re-mew**!

What state has a lot of cats and dogs? **Petsylvania**!

In what kind of weather is a vet the busiest? When it's **raining cats and dogs**!

How does a cat decide what it wants from the store? It flips through the **cat-alog**!

Why can't cats play poker in the jungle? Too many **cheetahs**!

What do you call a cat who loves to bowl? An **alley cat**!

Where does a cat go when it loses its tail? The **re-tail** store!

What's a cat's favorite dessert? Chocolate **mouse**!

What's a cat's favorite color? **Purr-ple**!

What's a cat's favorite magazine? *Good **Mousekeeping***!

What do cats like to eat on a hot day? A **mice-cream cone**!

Why do cats always get their way? They are very **purr-suasive**!

What do cats eat for breakfast? **Mice Krispies**!

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.

From the https://www.scscc.club, dkretch@gmail.com.

* * * * * BITS and PIECES in the NEWS * * * * *

Editor’s Note: To continue reading the following articles, you may copy the long URL at the end of the article and enter it into a web browser **or** click on the URL in the PDF or web versions of this newsletter.

It's Not just France: Your Phone is a Surveillance Device

By Loz Blain, July 06, 2023

There's a lot of news going around today about the French Government's new policy to allow police to remotely take over a suspect's devices, with access to cameras, microphones and GPS data. But if you think that's uncommon, you'd be very mistaken. Governments and police agencies the world over have access to your smartphone as a surveillance device.

Promising it would only be used in "dozens of cases per year," French Justice Minister Éric Dupond-Moretti yesterday welcomed new legislation allowing such spying for up to six months, where approved by a judge, in cases where possible sentences are at least

Odds and Ends

Heart Valves Made in Minutes

July 6th, 2023 Conn Hastings, Cardiac Surgery

Researchers at Harvard University have developed a technique that lets them create biomaterial heart valves in a matter of minutes. The approach, called 'Focused Rotary Jet Spinning', has been described by the researchers as 'a cotton-candy machine with a hair dryer behind it.' Essentially, the technique involves using jets of air to direct polymer strands onto a heart valve shaped frame. This results in a porous scaffold that allows cardiac cells to enter and grow. The formed constructs also have the mechanical properties to function as a one-way valve within the heart. The scaffolds contain nanoscale cues that encourage cells to enter and proliferate, with the ultimate goal that the biomaterial scaffold will be progressively replaced by cells, eventually resulting in a regenerated heart valve.

Continue this fascinating development at https://www.medgadget.com/2023/07/heart-valves-made-in-minutes.html.

five years. "We're far away from the totalitarianism of *1984*," he added. "People's lives will be saved."

Clearly, it feels like the most obscene invasion of privacy that some police or government operative could hack into your phone and casually observe a livestream of your life. And clearly, it opens the door to casual abuses of civil liberties by people in positions of power, as well as more focused abuses of that power by bad-faith actors.

But the horse has bolted on this one in most places, folks. All the way back in 2006, before the first iPhone came out, the US FBI was remotely activating cell phone microphones – even with the phones switched off – and eavesdropping on suspects, perfectly legally. Back then, you could still pull the batteries out of many phones. Now, not so much.

A *Comparitech report in 2022* found that of 50 countries studied, *every* police force had some level of access to smartphones and their data.

Read more at https://newatlas.com/mobile-technology/smartphone-surveillance-camera-microphone/.

Making Rubbery Materials That Can Take a Beating Without Losing Their Bounce

RA Smith science writer, June 22, 2023
Véronique Koch senior science producer

Research could pave the way to flexible-yet-durable materials that help cut down on microplastic pollution from things like the wear and tear of car tires.

DURHAM, N.C. -- When it comes to the environmental impacts of cars, much ink has been spilled on tailpipe emissions. But there's another environmental threat from cars you might not think about: microplastic pollution.

Car tires are made of rubber but also plastic polymers and other materials. Tiny bits of these materials, most a fraction the size of a grain of sand, slough off whenever tires rub against the road. Some are washed into soils and waterways; others enter the air, where their long-term effects on the health of humans and other living things are unknown.

Duke chemistry professor Stephen Craig thinks we can do better. Craig is part of a team from Duke and MIT that has been studying the molecular reactions within a class of flexible polymer-based materials called elastomers. Think rubber tires, the nitrile in medical gloves, or the silicone in soft contact lenses. What makes these materials amazing is the fact that they can be stretched and squished repeatedly and still return to their original shape.

Continue at https://today.duke.edu/2023/06/springy-yet-tough.

Space Borne Solar Prototype Successfully Beams First Wirelessly Transmitted Power to Earth

J.BUENCONSEJO, Jul 07, 2023

Beaming down solar power from space could theoretically provide an endless energy source with limitations at its efficiency and reliability. For the first time ever, a prototype in space has been able to beam down wireless power to Earth.

Space Solar Power Prototype

According to Power Mag, the recent achievement was a significant step forward in space-based solar power. The prototype came from the California Institute of Technology (Caltech) and seeks to transmit power from space to Earth wirelessly.

This achievement gets humanity a step further into potentially harvesting solar power in space and sending it to Earth. To send the space-gathered energy, the prototype must beam it down via microwave radiation.

Reported by https://www.sciencetimes.com/articles/44745/20230707/space-borne-solar-prototype-successfully-beams-first-wirelessly-transmitted-power-to-earth.htm.

Indian Space Research Organization (ISRO) Set To Launch Lunar Lander Chandrayaan-3

Caleb White, July 7, 2023

India is pushing its third lunar exploration mission Chandrayaan-3 next week. The Indian Space Research Organization (**ISRO**) aims to land a rover on the moon.

ISRO to Launch Chandrayaan-3

The next Chandrayaan mission, which means "moon vehicle" in Sanskrit, will be launched by the Indian Space Research Organization (ISRO) at 2:35 p.m. IST (2:05 a.m. PDT) from the Satish Dhawan Space Centre on the island of Sriharikota in South India on July 14, according to a **tweet** from the space agency on Thursday. The LVM3 M4 mission has the codename LVM3 M4, which will have a lander, propulsion module, and rover to softly and safely touch down on the lunar surface, roving, and perform on-site scientific investigations.

Read the rest at https://www.sciencetimes.com/articles/44744/20230707/indian-space-research-organization-isro-set-launch-lunar-lander-chandrayaan.htm.

Club and Regional News

****

Check out the new website of the Cape Computer & Technology Club, https://sites.google.com/view/capecomputerclub/home**.** Our club is mentioned and we share newsletters with them. I have printed some of their articles.

****

Got Questions?

Send an email to either person below and they will get back to you. The questions can be related to the OS (Operating System) or hardware related issues. Please give them time for a response, as they do this service on a volunteer basis. Thank you.

Windows OS: . . . . . Arpad Kovacs, podcomputer@gmail.com

Linux & some Mac: Carl Schmidtmann, unixgeek@faultline.com

Our Meeting Place

St John's Meadows at Johnsarbor Drive, is on the left, past Clinton Avenue, when going West on Elmwood Avenue. The opening in the white fence is Johnsarbor Drive. At the 'T', turn right. The meeting is in the SECOND building on the left – **Chestnut Court**.

Our meeting place can change. Please check our website before each meeting. **www.rcsi.org**