Volume 25 Number 04 Apr 2025

SCA Computer Club notes

Classes for the Month of Apr

To enroll, log into the website at https://computer.scaclub.org. Go to **Calendars> Classes/Events**. Click on the class you want to take and under "Action", click on "**Enroll**". 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. You must have your **SCA Resident ID** with you to check-in. **Please read the article How to sign up for classes? in the Feb issue of the Newsletter for a full explanation of class enrollment.**

iPad/iPhone/Mac Tips & Tricks: Learn how to navigate your iPad, iPhone and Macs operating systems, widgets, settings and all the things you don't know even exist on your device. We will also cover short cuts to make your day to day life with your devices easy as pie.

Photoshop Elements: Learn how to organize and edit your pictures. This hands-on class for both Mac and Windows users gives a basic introduction to Adobe Photoshop Elements. ***Prerequisites***: Must be comfortable using either the Windows or Mac operating system.

Mastering the iPhone: Join us as we explore the latest iOS updates, exciting new apps, and enhancements to Apple's suite of tools like Photos and other key apps. Whether you're looking to stay up-to-date or simply want to get more out of your iPhone, this class is for you. Don't miss this opportunity to connect with fellow club members and gain valuable insights from our trusted Apple guru. Bring your questions, your curiosity, and your iPhone—let's unlock its full potential together!

Buying a Computer: Buying a new computer? Learn the basic terms: gigabytes, hard disks, volatile memory, Ethernet card, cable modem, etc. in this class in order to make an informed decision.

New Member Orientation: This orientation session is designed to familiarize new Computer Club members with the Club's activities.

A Basic Introduction to AI (Artificial Intelligence): Keep up with today's technology. Have you ever wondered what all the hype is about AI? What is it? What does it do? How can you use it? Join us in this basic introductory class on AI; its uses, why it might be important for you and what you can use it for in everyday life.

Macintosh Calendar App: Account configuration, making and using multiple calendars, creating events including repeating events and the use of alerts. Sharing Calendars and subscribing to public calendars will be covered. Prerequisites: Mac for Beginners or familiarity with Mac operating system.

Macintosh Contacts App: Account configuration, using groups to organize contacts, integration with the Mail app, and import and export options will be covered. Moving contacts between servers will be covered. printing including labels will also be covered. Prerequisites: Mac for Beginners or familiarity with Mac operating system.

Classes for the Month of Apr (continued)

Mac Photos—Part 1: An introduction to Photos including how to connect you camera or memory card and how to organize your photos. How to create albums of selected photos and smart albums using several different search criteria. If time permits an introduction to location tagging and facial recognition will be included.

Mac Photos—Part 2: This second part of the Photos class is a presentation on the editing capabilities built into Photos. We will cover correcting the lighting by changing the exposure, shadow brightness and highlight brightness. We will also cover color correction and show how to correct flaws in pictures including restoring old photos scanned into Photos.

Plustek Slide Scanner: Do you have 35mm slides that you would like to digitize and store on your computer? Do you know that the Computer Club has a fabulous scanner to scan and convert slides and film? This class will discuss how to use the Plustek scanner and Vuescan software to not only scan, but also enhance the digitized image before saving. Bring a slide or two to get hands-on experience. **Prerequisites:** Some experience using a photo editing program such as **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.

Apple Talk is an ongoing discussion of all Apple products. It will include presentations and demonstrations of iPads, iPods, iPhones, Apple TVs and of course, Macintosh computers and related peripherals. As new Apple products are introduced, they will be included. Topics for discussion may include: your Apple device, your experiences, your problems or your accomplishments. Others will add their bit and you will all come away with something more than when you entered the room. The next meeting is on **Saturday, Apr 12** from 10 am - noon.

Computer Talk is an open discussion on any computer topic. It meets **weekly** on **Thursdays** from 9 - 10 am.

Photoshop Elements Advanced Topics includes topics that 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. The next meeting is on **Friday, Apr 25** from 9:30 -11:30 am. **Prerequisites:** The basic **Photoshop Elements class** or some experience using either **Photoshop Elements or Photoshop**.

The Computer Club Board will meet on Tuesday, Apr 8th at 1:00 pm in the classroom to discuss club operations. Any Computer Club member in good standing is welcomed to attend and listen to discussions. A Member's Comment period is held at the end of discussions for any member to address the Board; ask questions, provide comments or make recommendations regarding our Club.

** RECYCLING EVENT **

The Computer Club will be able to host a Recycling Event this year. Mark your calendar for **Saturday, April 5th** from **8am - noon**.

The truck will be in the Anthem Center parking lot in front of the Bocce Courts (adjacent to the Tennis Courts).

Please review the item list below and only recycle those items on the list.

WHAT THEY DO NOT ACCEPT:

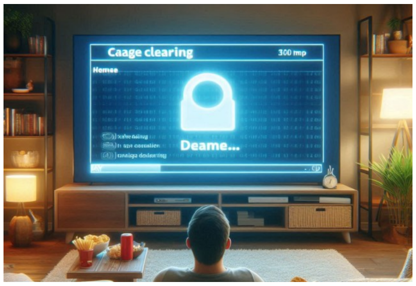
*** Plastic Bottles and Aluminum Cans, Household Batteries, Oil and Liquids, Hazardous Medical Waste.**

Electronics Recycling
LAPTOPS COMPUTERS TV & MONITORS CELL PHONES VCR's & STEREO PRINTERS COPIERS
Nevada State Recycle
"Helping Make Las Vegas A Green City"
Electronics Recycling
HOME • BUSINESS • SCHOOL
702.979.1280
Data Destruction Available
Nevada State Recycle
Las Vegas Electronics Recycling
nevadastaterecycle.com

What Do We Recycle?

- Appliances: Refrigerators, Washers, Dryers etc.
- Adaptors and Chargers
- Audio & Video Tapes
- CD & DVD ROM Discs
- Cellular Phones & Pagers
- Circuit Boards/Motherboards
- Computer Monitors
- Computers, Desktops, and PC Towers
- CD & DVD Players
- Fax Machine, Copiers, & All-In-One's
- Floppy Disks & CD-ROM Drives
- Gaming Equipment & Slot Machines
- IT Equipment
- Keyboards and Mice
- Laptop & Notebook Computers
- LCD's, and Plasma Screens
- Microwaves
- Modems & Routers
- Medical Equipment: X-rays, Mammograms
- PDA/Handheld Systems
- Printer Ink Cartridges and Toners
- Printers and Scanners
- Radio Equipment
- Rechargeable Batteries: Lithium Ion, etc.
- Servers and Server Racks
- Scrap Metal: Steel, Aluminum, Brass, Copper
- Speakers
- Stereo and Audio Equipment
- Typewriters
- VCR Players
- Video Cameras
- Wires & Connectors

Clearing one’s Television’s cache



Ever think about clearing your TV cache? Why would you do so? What exactly is cache anyway? A cache is a temporary storage area that holds data for quick access. On smart TVs, it stores information like app data, thumbnails, and login details to speed up loading times. However, over time, the cache can become overloaded with outdated or unnecessary data, leading to sluggish performance, app crashes, or buffering issues.

Why Clear Your TV's Cache?

To improve performance because too much cache can slow down one’s TV’s processing. Think sluggish or delayed app launches or buffering issues. By clearing one’s cache, it can free up space as well as allow one’s TV to run more efficiently.

By clearing the TV cache, it may resolve any application specific problems one might be experiencing. These can be crashes or login errors, or something acting weird within a particular app, so clearing the cache for that app may just be the fix one needs.

Clearing the cache varies depending upon the brand and model of TV, but the steps are similar across most brands. There usually is a **Settings** menus that allows one to navigate to an **Apps** section, that list all of the downloaded apps. By selecting any one will usually show options to **“Clear Cache” or “Clear Data”.** Now keep in mind that clearing cache will *remove temporary files*, but clearing data will *erase* all app information and therefore require one to login again. For detailed instructions, search online for your TV brand and model and “clear cache”. Remember the benefits to clearing cache include:

- Improved performance because over time, cached data can add up and slow down your TV’s processes
- Increased storage space
- Resolve app issues due to corrupted cached data
- Enhance privacy as some cached data may contain personal information

The process of clearing one’s TV cache varies by brand (and model) but here are general steps:

1. Access the Settings menu on one’s TV
2. Navigate to the Apps or Application Manager section
3. Select the app for which you want to clear cache
4. Look for an option that states “Clear Cache” and select it

Samsung Smart TVs:

- Go to Settings > Support > Device Care
- Select "Manage Storage"
- Choose the app you want to clear the cache for and select "View Details"
  Select "Clear Cache"

Clearing one’s TV cache (continued)

For LG TVs:

- Press the Home button on your remote
- Go to Settings > General > Storage
- Select "Clear Cache"

For Android or Google TVs (including Sony models):

- Go to Settings > Apps
- Select "See all apps"
- Choose the app you want to clear the cache for
- Select "Clear Cache"

Roku TVs don’t have a built-in cache clearing option; however, one can achieve similar results by restarting the TV or removing and then reinstalling any problem apps.

Remember that the exact menu names and options can vary between TV models and software versions and that one might have to clear the cache for individual apps rather than the entire system on some TVs. Clearing cache is generally safe to do and won’t delete important data, but clearing the app data may reset some settings. If one is not sure, first consult one’s TV user manual for specific instructions for one’s brand and model.

Do you use **Skype** to talk to others, perhaps your grandkids who live miles away and you don’t get to see often enough? What is it? Skype is a free video and voice calling app that was first released in Aug 2003, so it has been around the block a time or two. In May 2011, Microsoft bought Skype and used it to replace Windows Live Messenger. Well, if you are one of the 30 million folks who use it, guess what? You will no longer be able to use it because Microsoft is shutting it down on May 5th, 2025, replacing it with Microsoft Teams. Now Microsoft Teams is not a new app either; it was first launched worldwide in Mar 2017. It provides chat, video conferencing, file storage and is integrated with other Microsoft services. Teams allows file sharing, scheduling meetings and collaboration on projects and is used to improve productivity within businesses, corporations and store workspaces.

MS Teams is usually associated with work groups, but it also works for individuals much like Skype did. It is free for individual use. The free version of Teams provides free 1:1 calls between Teams users for up to 30 hours. It also provides free group calls and meetings for up to 60 minutes (and allows up to 100 participants per meeting). There is 5GB of cloud storage per user. There is file sharing and data encryption for meetings, chats, calls and files. If one has a Microsoft 365 Personal or Microsoft 365 Family subscription, then one gets extra features in Teams which include unlimited group calls and meetings for up to 30 hours and up to 300 participants per meeting, as well as 1 TB of cloud storage.

So if you are a Skype user, you might check out Microsoft Teams or other products such as Facetime (for Apple users), Zoom, Google Meet, WhatsApp, Slack, Google Duo, Viper etc. One can search and find other alternatives (to Microsoft Teams) now that Skype is going away in May. Let us know what you think.

Staying Safe from breaches is something we all need to be aware of

Data breaches and ransomware attacks affect many sectors, think healthcare, education, government, manufacturing, technology and finance. Healthcare breaches are a major concern because sensitive patient data is targeted. But Finance breaches are becoming increasingly more common and involve banks, fintech companies and investment research firms.

A company called Zacks Investment Research, which helps people with stock and financial advice, experienced a data breach. The breach happened in June 2024, but it was only discovered in January 2025. This means hackers broke into their system and stole personal information from 12 million customers. The stolen data includes names, email addresses, phone numbers, and even passwords. Unfortunately, this isn't the first time Zacks has faced such an issue.

According to the hacker, they were able to obtain domain administrator privileges for Zack's active directory that allowed them to steal source code for not only Zacks.com, but for 16 other websites, which remain unnamed. They then put the stolen information up for sale on hacker forums (along with samples) for a small cryptocurrency payment to prove authenticity as reported by Bleeping Computer. If one is not a Zacks customer, one's stolen personal information could have been included through one of the 16 unnamed websites. So what can one do?

To Protect Oneself After a Data Breach, here are some actions one should consider taking:

Change Your Passwords: Update your passwords for Zacks and any other accounts where you used the same password. Make sure your new passwords are strong and unique.

Enable Two-Factor Authentication (2FA): This adds an extra layer of security by requiring a code sent to your phone or email when logging in.

Watch Out for Scams: Be cautious of emails or calls asking for personal information. Hackers might use your stolen data to trick you.

Monitor Your Accounts: Keep an eye on your bank and credit card statements for any unusual activity.

Check If You're Affected: Use websites like "Have I Been Pwned" to see if your email or information was part of the breach.

And another topic we regularly mention is **SCAMS**. This month, April, is when taxes are due. Not only does the government want your money, but Scammers do too! Scammers are busy this month with bad actors posing as the Internal Revenue Service (IRS), so be careful. A new warning has been issued by the Treasury Inspector General for Tax Administration (TIGTA) regarding text messages impersonating the IRS.

The new IRS scam is based upon the actions that the IRS has been sending out Covid-19 stimulus payments worth up to $1,400 to around 1 million tax filers who missed them. At first, these payments were self-claimed, but now the IRS is automatically issuing them to ensure eligible taxpayers get what they are owed. This is known as the Recovery Rebate Credit and allows people to claim missed stimulus payments from 2021. If one was eligible, but didn't receive the funds, one can still claim them by filing a tax return by April 15, 2025. Payments will be deposited directly using the banking information listed on the taxpayer's 2023 return or sent as a paper check.

Scams (continued)

However, now it is reported that scammers are sending fake text messages claiming that a recipient will receive an “Economic Impact Payment” from the IRS and within that message, requests sensitive personal information, banking details and one’s social security number. The bad actor scammers then use this information to steal one’s identity and/or financial data. DO NOT BE FOOLED!

The IRS has made it clear that eligible taxpayers who didn’t claim the Recovery Rebate Credit on their 2021 tax return will receive their payments automatically and no action is required. Today, most phones and PCs have protections to keep bad actors at bay. In almost all cases, the only way anyone can access one’s device and data is if one gives it to them. How does one “give it to them”? Well, if one is using a device that is not up to date or one goes to sites that are not secure (think no lock in the URL line) or by responding to emails, texts, etc. from unknown senders, or perhaps clicking on phishing links that impersonate government agencies or legitimate sites. Doing so may install malware on one’s device to collect data which the hackers can then use.

The most important part of staying safe online is knowing how to distinguish between legitimate and scam emails, texts, or calls. Here are some things to remember:

- *Type of communication:* The IRS will never contact anyone via text for things like the Economic Impact Payment or financial information requests. The IRS will send correspondence via a letter, either mailed or faxed. If you receive notification any other way, it’s likely a scam.
- *Suspicious links:* look at the sender’s address. Government websites will end in “.gov” and not “.com” or “.net” or anything else..
- *Demands or threats:* Always be careful regarding messages that create that sense of urgency or threat; think act now or miss out or you have only 2 days to reply or if you don’t act now, we’ll notify the Sheriff’s Office or Police Department who will send someone out to speak with you. These types of messages most likely are SCAMS. Also look for misspellings or other odd things in the link, like a link that has an unusual number of characters/numbers such as: Amazon569ef7irj.com or Cox@local89044.net
- *Never act hastily* in response to a text or email or even a call from an unknown sender. If it is a legitimate email or text or call and you don’t answer, chances are they will try again to reach you. Always check the sender’s address or better yet, just don’t answer a call if you don’t recognize the number or if the number is not in your contact list.

Remember to keep your devices up-to-date and use antivirus protection. macOS has built-in antivirus protection called XProtect just like Microsoft Defender is built into Windows. And Android has Google Play Protect.

Always verify the authenticity of unsolicited emails, texts or calls and don’t click on any embedded links if provided. Contact the agency or vendor to see if what you received is legitimate or not. For example, if it is a credit card company, use the telephone number provided on the back of your credit card and not the one provided in the suspicious email or text.

Use strong, unique passwords for each account; don’t use the same password for multiple accounts. Yes, it is simple to use only one password, but you are putting your accounts at risk.

Scams (continued)

If your password is compromised, then all of your accounts are compromised. Scammers rely on stolen passwords to access accounts and impersonate agencies.

Monitor your tax account because scammers impersonate the IRS by filing false tax returns using your information. One can check one's account at **www.irs.gov** to confirm the status of one's tax return and verify that no unauthorized tax filing has occurred.

Be sure to report ANY suspicious tax-related activity immediately. This includes receiving a fake message pretending to be from a government agency. The IRS and other government agencies have dedicated channels to combat such scams. Reporting them not only helps you, but others as well.

Remember, with today's technology many protections are built in to software applications, programs and browsers to help thwart scammers from obtaining your personal information. BUT, **YOU** need to help protect yourself by being knowledgeable and recognizing possible scams AND by not acting urgently to click on any link or provide any personnel information or any login credentials in response to an unwanted or unsolicited email or text. Verify the sender if you are not sure and stay SAFE. Most scams today happen as a result of an action that we, ourself, mistakenly took. So slow down and if in doubt, don't. Don't click, don't call, don't respond.

QR Codes...what are they...how do they work...

A Quick Response code (QR) code is a square-shaped graphic that has tiny black squares on a white background. It might remind one of a pixelated maze and its design has information which can be scanned using an smartphone or QR code reader that will then direct the user to a website, an app or specific content like product information or promotions, etc. The QR image has three (3) small squares in each corner (except for the bottom right corner) and they are referred to as alignment markers to help devices read the code properly. Perhaps you have seen them in restaurants or fast food places? It is not the barcode that one sees on the backs of packages.

Ticketing and payment systems are using them and while there have been promotions for recommended QR reader apps, it is NOT necessary to even have one of those apps because almost all smartphones are able to scan QR codes within their camera apps. To use the QR reader on an iPhone, open the camera app and point the camera at the QR code you want to scan. Your camera should then recognize the code automatically and a notification will appear at the top of the screen with a preview of the website or action associated with the QR code. Tap the notification to open the website or perform the action.

If you have an Android phone, open your camera app and point the camera at the QR code and wait until it focuses in on the code. You should see a notification pop up asking if you want to open the link associated with the code. (If not, tap the notification that appears to open the link.)

If the Camera app on your phone doesn't recognize the code, make sure it is in focus or adjust the angle or distance of the camera. Some older phones may not have the capability or software to scan QR codes.

Is it safe to scan these codes? Excellent question! Like everything else these days, scammers have

QR Codes...what are they...how do they work... (continued)

started to infiltrate QR codes in order to look like the real thing and send folks to an illegitimate site. The phishing attacks are known as "QR phishing" or "quishing" and they are on the rise, tricking unsuspecting users into scanning malicious codes so that they can steal personal information, login credentials, financial information, install malware or even redirect the user to fraudulent websites. And QR codes can also be sent via email or text messages, claiming to be from trusted sources (e.g. a bank, delivery service, tech support team, etc.) The email or message may create a sense of urgency like saying one's bank account has been compromised, or verifying a payment so the user needs to click on the embedded QR code.

Typically, if it is a fake QR code, it will ask one to provide all kinds of personal information which will then be available to a hacker. QR codes are growing in popularity as a form of payment (think restaurants or fast food places) and scammers are taking advantage of creating fake codes to have one's money sent to the wrong account, or a higher amount than required sent from one's account or using the code to install malware on one's device. Even the FBI has issued warnings about QR phishing, so how does one protect oneself from being duped?

Be aware and don't just arbitrarily scan a code. Look at it. Does it look weird or off? If it is a business code, does the logo look legitimate? Does it match the brand colors or other specifications? If in doubt, then don't scan it. When you do scan a QR code with your camera's app, a notification will pop up on the screen immediately (after the camera's QR sensor captures the code). Once the URL appears, check or verify it for malicious signs and only click on it if it has "https://" in front of the link and is encrypted. And don't be one of those who just "have to try out the latest new thing". Avoid scanning codes from emails or text, especially if the email or text is unexpected or creates a sense of urgency that one needs to take action upon.

Don't just find any QR code and click on it just to see what it does. Even though vendors are using (and posting) QR codes in their shops, stop and think about the above, because in some cases, scammers have placed fake QR codes (or even replaced the real QR codes) over the vendors real code in order to steal privacy information. Here in Las Vegas, scammers have used parking meters to replace legitimate QR codes with their fake ones by placing the fake code over the legitimate code, so be careful. You might even want to skip using a QR code for payment in restaurants that have them. Just tell your server you would rather pay in cash or by credit card. And avoid any emails or texts that you receive informing you that you just won a prize or you can get a discount by scanning the code or if it indicates a security alert that wants you to immediately scan the code to be safe. It's all what we call "hogwash", so don't fall for it.

If you do plan to scan QR codes, keep your device up to date and use the built in QR code reader on you phone instead of downloading a QR code reader elsewhere. And if you must have a separate QR code app, download it from the Apple store (for iPhones) or from the Google Play Store (for Android phones). Don't be afraid to use technology, just use it safely. It's a fast moving train so keep up-to date and read your club's newsletter each month and take advantage of all the classes your club offers.

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

that we made up ourselves

Q. In the Introduction to AI class, I tried Copilot for the first time and it was fun. But I am an Apple user, not Windows. Can I still use Copilot on my computer?

A. Excellent question! When Copilot was first introduced two years ago, it was only available on Edge, Chrome, Firefox and Safari web browsers. But in 2024, it rolled out on Android, iOS and iPadOS and is also integrated into Teams, Outlook and other Microsoft apps. And yes, the new Copilot app is available for Mac users too. The macOS app requires one to have macOS 14.0 or later, as well as a Mac model with an Apple M1 chip or later. And you can download the Copilot for Mac app from your Apple Store. All Copilot users now have free, unlimited access to "Voice" and "Think Deeper" features. Copilots' Voice capability can help users practice a new language and Think Deeper is powered by OpenAI's o1 model and can tackle complex tasks so give it a try and let us know what you think.

Q. I am new to using a laptop; new to technology, new to using email and online shopping etc. My grandson in high school wants to be a computer consultant. He wants to help me set up my email and asked me to provide a "username". So I told him to use my name, Millie and the year I was born. It would be Millie1949@gmail.com but he said "Oh no, grandma, don't use your real name or birthdate". Why would he say that?

A. Usernames do not require your real name. Using your name and birthdate makes it easier for hackers to identify you and you are providing more data for them to hack your account. Things to avoid in usernames include your date of birthdate, address, email address, phone number, an ID number, your social security numbers and even your hometown, etc. since usernames are public information and hackers have the same access to them as you do. And if you have more than one type of account, you might want to use different usernames for each. You can mix words or phrases that you will remember from your hobbies or personal characteristics, your favorite items or old nicknames or even favorite games, TV shows, movies, etc. And then add in random characters. For example, if your favorite game growing up was hopscotch and you liked hotdogs, you could use "hotdogs4hopscotch" as a user name. When it comes to passwords, they too should be unique and not related to your username, but something you can easily remember. You do not want your username and password to be connected so using a username of "antsmarching2x2" and a password of "thelittleonestoppedtotiehisshoe" would definitely be related and not a good combination, although easy to remember. The same goes for a username of "JackandJill" and a password: "felldownthehill". You get the point. Use something you can remember but be sure your username and password are not related. Now there are random username generators and even some password managers have them, e.g. 1Password, Bitwarden, etc. Ask your grandson for help in setting something up. And ask him for recommendations on password manager apps.

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

that we made up ourselves (continued)

Q. I have an Echo Dot. I recently received an email from Amazon saying they need my consent to having my voice recordings sent to their cloud for processing. I have had the "Do Not Send Voice Recordings" enabled since I wanted the commands locally processed. I understand that this setting is no longer available . Is this true or a scam email I should ignore?

A. We think the email is legitimate. Starting March 28, 2025, Amazon revealed that the Do Not Send Voice Recordings setting will no longer be available and that all recordings will be processed at the Amazon data centers. Any Echo that still had this setting enabled would be automatically switched to Don't Save Recordings and that voice commands will be transmitted to Amazon's cloud for processing but deleted afterwards. Previously saved recordings would also be deleted and Alexa's voice ID (a feature that recognizes individual users' voices to provide personalized responses) would be disabled. Amazon's decision to discontinue the Do Not Send Voice Recordings setting was so that it could "expand Alexa's capabilities with generative AI features that rely on the processing power of Amazon's secure cloud." In other words, Amazon is collecting more voice data to enhance AI training and improve its smart speaker technology. The news that Amazon is focusing on privacy tools and controls that their customers use most and work well with generative AI experiences came after they launched Alexa+, an AI version of Amazon's digital assistant. Amazon also indicated that voice recordings will be encrypted while in transit and that their cloud was designed with layers of security protections to keep customer information safe. So the bottom line is that Amazon is mandating cloud-based processing for Echo voice commands and removing the ability for users to locally store them. And in order to expand their generative AI capabilities, Amazon has disabled Alexa's voice ID. You can still use any of your Alexa or Echo devices like you do and maybe they will be even more helpful in the future?

What's on the horizon? The Global System for Mobile Communications (GSM), is a digital cellular network technology that enables mobile phones to transmit both voice and data. The GSM Association recently announced that the latest Rich Communications Services (RCS) standards and specifications will be including end-to-end encryption based on the Messaging Layer Security protocol. So what does all this mean? Simply put, this means that nobody else can see your messages but you, not your carrier or companies that make messaging apps. And that Apple, who had end-to-end encryption for their devices, will soon add support for end-to-end encrypted **RCS** messages to iOS, iPadOS, macOS and watchOS in future software updates. Apple had rolled out RCS support for iPhones with the iOS 18 update, but the security feature for **RCS** messaging for its other devices was not available because it couldn't handle cross-platform encryption. Android and Google Messages did offer end-to-end encryption for **RCS** texts but **only** when chatting with other Google Messages users. In other words, iPhone messages could not chat with Google Message users and Google Messages could not chat with iPhone message users. **BUT** this new standard fixes all that and it will be a big **WIN** for everyone when this security feature arrives...soon we hope. Android and Apple will be able to chat with each other via messages!