

SCA Computer Club notes

Classes for the Month of Jun



Watch out for the
kids...school is out for the
summer!

To enroll, log into the website at <https://computer.scaclub.org/>. Go to **Calendars** and select **Classes/Events**. Click on the class you want to take and under "Action", click on "**Enroll**". (Be sure to check the date as there may be multiple offerings of the class). If you need to cancel your enrollment, please log back in, select the class again and click on "**Drop**". All classes are **FREE** to Computer Club members in good standing and are geared for *beginners* unless otherwise indicated. A member can take any class as many times as desired. **IMPORTANT:** You must have your **SCA Resident ID** with you to check-in at the **Monitor desk** AND **AGAIN** in the **front of the Classroom** to ensure you are enrolled on the day of the class. Check-in will begin 20 minutes before the scheduled class time. If you are late, you may be bumped from the class by someone on the waiting list.

How to Stream to Your TV: This class will help you select a streaming device like a smart tv or an external streaming device like a Roku or Firestick. It will show you step by step how to setup and use one of these devices. Lastly, there will be a description of available streaming services and how to make your selection.

Pages for Mac- Part 1: This class will provide the basics of using Pages to create documents and perform simple task like setting margins and idents, typing, dictating, cut, copy and paste functions, font selection, size and color. We will also cover creation of bulleted and numbered lists and paragraph formatting basics.

Buying a Computer: Are you considering buying a new computer for yourself or as a gift? Should you buy a desktop, a laptop or a tablet? What are the differences between them? Should you buy a Mac, PC or even a Chromebook? Will it be used for email, to watch movies, organize your photos, write a book, etc.? Have your questions answered before you shop and buy.

Pages for Mac- Part 2: This class will get into the insertion of text and graphic elements and the options for integration into the document flow. The concept of flowing text between distinct portions of the document will be presented in detail. **A basic understanding of the operation of Pages is prerequisite for this class.**

If you've recently joined our Club we highly encourage you to attend the **New Member Orientation** class to familiarize yourself with our Club's activities. Learn how to sign up for classes, schedule a house call, volunteer to be a monitor and more.

Introduction to Windows 11: New to Windows 11 or wondering if you should upgrade? Learn some basics before you do, or become more familiar with Microsoft's newest operating system (OS).

Photoshop Elements: Do you take pictures with either a digital camera or a smart phone? Learn how to organize and edit your pictures. This hands-on class for both Mac and Windows users give a basic introduction to Adobe Photoshop Elements.

Special Topics

Special Topics classes meet on a weekly or monthly basis. We invite ANY Computer Club member who is interested in learning more about a specific product/application or a specific topic to join in the discussions. All groups meet in the computer classroom. Participants ask questions and discuss various topics at each session.

If you are an Apple user, attend *Apple Talk* that meets **monthly** to investigate Apple products. Did you recently buy an iPhone, Mac, an iPad, MacBook Air, or other Apple product? Do you have questions regarding specific Apple products or applications? Sit in on this month's meeting on **Saturday, Jun 10** from **10 AM - noon** and see if this is the group you have been looking to join.

Computer Talk meets **weekly from 9-10 AM** every **Thursday** and is designed as a "question and answer" session. Can't figure out how to do something? Do you have a question regarding a specific product or application? This group is for computer related discussions and not limited to any specific product. Bring your Android, Apple, Chromebook, Windows, etc. questions and we'll try to answer them. Please don't ask how to replace your garbage disposal or fix your washing machine. New members are always welcome.

Photoshop Elements Advanced Topics: Enhance your ability to work with digital photos. Monthly topics build upon skills learned in the Photoshop Elements class. These have included enhancing photos by adjusting coloring and lighting, removing imperfections and unwanted objects, clearing haze, and combining photos. Some are simple fixes and others make use of the power of adjustment layers. Topics are repeated periodically, depending upon interest. Meets on **Friday, Jun30** from **9:30am -11:30am**. **Prerequisites**: The basic *Photoshop Elements class* **or** some experience using either *Photoshop Elements* or *Photoshop*.

If you like reading the Newsletter each month, let us know. You can login to your account at: <https://computer.scaclub.org/> then select **Contact Us** from the menu.

Select **Newsletter** from the contact options, then **Next**. Fill out the information and **Send message**. Is there a particular topic you are interested in? Want more articles on Android devices, networking, staying safe while on the Internet or ??? While we try to keep articles relevant, we could always use an idea or two, so don't be shy.

Contact Us and let us know if you like the Newsletter, or ways to improve it. Or, if you don't even read it and couldn't care less if one is written or not, let us know that too! It could save us a whole lot of time and effort (smile) and we could go out for dinner (yum, dim sum), enjoy a hike on the Shadow Canyon Trailhead, take the grandkids to the local museums, gamble that extra money from our Social Security check on our favorite slots down on the Strip, etc. (Ha Ha). **No, really, we'd love hearing from you, so don't be shy! If you like reading the Newsletter each month, let us know.** You can login to your account at: <https://computer.scaclub.org/> then select **Contact Us** from the menu.

Virtual “Kidnappers” Using Artificial Intelligence (AI) to Extract Enormous Ransoms

By Linda Norton

According to the Federal Trade Commission, in 2022, Americans lost approximately \$2.6 billion to imposters who claim that a family member has been kidnapped and is being held for ransom.

According to the FBI, the average family loses \$11,000 in each kidnapping scam.

The premise is simple; snag just a few seconds of an audio recording of a person’s voice, but tweak it to add a considerable touch of “terrified” (such as a blood-curdling scream happening in the background), then start contacting that person’s family and friends. Since so many of us post regularly on social media, finding the next target is surprisingly easy for these predators, most of whom operate out of Mexico and are therefore beyond the reach and jurisdiction of US authorities.

Something as simple as answering your telephone before you know who you’re speaking with can kick-start this whole process. “Hello... Hello... Yes... Who’s calling?” So can posting one’s future plans on Facebook or other social media platforms, since scammers know exactly when that person will be out of the mix and therefore unable to respond to their loved ones’ panicked phone calls.

The Most Important Security Step to Take Beforehand

Create a family password. This harkens back to basic security procedures you likely put in place when your children were young. If the “kidnapper” cannot accurately report to you what the family password is, then they don’t really have your loved one. Obviously, never share the family password with anyone; not even the authorities.

What to Do if You Receive a “Ransom Call”

First, try to buy yourself as much extra time as possible. For example, tell the caller you’re trying to figure out how to get the money. Mute the call, on and off, but keep the conversation going.

Second, have another family member or friend try to contact your loved one.

Third, call 911 and have the dispatcher notify the FBI. If you are still actively on the “ransom call” you will need to ask for help with this; whether from someone else in the house, a nearby neighbor, or even a cashier at the corner store with an available cellphone.

Finally, do not under any circumstances provide financial information over the phone. Virtual kidnappers will always demand a ransom (that’s the whole point of their game), whether payable through a wire transfer service, a cryptocurrency (such as Bitcoin), or gift cards.

Editors’ Note:

While we are on the subject of scams, here is a list of the top scams in 2023. Often seniors are targeted for a variety of reasons, e.g., lonely or homebound, FOMO (fear of missing out), more trusting (grew up at a time when integrity existed), etc. Like malware and viruses, scammers using these methods continue to evolve as they try to separate seniors from their hard-earned cash. Scammers take advantage via texts, emails, social media sites (e.g., Facebook), etc. Be aware and always be skeptical if you receive something that sounds too good to be true OR if you threatened OR if there is something indicating time is of the essence (e.g., “last day” to get in, “you’ll miss this opportunity if you don’t click this link now”, etc.

1. Cryptocurrency-romance scam – always scrutinize investment opportunities and remember romance scammers deceived almost 70,000 people out of \$1.3 billion in 2022 (per the FTC).

Virtual “Kidnappers” Using Artificial Intelligence (AI) to Extract Enormous Ransoms (continued)

2. Payday loan scam – hair on the back of your neck should stand up if anyone asks you to pay for a loan fee with a gift card or even cash.

3. One-time password (OTP) bot scam- scammers pretend to be legitimate financial institutions or vendors (think Amazon) and may contact you regarding your account. They will ask you to approve a charge or ask for your two-factor authentication code. Never share this information or respond to any unsolicited text, email or phone call.

4. Student loan forgiveness scam- have a grandkid in college? Don’t fall for phony sites promising loan forgiveness, asking for personal information e.g., social security numbers, bank information, etc.

5. Puppy purchase scam- looking to adopt a pet? Go to an animal shelter or better yet, contact our SCA Pet Club and they will help you find one.

6. Check washing scam – if you still write checks, use an indelible black gel ink (think gel pen) instead of the old black or blue ink pens that contain dye-based ink. Scammers can “check wash” dye-based ink and erase whom the check is paid to and the amount, then fill in their name and amount, leaving your signature untouched. Also, don’t leave outgoing mail in your mailbox for days. It’s safer to drop off letters at the Post Office, especially if paying a large bill with a check.

7. Free-gift QR code scam

This is a variation on a basic [QR code scam](#) that the FBI warned about: Scammers put fake codes over real ones to exploit the convenience of the barcodes people scan into their phones to see restaurant menus or make payments. Experian’s Bruemmer says scammers may call and say they’re going to send a QR code to your phone, so you can receive a free \$100 gift card. In reality, the QR code may take you to a malicious website.

How to stay safe: If you receive a QR code out of the blue, contact the person or company that supposedly sent it, to make sure it is for real. Use a phone number you know is authentic.

8. ‘Oops, wrong number!’ texts

Seemingly misdirected messages are increasingly the start of a scammer’s ploy. A [text message](#) addressed to someone else pops up on your phone. It seems urgent — a rescheduled business meeting, or maybe a romantic get-together. You text back, “Sorry, wrong number!” The scammer keeps up the friendly texts, and may eventually invite you to join an adult website to see revealing pictures so you hand over credit card info and money, or try to convince you to make a cryptocurrency investment (and take your money).

How to stay safe: Don’t respond to texts from numbers you don’t recognize. **Don’t** click on links in them or respond with “STOP” if the messages say you can do this to avoid future messages. Block the phone numbers they come from.

9. Fake barcodes on gift cards

Law enforcement agencies warn that nimble-fingered crooks affix fake barcode stickers over the real ones on the back of [gift cards](#) in stores. When you purchase the card, the cashier scans the fake barcode at checkout — directing your money into the scammer’s gift card account.

How to stay safe: With some gift cards, you can make sure the number of the barcode matches the number on the packaging. Or feel or gently scratch the barcode on a gift card before buying. Don’t purchase if the barcode is on a sticker, or if the package is ripped, wrinkled, bent or looks tampered with.

Virtual “Kidnappers” Using Artificial Intelligence (AI) to Extract Enormous Ransoms (continued)

10. Crypto refund swindles

Beware if you’ve lost money in a cryptocurrency scam: Criminals set up fake “get your crypto cash back” websites, including one that looks like it’s from the U.S. Department of State. After luring targets, they contact those who respond by phone, email or social media and ask for personal ID information, including account numbers and passwords, plus an advance fee for their services payable by gift card, cryptocurrency or wire transfer. You get nothing, warns the FTC.

How to stay safe: Crypto investments aren’t insured by the government the way bank accounts are. For the most part, funds lost to crypto scammers are gone. Don’t trust anyone who contacts you saying they can get your money back, says Frank McKenna, chief fraud specialist for the fraud detection company *Point Predictive*.

11. Bank impersonator racket

Let’s say you’ve set up your bank or credit card online accounts so you can access them only with a live code sent from the institution. And let’s say a criminal has your bank or credit card username and password login and wants to steal from you. What would he or she do? In this increasingly common fraud, they call you, claiming to be from your bank and warning about a problem with your account. The caller tells you they’re emailing or texting you a “onetime passcode” for logging in and asks you to read it back to them for verification. In reality, the scammer’s login attempt triggered your bank to send you the passcode. Handing it over gives [criminals full access to your account](#).

How to stay safe: *Never give your onetime passcode to anyone who calls you.* Hang up, find your institution’s phone number on a bank statement or on your credit card, and call. Ask if there really is a problem and report the con to the bank’s fraud department, McKenna recommends.

12. LinkedIn relationship fakes

A criminal might send you a message on LinkedIn, claiming to be just starting out in the same industry you’re in, seeking advice from a more experienced colleague. It’s flattering and fun to be a mentor, so you agree. You get to know each other, and eventually they ask to move your conversation onto a personal device, then lure you into a scam.

How to stay safe: A request to continue your chat on a more private channel is a warning. So is talking up crypto. LinkedIn may flag requests to go off-platform as it tries to remove fake accounts. But you should end the conversation and block the scammer.

13. ‘I’ve got your package, where’s your house?’ hoax

New [package delivery scams](#) include texts and phone calls purportedly from a professional-sounding delivery driver who can’t find your house. Didn’t order anything? They may try to convince you someone’s sent a gift. Or you may receive an email about rescheduling a drop-off or a fake “package - delivery attempt” sticker on your front door. Their goal? To get you to provide personal information or simply click on a link they provide. That link then downloads malware that will harvest passwords and account info from your computer.

How to stay safe: Contact the seller or delivery service using a verified phone number, the FCC recommends. Don’t use numbers or links provided by potential scammers.

14. Out-of-stock item scam

Scammers often place fake ads on social media sites for products at too-good-to-be-true prices, take your order and payment info, then tell you the item’s not available right now. Your refund is on the

Virtual “Kidnappers” Using Artificial Intelligence (AI) to Extract Enormous Ransoms (continued)

way, they promise, but it never arrives. And you can’t reach anyone at the company about it.

How to stay safe: Research businesses online before you buy, and only shop on secure websites with a lock symbol in the browser bar and an internet address that begins with “https.” And pay by credit card, the FTC recommends. That way, you can withhold payment pending an investigation.

We hope that this information will make you more aware and help keep you safe while online. We use online resources more and more each day and even though measures are taken to protect us from scammers, new ones appear almost as soon as ones are identified and removed. So just be careful on what you are reading and what you are clicking on and go with your gut: if it seems out of place or you are not sure if it is real or not, or when in doubt, don’t click on that link and don’t trust that scam voicemail or text.

What, Really? This isn’t April, so we guess it isn’t an April Fool’s joke!

We all recognize the little lock symbol used on the Chrome browser, right? Word has it that Google plans on retiring it and replacing it with a **new “tune” button** this coming September. But why? The lock icon tells us if a site’s HTTP connection is secure (encrypted), also known as HTTPS, at least that is what we have been told.

But now Google is saying it could be misleading users to think the site is safe and secure to use. Well, isn’t it? According to Google, the lock icon **only** designates that a website is secured with HTTPS and preventing traffic from being transmitted in plain text, and thereby stopping eavesdropping. **BUT** a phishing page that hosts malware can **ALSO** trigger the lock icon to appear on Chrome. A hacker needs only to install an SSL certificate with their phishing site to secure the connection with HTTPS. So in essence, the lock icon is **NOT** an indicator of website safety.

Say it isn’t so. We have been telling our folks to look for the lock on a website as an indicator of safety and NOW Google is telling us that it isn’t necessarily true? For years Google (and others) have pushed to adopt HTTPS. So what’s the alternative?

Google will replace the lock with a new “tune” icon that can open up additional privacy related controls to the visited site. Many users never realized that clicking on the lock icon can show additional controls, such as the ability to shut off notifications from a site, or to cut off its access to the web camera or phone, or prevent tracking or setting cookie permissions, etc.

Did you know that? Next time on a website, try clicking on the lock icon in the URL and see what additional controls appear. And remember you can also double-check the spelling of a website URL to ensure it is the real one or the one you are looking to view.

Anyways, come September, look for a new tune icon.

It is supposed to look like this:



Tell us what you think. Confusing or what?

What to Know about Malware

Cybercriminals use malware (or malicious software) aka intrusive code or files to distribute over a network in order to steal data from unsuspecting users. What happens is that the malware obtains information about one's device, as well as, personal credentials and forwards the information to hackers to commit identity theft or fraud. So, what type of information are we talking about? Well, think bank account details, login in credentials, social security numbers, credit card account numbers, etc.

Malware attacks include ransomware, Trojan horses, adware, spyware, etc. Each may infect and cause damage to users' systems differently, but their main objective is the same: to steal sensitive data to provide remote unauthorized access to hackers, who then can control one's device.

Why is this done? Primarily to earn money because cybercrime is a **BIG** business. An estimated cost of a data breach (global average) amounts to \$4.35 M per year. It is estimated that in 2022, world-wide malware incidents reached \$5.5M.

How is this done? Well, hackers use various techniques such as ransomware, spyware, brute password attacks, etc. to obtain the data from users, sometimes destroying computer systems or holding them hostage. They also sell one's personal data and financial information on the dark web for profit.

An unsuspecting user clicks on an infected file thereby infecting one's machine. ***The majority of malware infections are the result of a user's actions.*** A user may be pressured or threatened into clicking on an "urgent" message or email after receiving an alert that "your account is compromised" or "log in to check on recent changes" or "scan your computer now". Malware can even be set up that triggers a payload to the user's PC if the user clicks on a link. Beware, the link may offer a "yes" or "no" but clicking on either one triggers the infected file and the payload is delivered.

Malvertising is a form of malware that uses advertisements to inject code into legitimate websites and users may unsuspectingly click on them which results in activating the malware. Once activated, the malware can destroy one's PC, populate one's desktop with pop-up ads, install programs that record keystrokes, e.g., keyloggers, replicate and spread to other devices on one's network, or even restrict access to programs and file.

Is anyone safe from malware? **Yes**, users can protect themselves by keeping their systems up to date and using some type of antivirus/antimalware software. But is there anything one can buy to absolutely guarantee against being infected? Unfortunately, **no** there isn't. Remember, *it is a user who normally triggers such infections by one's actions.*

Common attacks may be targeted towards larger organization and industries, including education, banking and financial services sites. This also includes government sectors and healthcare as the potential payout is much greater than in individual user. But individual users are most likely to be more vulnerable than major corporations who go to great lengths to secure their systems. Even so, energy and utilities have become recent targets because of the critical services they provide. Imagine how devastating it could be if the electric grid was held ransomware and folks could not get electricity until the electric company paid up.

How can I tell if I have been infected by malware? That is an Excellent question. There are some signs or indications one should be aware of. For instance, if one's system takes longer to start than normal, or if it freezes more than normal, or if it is recently crashing, one might be infected. Or if one gets frequent pop-up ads all of a sudden, or one notices a new icon or toolbar that has been installed (that one did not install), or if your battery is discharging faster than normal. Or perhaps one's contacts all of a sudden receive texts or emails, purportedly from you (that you know you did not send). These could all be signs of a malware infection on one's system.

What to Know about Malware (continued)

If infected by malware, what does one do? Here are some suggestions to take immediately:

Disconnect or disable one's Internet connection. This is to prevent the malware from establishing a connection with the malware server.

Use the safe mode to login to one's device so that one's system will start in a diagnostic mode rather than an operating mode in order to better troubleshoot the problem.

Turn on the activity monitor to check for newly upload malicious files and delete any temporary files, as they may have been installed by malware.

Runs a malware scan on one's device to detect and delete any program it identifies as malware.

Now restart one's device.

Since it is possible, that personal data was compromised, BE SURE to CHANGE passwords on one's account. Remember, the longer the better, as in pass phrases.

Check your accounts to see if any unusual behavior has taken place and if so, **NOTIFY** the institution of a possible breach. One can put a hold on one's account for a specific period of time or even dispute a charge made. Be sure to check financial accounts if one uses online banking.

Remember that even though there has been an increased awareness regarding malware, in 2022 there was a 2% increase in cases worldwide. So be safe, be aware, and exercise common sense and caution while on the Internet. Have a great day!

How to scan a QR code on your Android (no apps required)

QR codes are becoming more and more used these days. What are they? A QR code is a machine readable code that looks like an array of black and white squares that are used to store URLs or other information that can then be read by a smartphone camera. When scanned, the unique pattern of the QR code translates into readable data. **QR stands for "Quick Response"** which is appropriate because once scanned, the readable information is almost instantly displayed on one's screen. A QR code can hold more data than just a barcode because while a barcode holds information horizontally, a QR code does it both horizontally and vertically, thus increasing the amount of information it can hold over a hundred times more.

Today we see these QR codes in advertisements, on food packaging, in retail, business cards and more. And once scanned, it produces more information regarding a product or it can direct one to a website for additional information (and you don't even need an application for that to do so). A QR code leads one to discover more information about something or even answer questions. Want to know how many calories are in a fast food? Or where to buy that pair of shorts that are advertised? Well, scanning the associated QR code of a product can do just that.

Your Android smartphone most likely has the ability to scan QR codes without needing a third-party app. (This also works on iPhones, too.) How does it do it? Through it's camera. All one has to do is point one's camera at the QR code and hold it steady for a few seconds. A notification should appear and when it does, tap on it. Now, if you don't get a notification, go to **Settings>** and **enable QR code scanning**.

If you have a Samsung smartphone, do the same thing. Open your camera app, point it at the QR code, hold steady and wait for the notification to appear. If it doesn't, go to **Camera settings** and toggle on **Scan QR codes**.

Now for the FUN part. Ever use **Google Lens**? If not, you are in for a pleasant surprise.

How to scan a QR code on your Android (no apps required) (continued)


What is **Google Lens**? Glad you asked. It is a feature that first appeared in Pixel phones, but now it has become a standard in many Android phones as part of the camera app. And WOW is it ever fun to use. It can identify all kinds of things, like a flower, an animal, an insect, a product (from a picture), etc. Here's how to use it:

- Open your camera app and tap *More > Google Lens*. You'll have a Lens icon you can use whenever you open your camera app.
- Alternately, you can activate it by using the Google Assistant and saying, "OK, Google". Then tap on Google Lens at the bottom right.



On an Android phone or tablet:

- Open the Google app and at the bottom, tap "**Discover**".
- In the **search bar**, tap **Google Lens**.
- Select the area you want to use to search.
- At the bottom, scroll to find your results.

Since there are many different manufacturers of Android phones, here is another alternative to try if the above does not work on your particular phone. (Note: You can also use an iPhone/iPad to do this.)

- On your phone or tablet, go to **Google Images**.
- Search for an image, then tap on it.
- At the bottom left side, tap on Search inside image .

To search with a website image in the Chrome app, one must first make Google one's default search engine. Then do the following:

- Go to the Google app or Chrome app.
- Go to the website with the image and touch and hold the image.
- Tap **Search Image with Google Lens**.
 - To search an object in an image (if available on the object), tap Select .
 - To search only part of an image, tap Select image area  and then drag the corners of the box around your selection.
- At the bottom, scroll to find related search results.
- To refine one's search, tap "**Add to your search**" then enter keywords.

So if you haven't yet tried using Google Lens, give it a try. Next time you are on a walk around your neighborhood, stop and take a picture of a neighbor's flower or plant and Google Lens will tell you what it is. Try it and let us know how you like it!

Summer is coming this month! Get out and enjoy the fresh air. Use the pools. Use the Fitness Centers. See an upcoming show or attend a seminar. If you belong to one of the **fifty-seven (57)** SCA Chartered Clubs, get out and attend one of their meetings or take advantage of one of their facilities. If you don't belong to a club, you can attend a meeting to see if you would like to join it. Or, try one of the **twenty (20)** Interest Groups here in SCA. Find all of the clubs and interest groups listed in your monthly Spirit magazine. Get involved. Have fun. Enjoy the summer!

Passwords, PINS, Passphrases and now Passkeys?

It is so hard just trying to keep up with all the new technology. I finally learned to strengthen my password by adding a number and/or special symbol along with both upper and lower case letters and increasing its length to 18 digits. You know hard that was to change all of my passwords and then find a place I could remember to put them in, in case I forgot? I know only about five (5) of my most used passwords by heart. The rest I have to look up when I need to use them. Oh yes, there are password managers that can do all of this for me, but I am not ready to move into that arena just yet. BUT, now I read that they too may soon be obsolete. Everything seems to be moving so fast and its hard to keep up, but I keep trying (smile).

So what is this NEW thing called **PASSKEYS** and how do they work? A passkey is supposed to be even more secure and eliminates the need for passwords. Essentially it is a login credential requiring either a biometric authentication (e.g., fingerprint or facial recognition) or a PIN (personal identification number) or a swipe pattern (used with Android machines) for access to a site. ***The passkey works on a user's device*** so no one can hack one's account due to a data breach or finding one's password taped to the bottom of one's keyboard. Passkeys were created using public key cryptography for access, with each key being unique and encrypted for added security.

But why is this new? Face ID, fingerprints and PINS have been in use for a while now. Doesn't Apple already use this technology? Yes, and so does Microsoft. And some third-party websites have adopted passkey use. In the World Password Day event (May 4, 2023) Google announced that it too will start using this method for logins.

Passkeys use Bluetooth technology which requires a *physical proximity* and therefore increases security and makes it harder for scammers to crack one's login access. Once a user signs into an account or website, a push notification is sent to the user's device through Bluetooth. The user then needs to unlock their device with their private key that relates to the login. At the next login, the user will only have to use the chosen credential when prompted (which is their private identification and no password to remember). The passkey option appears in the username field. Both Google's Chrome and Apple's iCloud Keychain synchronize passkeys across multiple devices through the cloud. Confused?

Here's an example. A user tries to login to one's mail account on their computer. Next they get a text message on their phone asking if they are trying to login to the mail account? They answer Yes and now they are in their mail account without typing in any password.

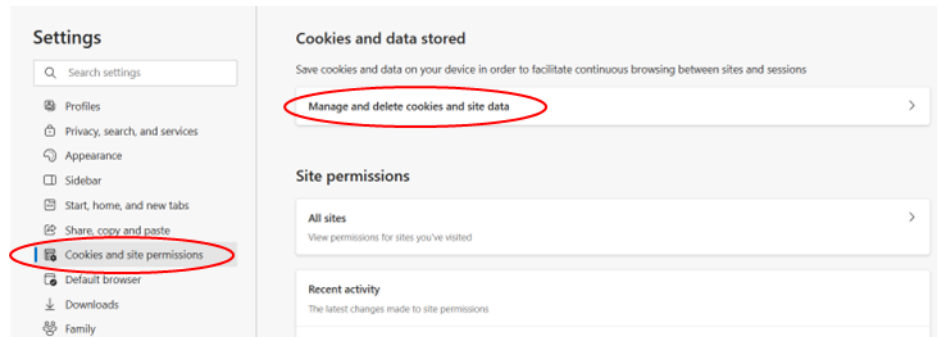
Passwords are vulnerable to cyber attacks, brute force attacks and data breaches. Folks are also sometimes tricked into revealing their passwords through phishing scams or fraudulent websites. ***A passkey cannot be stolen as easily as a password because data is stored on one's device and NOT on a web server.*** In other words, a scammer would need to access one's device via a fingerprint, facial ID or PIN to unlock it and would have to be in near proximity to use Bluetooth. If one loses one's device, the scammer would be unable to access information without biometric authentication.

Apple, Google and Microsoft are working to ensure passkeys are implemented and working across all platforms since password only authentication is becoming a security problem when folks re-use their passwords on multiple sites creating more risks for data breaches and stolen identities. Currently, Google only supports passkeys on Chrome, Edge and Safari browsers, but passkey technology is coming more and more accepted and websites and apps may start offering it as an option as opposed to just using passwords.

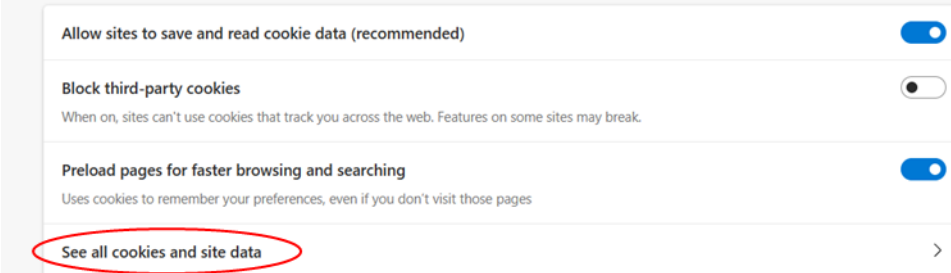
Useful things you may want to know, or Frequently Asked Questions (FAQs) that we made up ourselves

Q. *I read about browser history and cache in last month's Newsletter. Now I would like to know if there is a way to remove specific cookies from my browser (and not all of them). I use Microsoft Edge on a PC.*

A. Yes there is and sometimes when browser cookies don't function as designed causing websites to break or just load incorrectly, you can correct the issue by deleting cookies associated with that particular website instead of deleting all cookies. In MS Edge, when you are at a website, click on the three dots in the upper right-hand corner and scroll down until you see "Settings". Click on Settings to display a list of options. You need to click on "Cookies and site permissions" in the left-hand margin, then select "Manage and delete cookies and site data" in the right hand side of the page. Another display will appear.



← Cookies and data stored / Cookies and site data



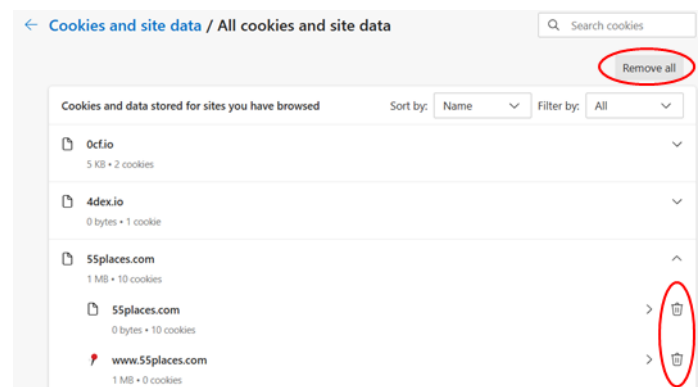
Select "See all cookies and site data" to review all of the cookies stored for sites you have browsed. You can now select individual cookies by clicking on the down arrow, which will display a trash can icon to delete the cookie.

If you choose to remove all cookies, you can do that also by selecting the "Remove all" button at the top of the page in the upper right hand corner. But that is not necessary if you are only having an issue with a particular site. Let us know if this answers your question.

Q. *I know that I do not have to update to Windows 11, as Windows 10 will be*

supported until Oct 2025 AND my current computer just doesn't meet the specs to run Windows 11. But I heard that Microsoft is not going to release any more versions of updates for Windows 10. Is this correct?

A. Actually, not quite. Microsoft is going to stop adding **new** features to the operating system (OS). What



Useful things you may want to know, or Frequently Asked Questions (FAQs)

that we made up ourselves (continued)

does that mean? If you are using Windows 10, you will receive **performance fixes** and **security patches only** through future Windows 10 updates. There are an estimated 73% of Windows users still using Windows 10, so you do not have to worry about it. You can continue to use Windows 10 until 14 Oct 2025 or until you decide to buy a new PC that supports Windows 11.

Q. I attended last month's class on streaming to one's TV because I am seriously considering cutting my cable. I know a few sites were mentioned in the class. I was wondering if there were more?

A. Here is a list of **12 Free TV Apps** that may help you decide whether or not you could "Cut Cable" and still enjoy your television set. **The bold, italic ones** were mentioned in the class slides:

- ***Crackle***
- ***Tubi TV***
- ***Pluto TV***
- NewsON
- PBS Kids
- Xumo
- Crunchyroll
- Twitch
- Freevee
- YouTube
- ***The Roku Channel***
- Popcornflix

Q. How do I create a passkey to use on my Gmail account?

A. This should work if using an Android device. First log into your Gmail account. In the upper right-hand corner, click on your account icon (e.g. your profile, picture, name, etc.) and select "*Manage your Google Account*". On the next page displayed, on the left hand margin, select "*Security*". In the middle section, scroll down until you see a section titled "*How you sign in to Google*". It will list options such as 2-Step Verification, Passkeys, Password, Recovery phone, and Recovery email. Select the arrow (>) next to "*Passkeys*". On the next displayed page, you may see "*Automatically created passkeys and a device listed*", e.g. your cell phone. Below that you will see a box that reads "*Create a passkey*". Click on it and follow instructions. **OR**

Alternatively, when you select the arrow next to Passkeys and see "*Start using your passkeys*", click the blue box "*Use passkeys*". It will display a new page indicating you can now use your passkeys to sign in. Click "*done*". The next time you sign into your Gmail account, it will ask you to confirm. Select "*Continue*". A QR code will be displayed. Follow the instructions and scan it with your cellphone. Follow instructions on your phone to allow permissions. Give it a try.