Volume 24 Number 10 Oct 2024

SCA Computer Club notes

Classes for the Month of Oct

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.

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.

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.

Windows 11-Introduction: Want to learn about Microsoft's newest operating system (OS), Windows 11? Are you wondering if you should upgrade or do you want to become more familiar with it if you recently upgraded? Learn about some basic capabilities to this ever-changing OS.

PowerPoint Basics: This introductory class will familiarize the student with the basics of Power Point. Learn to create and design slides using the menu commands and how to set up and run the slide show. The class has hands-on interaction to practice various skills.

iPad/iPhone Introduction: Basic iOS settings and features to set up iPhone and iPad, including iCloud linking all devices.

Apple Watch-Introduction: An introduction to the basic capabilities of the Apple Watch including; pairing with your iPhone, basic setup and use.

iMovie for Mac/iPad: In this beginner-friendly class, you will learn how to transform your videos into professional-looking movies using iMovie on both Mac and iPad. We will cover a range of essential video editing techniques and effects to elevate your projects.

- **Basic Editing Skills**: import and organize your video clips.
- **Picture in Picture**: Create dynamic videos by overlaying one video clip on top of another.
- **Green Screen**: Replace backgrounds and create immersive scenes with green screen effects.
- **Cutaways**: Insert additional footage into your main video.
- **Audio Editing**: Add, edit, and fine-tune audio to complement your visuals perfectly.
- **Movie Trailers**: Create movie trailers for your projects.

By the end of the class, you will have the skills to create polished videos with a variety of effects, and you will have completed your own movie trailer project. Join us to turn your video footage into cinematic masterpieces!

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 investigation of all products Apple. It will include presentations, discussions 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:

- your Apple device
- your experiences
- your problems
- 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, Oct 12** from 10 am - noon.

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

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. **Prerequisites**: The basic **Photoshop Elements** class or some experience using either **Photoshop Elements or Photoshop**. The next meeting is on **Friday, Oct 25** from 9:30 - 11:30 am.

Your Computer Club Board will meet on **Tues, Oct 8 from 2:00 - 3:00 pm** in the Classroom. Any member in good standing is welcomed to attend. Listen to the discussions and learn how your Club operates. A Member's Comment period (near the end of the meeting) allows for members to address the Board, provide recommendations, ask questions, etc. regarding the meeting. Come and learn how your Club operates and consider running for the Board in 2025.

If you are interested in running to be either an officer or a leadership team member at large please submit your:

Name, e-mail address, and phone number and the position you would like to hold (Position: President, Vice President, Secretary, Treasurer, Assistant Treasurer, or Leadership Team Member at Large) **NLT than Oct 18th** to ***Terri Begas*** using the **club's website Contact Us** form at **https://computer.scaclub.org/contact** and selecting **Election**. 2025 will be a new year to try new things and being part of the Computer Club Board can be a new adventure for you. Don't pass up this opportunity.

The next general meeting for our Club will be on Friday, Nov 1 from 1:00-3:00pm in the Anthem Center Ballroom. Mark your calendars now so you can listen to the candidates running for the 2025 Board.

Things you might want to know?

Do you take photos? Did you know that every photo includes EXIF (exchangeable image file format) data with details about the image, including the kind of camera, exposure levels, color information and GPS (global positioning system) data? The GPS data by default includes the pinpoint location of where the photo was taken. And while this might be good-to-know information if you are a photographer, it could also be something you might not want to share. Today, privacy is exploited and anyone with an interest in your activities can look you up online, find photos you have shared and use them to gather information about you. Well, some social media sites, like Facebook, strip location data out of images for you, other sites (or apps) may not, so you might want to remove that location information yourself before sharing your photos online or with friends.

Here's how to do it on Windows. Fortunately, in Windows 11, the functionality is built-in. You simply right-click on an image, open its ***Properties*** and then go to the ***Details tab***. Now click on *"Remove Properties and Personal Information"* and location data will be removed.

With Android devices, *open Google Photos, select the photos*, tap ***More***, then ***Edit location***, and finally *Remove location*. On a computer, open the photo, tap the *three-dot menu*, tap the *edit icon* next to the location, and then tap *Remove location*.

To do so in MacOS, open the image file in the ***Preview app***, then go to ***Tools> Show Inspector*** (or press the combination keys of Command + i). In the Inspector window, click on the ***information tab*** (the one with the "i" icon), then click on the *GPS tab*. Finally click on *"Remove Location Info"*.

iOS and iPadOS lets you remove location data from the ***Preview app***. Open the image, then *select the three (3) horizontal dots* (at the top of the screen aka the *ellipsis icon*). Select ***Adjust Location***, then tap *Remove Location*.

Did I just download a virus?

Ever download something and weird things started happening? Viruses can cause unusual behavior in the way your system operates. Sometimes an app is downloaded from an illegitimate source and packed with unwanted apps or malware. That is why it is recommended only to download apps from a legitimate source such as the Apple, Google Play or Microsoft stores since they do take measures to scan for malware in their apps. Does that mean the apps are 100% safe to download? Of course not, but chances are better to download from one of those reputable sources than some unknown source.

Viruses often hide in files that resist being erased by normal methods, like if the program behind it is still running in the background. Some even prevent total deletion by regenerating if you try to delete them, allowing malware to maintain control of your computer. So if you have a file you can't delete or if you look in your Downloads folder and see a file with a suspicious name or a jumbled string of letters, you might have unknowingly downloaded a malicious file.

Another indication of possible malware may be that your computer keeps waking up on its own (after you have put it to sleep). A hacker can use this as a way to steal data or use your computer for crypto mining.

Have you ever downloaded a file and then could not find it? Well, perhaps your antivirus software quarantined it. That's a good thing. If a file has disappeared, check your antivirus quarantine folder to see if it is there and if it is, don't try to download it again as it could very well be a virus.

What are some signs that you may have downloaded a virus or malware? Unexpected

Did I just download a virus? (continued)

pop-ups, undeletable files, odd wake-ups, and disappearing files. If you notice any of these abnormalities, do yourself a favor and run a malware scan immediately. This could identify and remove any infectious files you might have unknowingly downloaded.

Remember when downloading anything on your system, always be cautious and don't rush. Read the prompts carefully before taking any actions. With phone apps, be certain you want to allow an individual app permissions (e.g. location, microphone, camera, etc.), especially if it isn't needed to use the app.

Download apps from an approved source such as one of the App stores: Apple, Microsoft, Google Play, or the Galaxy Store (for Samsung apps). And also remember, if in doubt, don't. If you are not sure about whether or not the action you are about to take is safe or not, don't take that action. It's much better to be safe, than sorry.

Android's latest updates for its mobile operating system

Most of us know what a screenshot is, right? Well, **Circle to Search** is an easy way to capture a specific, limited area of one's screen, not the entire screen. One can highlight an image on one's screen and then using circle to search, to look up and identify that image in a photo or video or share just a portion of one's screen with others.

Multisearch provides one the option of searching text and images at the same time to help one understand ideas or topics. For example, one could use *circle to search* by drawing a circle around an image of a Pizza Margherita. If one didn't know what that was, one could ask "what is a pizza margherita?" or "why is it called a pizza margherita?" or "what are the ingredients of a pizza margherita?" Then one will quickly get an answer. This is an example of the latest AI-powered upgrades for use with Android phones to search anything without having to open additional apps.

But the only drawback for now is that it is only available on certain phones/products. These include phones such as the Pixel 9 series, Pixel 8 series, Pixel 7 series, Pixel Fold and Pixel Tablet. It is also available on Samsung series phones; the Galaxy S24 series, Galaxy S23 series, Galaxy Z Flip and Fold 5, some Galaxy A series, and the Galaxy Tab S9 FE and FE+.

Circle to Search is only one of the latest updates for the Android mobile OS. The others include **Talk Back**, an accessibility feature for those who are blind or have low vision. It will provide detailed audio descriptions of digital images so the user can hear the description of all sorts of images (e.g. online products, photos and even pictures in text messages). **Listen to this page** is another accessibility product allowing users to listen to web pages in the Chrome browser. Users can pause, rewind and fast forward as well as set their preferred listening speed, type of language and voice. It currently supports English, French, German, Arabic, Hindi and Spanish.

Although Android has had an Earthquake Alert System available for some time, it has expanded to all U.S. states. It was first launched in 2020 in California and uses sensors to detect tremors to help folks prepare for natural disasters and emergencies. For earthquakes with a magnitude of 4.5 or higher, Android sends warning alerts. These features will launch with Android 15.

If you missed our last General Meeting (Sep 4, 2024) then you missed the presentation on "AI and You" presented by Dr. Michael Lee from the UNLV Lee Business School. BUT, you can see the slides on our website, so take a look. Go to: https://computer.scaclub.org/

How to set up Apple Pay on an iPhone or Google Pay on an Android phone

We had a question regarding the use of mobile pay and whether was it safe to use. We answered that (look in our FAQs at the end of this newsletter). But here is some additional information which we thought might be useful for those who are interested in using mobile pay.

To set up mobile pay on one's cell phone, if desired:

iPhone

- Open Settings> Wallet & Apple Pay. Tap Add Card.
- Select either Debit or Credit card. If you have a physical card, position it within the frame on the screen and your iPhone's camera will attempt to scan the card details automatically. OR you can choose the option to Enter the Card Details Manually.
- Follow the on-screen instructions and provide necessary information (e.g. card number, expiration date and cardholder name). You might be asked to enter a verification code sent by your card issuer to verify your identity. Once you entered all of the required information, tap Next and Add Card to proceed.
- Your card issuer will verify the details and may require additional authentication steps (e.g. a one-time password or confirming your identity through their app or website). Follow the instructions provided by your card issuer to complete the verification process.
- Once verification is successful, your card will be added to your Apple Wallet and you can start using it for contactless payments. The card you enter will become your default payment method for new charges.

To make a purchase using Apple pay, use your default card.

- If your iPhone has Face ID, double-click the side button. If prompted, authenticate with Face ID or enter your passcode to open Apple Wallet.
- If your iPhone has Touch ID, double-click the Home button.
- Hold the top of your iPhone near the contactless reader until Done and a checkmark appears on the display.

NOTE: if you want to use a different card, (provided you added that to your Apple Wallet already) tap your default card to see your other cards. Tap a new card and authenticate.

Android phone (NOTE: the steps and options may vary depending upon your device, Android version and location)

- Download the Google Pay app from the Google Play Store and open up the app on your Android phone and sign in with your Google account. Make sure you are signed in with the same Google account you want to associate Google Pay with (in case you have multiple Google accounts).
- Follow the on-screen prompts to set up Google Pay. This includes agreeing to the terms and conditions and granting necessary permissions to the app.
- If your screen has screen lock enabled (e.g. requires a PIN, pattern or fingerprint) you may be prompted to set it up or use your existing screen lock for added security.
- Next you'll need to add a payment method to Google Pay. You have options such as:

How to set up Apple Pay on an iPhone or Google Pay on an Android phone

(continued)

adding a debit or credit card, adding a bank account or adding a supported mobile payment service.

- To add a debit or credit card, use your camera on your phone to scan your card information or manually enter the card details.
- To add a bank account (if your bank supports it), link your bank account to Google Pay for direct debit payments**.**
- Some countries and regions support payments from PayPal, Venmo or others. If available, your can link your account to these services by adding a supported mobile payment service.
- Once you've added your desired payment method, follow the prompts and provide any necessary information for your chosen payment method. This might include card details, bank account information or account credentials for mobile payment service. Now Google Pay will attempt to verify it. The verification process may differ depending upon which payment method you choose.
- After your payment method is successfully added and verified, your can use Google Pay for transactions e.g. in store payments at NFC-enabled terminals, peer-to-peer payments, and online purchases.

To use Google Pay for an in-store purchase

- unlock your phone's screen and hold the back of your phone near the contactless payment terminal or the NFC reader. Google Pay should automatically open and if it doesn't you might need to open the Google Pay app manually.
- Follow the instructions on your screen and Google Pay will communicate with the terminal to complete the transaction.

To use Google Pay for an online or in-app purchase

- Look for the Google Pay or G Pay button at checkout on the merchant's website or app and tap on it. It will then initiate the payment process.
- Verify the payment details and confirm the purchase using the authentication method set up for your Google Pay account. This might be your fingerprint, PIN or other security measures. Once the transaction is completed, you will receive a confirmation within the merchant's website or app.

To send money to friends or family

- Open the Google Pay app on your phone and look for the Send or Pay button. Enter the recipient's phone number, email address or select them from your contacts. Now enter the payment amount and any additional details requested by Google Pay.
- Review the payment details and proceed once confirmed.
- The recipient will receive a notification or email regarding the payment and the funds will be transferred from your linked payment method.

Once again the National Security Agency suggests

In our Jul newsletter, we mentioned that the National Security Agency (NSA) recommended rebooting one's mobile phone on a weekly basis. The NSA again has made this recommendation as a way to protect against zero-click exploits. What is a zero-click exploit? Well, it is a type of cyber attack in which the attacker uses malicious code and executes it on a device without requiring any user interaction. So it doesn't require someone to "click here" on a file or an embedded link.

So if it doesn't require one to do anything to enable it, how does it work? Good question! It works by taking advantage of any vulnerabilities in software, operating systems, apps, etc. Zero-click exploits have been identified in messaging apps, emails and network protocols. In recent news, they have been found in iMessage and WhatsApp messaging apps. They also were found in Apple's WebKit (the rendering engine for Safari), so when a user visited a malicious website, the user could be infected without even knowing. And zero-click exploits were also identified in some Android messaging apps.

How does one protect oneself against these exploits? Use common sense, which includes practices we talk about frequently such as:

- Keeping your software updated and limiting app permissions to those only needed for use with that particular app. And disabling features like automatic downloads for multimedia messages.
- Being cautious regarding clicking on links and attachments and never clicking on embedded links in emails, messages, etc. that someone you don't know sends you. And using different strong, unique passwords for your apps, websites, etc. Don't use the same one for each site and perhaps consider using a password manager or even passkeys.

NSA recommends regularly rebooting one's device to ensure any pending security updates are applied. Additionally, rebooting can temporarily clear temporary files and free up system resources. This could also help improve one's overall phone's performance. And restarting/ rebooting one's phone can disrupt any malicious software running in the background which makes it harder for it to persist. So why would you not want to reboot your phone on a regular basis? Too inconvenient as it takes a few minutes to do so? Is it not worth taking a few minutes out of your day to help provide more protection from unwanted viruses or malware? That is a personal choice one will have to make.

Help us help you

As a member of the SCA Computer Club, you have many benefits available to you. These include, but are not limited to access to our club's website, free classes, a monthly newsletter, general meetings with guest speakers who present intriguing information we may not have thought about, house call assistance with our computer issues or personalized teaching sessions, use of computers in our lab and classroom, opportunities to serve on our Club's Leadership team and opportunities to assist other members by volunteering time to serve as a club Monitor.

We are always looking for fresh ideas for our Newsletter, so please provide input via our website and Contact US. Want to be a Monitor? Contact US via the website, select President and you'll be given more information on Monitor training available and how easy it is to become one. We look forward to hearing from you.

Experimenting with ChatGPT 4o mini

Have you been interested in all the talk about AI this or AI that? Well, if so, you are not alone. We too have been curious to see how it works and only recently tried to use it. In full disclosure, the following is the results of our using one of the AI products available for free for the very first time. The product we used was ChatGPT 4o mini and we asked it:

"Can you write an article about what passkeys are, why one should use them, sites that enable them today and why they are better than using passwords." Here is what it came up with. What do you think?

Understanding Passkeys: The Future of Secure Authentication

In a digital world where online security is paramount, the traditional password is increasingly becoming a liability. Enter passkeys—an innovative authentication method designed to enhance security while simplifying the user experience. This article explores what passkeys are, their advantages over traditional passwords, platforms that currently support them, and why they should be your go-to choice for online security.

What Are Passkeys?

Passkeys are a modern replacement for traditional passwords. They utilize a cryptographic key pair—one public and one private— to authenticate users. Instead of a static password that can be stolen or guessed, passkeys dynamically generate secure credentials that are stored on your device. When you log in to a site or app, your device uses the private key to sign a challenge from the server, which can then verify your identity using the public key.

Why Should You Use Passkeys?

1. **Enhanced Security**: Passkeys are significantly harder to steal than passwords. Since they are not transmitted over the internet, there's less risk of interception during login.

2. **Phishing Resistance**: Passkeys eliminate the risk of phishing attacks that often rely on tricking users into revealing their passwords. Since there is no password to steal, even if a malicious actor attempts to impersonate a site, they can't obtain the necessary credentials.

3. **Convenience**: With passkeys, you don't have to remember complex passwords. They can often be accessed using biometric authentication (like fingerprints or facial recognition) or PINs on your device, streamlining the login process.

Cross-Device Compatibility: Many passkey implementations allow seamless authentication across different devices. For example, if you save a passkey on your smartphone, you can use it to log into your account on a laptop without needing to type in a password.

Sites That Enable Passkeys Today

As organizations recognize the need for stronger security measures, a growing number of websites and applications have begun to support passkeys. Some notable platforms include:

- **Apple**: Through iCloud Keychain, Apple users can store and manage passkeys across their devices.
- **Google**: Google supports passkeys on its services, allowing users to log in using biometric data.
- **Microsoft**: Windows Hello and Azure Active Directory support passkeys for secure authentication.
- **GitHub**: Developers can now use passkeys to authenticate their accounts, enhancing security for code repositories.
- **PayPal**: The payment platform has begun rolling out support for passkey authentication to streamline secure transactions.

Experimenting with ChatGPT 4o mini (continued)

Why Passkeys Are Better Than Passwords

1. **Reduced Risk of Data Breaches**: Passwords are frequently leaked in data breaches, exposing users to identity theft. Passkeys, however, are much harder to compromise, significantly lowering the risk.

2. **No Password Reuse**: Users often reuse passwords across multiple sites, making them vulnerable. Passkeys eliminate the need for this risky behavior, as they are unique to each site and device.

3. **Simpler User Experience**: Forgetting passwords is a common frustration. Passkeys streamline the authentication process, allowing users to log in quickly without needing to remember complex strings of characters.

Built-in Recovery Options: Many passkey implementations offer robust recovery options, so if you lose your device, you can still regain access to your accounts securely.

Conclusion

As cyber threats continue to evolve, the need for secure and user-friendly authentication methods is more critical than ever. Passkeys represent a significant advancement over traditional passwords, offering enhanced security, convenience, and resilience against phishing attacks. With increasing adoption across major platforms, now is the perfect time to transition to passkeys and secure your online presence. Embrace the future of authentication—your digital security will thank you!

Wow! How's that? What do you think? Be sure to provide your comments to us through our website at: https://computer.scaclub.org/ and select "Contact Us", then Newsletter and Next again. Provide your info and your comments in the Message box. We can't wait to hear your thoughts? Maybe we should start using AI to write our newsletters for us?

Digital Footprints

What are they? A digital footprint is anything you do on the Internet e.g. where you go, what you click on, what you buy, who you talk to, etc. And even things you don't do. An active digital footprint is the data that you intentionally share online and can include photos you post, comments you leave on a forum, information you provide when signing up for online accounts, etc. A passive digital footprint is what is collected about you that you might not even realize e.g. your IP address, your location, your browsing habits, your device information, etc. Remember that websites also use cookies to see what pages your look at and how you interact with content on each page.

These footprints can be used in Personalized Marketing and Ad Targeting by building profiles about you to predict what you might be interested in and then serve up ads for stuff you have shown an interest in online.

They can also be used to help keep your online accounts safe. How? Well, financial institutions may use your footprints to spot unusual activities. For example, if you normally log into your checking account from one location and all of a sudden, an attempt to login is made from a foreign country, or an unknown device, the financial institution may prompt for extra verification to ensure that it is you.

Potential employers may check out one's online presence in addition to looking at one's resume. And law enforcement can use digital footprints such as one's browsing history or online posts and location data to solve or track criminal activity. Details we share without thinking can end up as evidence for or against us in legal issues.

So think twice about posting on social media sites and accepting cookies when browsing websites. You can set your browser to delete cookies automatically after each session. They are other ways to help keep your information off the Internet and we'll write about that in November. Just another reason to read your Club's newsletter each month.

What file types are used to hide viruses? Here are five (5) used most often

Malware can hide anywhere...in emails, in text messages, in files and even embedded in websites and apps. There are certain file types that malware has been commonly found in and they are:

1) Executable files (EXE): these are used to run most programs on a Windows OS system. When opened they run code to launch a program or an installation package. If it is a clean EXE file there is nothing to worry about, but a malicious EXE file will install malware on one's system. You might have seen this before. You download what looks like a legitimate antivirus software only to find out it is a virus. A common tactic used by software developers is to trick you to install a software and when you do, your display indicates your computer is infected. Now they want you to pay for a fake virus remover.
2) Compressed Files: ZIP/RAR is another file type that often contains many files and the files within may be of different types. You have no idea what is in the ZIP/RAR file until you open it. Unfortunately, within the folder, there just might be a malicious file that you just activated. If you ever downloaded templates from a website, that might be the case. Files can be very large so they are compressed into a ZIP file to keep the size small so you can download it, then extract it. If there is anything malicious within, you have just extracted that too when you unzipped it.
3) PDF files is another file type used to hide malware. PDF files are common so they are often a target for phishing attacks. We get or look at PDFs all the time, even out newsletter comes to us as a PDF file. That doesn't mean it's harboring malicious malware inside of it. But some PDF files can be used to do that and can contain zero-day exploits. It is probably best not to download random PDF files from the Internet.
4) Script Files (JS, PY, SH): these are file types that contain commands that your computer uses to execute. JS or JavaScript is commonly used with web browsers. Other commonly used files among developers are PY or Python scripts and SH or Shell scripts. In order for scripts to run, one has to initiate it (usually by being tricked into clicking on something). For example, maybe you saw an offer to download some custom fonts for free and you wanted to try them. The download might come as a ZIP file and when you extract it, you see a .js file within. Thinking that is part of the free font package, you activate it and now the malware is in your browser. Be sure you understand what the implications could be before just randomly clicking on something.
5) Microsoft Office Files (DOC, XLS, PPT): oh no, you are kidding right? Nope, not kidding. All of us have probably used these files. Yes, they can carry dangerous macros (small programs embedded in the documents that automate tasks or are programmed to install malware). Office 365 files extensions can potentially contain malware, disguised as an Office 365 file. Again, think before randomly clicking to download or open files you are not familiar with or that are randomly sent to you by someone you don't know. If a file asks you to "Enable Macros", think twice before doing so.

It is best to run an antivirus scan on an EXE or ZIP file you download from the Internet. Tools like Microsoft Defender and Malwarebytes can help catch malicious file before they cause you nightmares. You just might want to disable Macros in Microsoft Office and only enable them if you are sure the file is safe and you know what the macro is supposed to do. Keep your software up to date and please don't click on anything you are not sure about. Many times we just have a feeling that something is off or clicking on something is not a good idea. Go with your gut and trust your feelings to avoid being duped.

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

that we made up ourselves

Q. I heard there was some type of website that I could go to in order to find manuals for some of my appliances. We just moved to SCA and in our new house there is the refrigerator, microwave and washer and dryer, all appliances in brands we never used before. The seller did not leave any manuals for them and it would be helpful if we had them. Any suggestions?

A. Welcome to Sun City Anthem and yes, this may help you. There is a website, Manualslib (the ultimate manuals library). You can access it by typing the URL (uniform resource locater, better known as the address of a web page) into your browser to get to it. The URL is: **manualslib.com** Then you can search for the manual by putting in your appliance's (name, manufacturer, model number, etc.) and hopefully it will locate that appliance's manual. Let us know if that helps.

Q. Many of my friends use Apple Wallet or Google Pay when we go out to eat. I always pay with my credit card or cash and they tease me about being "old fashioned". Is it really safe to pay with Apple Wallet or Google Pay?

A. Hmm, we're by no means experts but both Apple and Google take fraud prevention seriously and have security measures in place. When everything is digital, you don't have to worry about card skimmers and it is hard to fool facial recognition and fingerprint technology. Your actual card number isn't given to the merchant when using Apple Wallet or Google Pay. Instead of the bank card number, they receive a secure payment token tied to the verified card. Some say that this is safer than using your actual card. Having said that, using mobile pay is a personal choice. You just have to set up Apple Pay on your iPhone or Google Pay on your Android phone first in order to use it. Refer to the article on pages 5 & 6 for instructions.

Q. I hate being placed on hold when I call certain businesses just to get some information or an answer to my question. I heard there is a way to bypass this but I don't know what that is. Have you heard of such a thing?

A. We hear you. It is so aggravating when that happens, right? Perhaps you are thinking about a new Google feature, "Talk to a live representative" that is being tested by specific businesses. Some airlines use it, some retail stores are using it, some service and telecommunications are using it. It is similar to an AI-powered option (Hold for Me) that Google introduced for its Pixel phones back in 2020, but Talk to a live representative is supposed to available for more devices such as Android, Apple and also desktop computers using the Chrome browser. How does it work? Well, it places the customer service call on your behalf and when it gets to the front of the line, it gives you a call and hands over the conversation. And text message updates are available in the meantime. You'll get an estimated wait time when you specify the reason for your request when you first place the call. That's all we know. Again, it is currently being tested.

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

that we made up ourselves (continued)

Q. I have always wanted to travel but put it off for one reason or another, thinking I'll do it later. Well now is later and I have physical limitations that prevent me from doing so. I am a museum buff and would really like to see some famous ones I've read about. Is there a way to see them on my computer?

A. Great question! Yes, there is. You can "Google" a museum by name but even better, there is an app called **Bloomberg Connects.** This **app** works with iOS and Android, partnering with museums to offer guides to exhibits and collections. There are over 500 institutions from 23 countries that are available to be seen via the app. And its not just museums, but botanical gardens, zoos, theaters, etc. Want to see the Metropolitan Museum of Art or the Art Institute of Chicago, or the Guggenheim? If you download the app, let us know what you think about it. Another place you might want to explore is: artsandculture.Google.com which is a non-commercial initiative to bring the world's art and culture online so that anyone, anywhere, can enjoy. These are just two examples you can try. Remember, we here at the computer club do not endorse any particular products. We just provide information in our articles and in our FAQs. Providing such information (which is available on the Internet) is NOT an endorsement, just sharing of information to our members.

Q. I have recently bought a M4 iPad Pro and was just getting used to it when all of a sudden I can't use it anymore. I was trying to install the iPadOS 18 update and my iPad just turned off and won't turn back on. Any suggestions? Should I get a house call?

A. Oh, so sorry to hear that. A house call is not going to help you. Although Apple recently released iPadOS 18, a problem was identified that affected the M4 iPad Pro when trying to install it. Apple has confirmed a problem exists and has taken down iPadOS 18 until it finds a solution as it has not affected everyone who has that specific iPad. But since it apparently affected you, it is recommended that you return your iPad to the Apple store and they will replace it for FREE. Thanks to our computer club member, Alan Gerstner, who is also an Instructor and House call Technician who provided us this information in one of our Computer Talk sessions earlier this month. Computer Talk meets every Thursday at 9 am in the classroom and is a discussion group for all things computer related. Join us. Just don't ask about how to change a light bulb or what plants to put in your yard. But if you have a computer-related issue, we'll try to assist you with it.