Volume 24 Number 11 Nov 2024

# SCA Computer Club notes

## Classes for the Month of Nov

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.

**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.

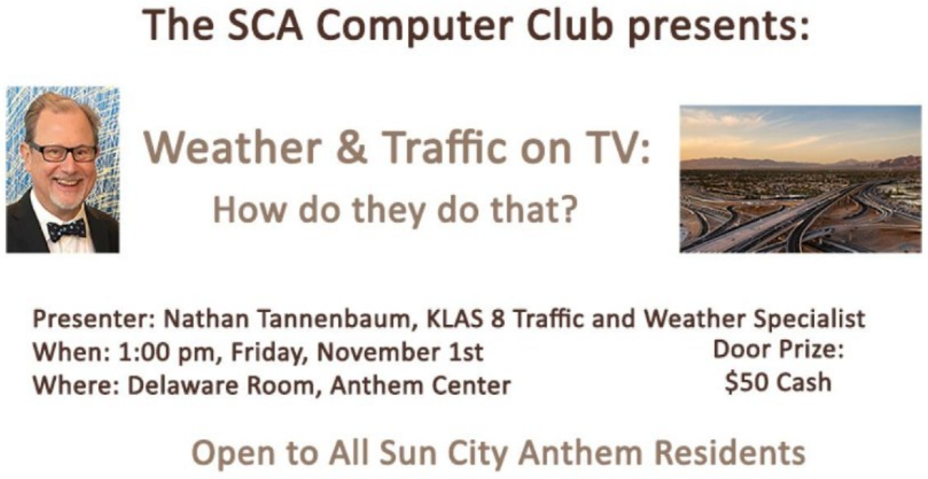
**Mac Photos – Part 1**: An introduction to Photos including how to connect you camera or memory card and how to organize your photos. How to create albums of selected photos and smart albums using several different search criteria. If time permits an introduction to location tagging and facial recognition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

**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.

**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.

**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.



**The SCA Computer Club presents:**

**Weather & Traffic on TV:**

**How do they do that?**

Presenter: Nathan Tannenbaum, KLAS 8 Traffic and Weather Specialist
When: 1:00 pm, Friday, November 1st
Where: Delaware Room, Anthem Center

Door Prize:
$50 Cash

**Open to All Sun City Anthem Residents**

## 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, Nov 9** from 10 am - noon.

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

### November is a busy month!

- Don't forget to vote on Nov 5th, if you haven't already.
- Veterans Day is November 11th, honoring all military veterans of the United States Armed Forces, both past and present.
- Computer Club computer auction, Nov 23rd. Look for details on the website.
- And of course there is Thanksgiving, Nov 28th, a time to share food with family and friends.

### Quick tips:

Want to browse in an incognito or private browsing window? Depending upon which browser you are in try, one can do so quickly by using the combination keys of Ctrl +Shift + N (if you are using Windows). Or if you are using a Mac, use the Cmd +Shift + N keys simultaneously. Using Firefox? Swap the "N" for a **P** instead. Remember, these modes won't make you completely private, but will stop from saving your searches, cookies, information you might have saved in forms you filled out while in the private browsing session, etc. When you close the browser the history and cookies, etc. are deleted. And if you bookmark a site or download a file, they will remain.

While using a smartphone you want to find that picture of your grandkid that your son sent you a month ago. You can scroll through your messages OR just open Messages, tap convo, then tap on the person's profile picture (in this case, your son). Now scroll to Photos> See All.

On an Android device (and it may vary depending upon which Android device you have), try opening Messages, then tap the search bar at the top, then choose the sender from the list of names. Or you might have to choose Known and then choose the sender (your son).

## Be aware of these latest Scams

We talk about scams frequently to keep you informed. Everyday something new surfaces and you should be aware to stay safe when you are using your computer, tablet, mobile phone, etc.

Do you use Gmail? Over 2.5 billion people do. You should be aware that there is a new, sophisticated phishing attack targeting Gmail users worldwide that uses advanced AI techniques, thereby making it harder to detect.

Here's how it works: Scammers send a fake account recovery notification and then follow up with AI-generated voice calls impersonating Google support. Don't be fooled. If you get an email telling you that you need to login to your Gmail account to reset its password, don't automatically do it. Think about it first. Were you having issues with your account? Did you request assistance or was this just an email out of the blue? Or if an email provides a phone number to call for assistance, don't use that phone number. Instead search for Google support's number from the Google site itself and ask them about it.

Some things to consider.

- Inspect the email address carefully. Is it associated with a Google domain? Did it have multiple addresses in the TO: line (other than yours)?

- Don't click on any links or attachments from unknown senders or suspicious emails. You can instead go directly to the website by typing in the URL into your browser.

- Be sure to have antivirus software installed on your devices. If you're running a supported version of Windows, you've already got Microsoft Defender Antivirus built in, helping to protect you against viruses, spyware, and other malware.

- Add another layer of security by using two-factor authentication (2FA), which requires a second form of verification (e.g. a text message or authentication app) that will make it harder for a scammer to gain access, even if they have your password.

- Don't forget to regularly monitor your accounts for any unusual activity.

Another scam is called **pig-butchering** and many times seniors are the target because they are lonely, perhaps looking for companionship, and are easily fooled due to their trusting nature. Don't become a victim, stay informed.

This scam is more involved and takes time to "fatten up the target". It's not clicking on a link, but involves establishing some type of relationship/friendship between the scammer and their victims. Many times these scammers are gangs or even prisoners working out of foreign countries. Here's how this scam works.

You meet someone online and start conversing with them. They seem "nice" and you exchange information about yourselves and you feel you have a lot in common. You might do this over a period of weeks or even months and although you've never really met them (and they seem really nice) you are starting to feel like you've got a new friend.

## **Be aware of these latest Scams** (continued)

And then he/she might ask for a favor. They may be needing a little money for a sick relative, a plane ticket to meet you, to fix their car, or even share with you an investment opportunity promising you great returns, etc. It may not be a lot of money and they promise to pay you back (but they never will). If it's an investment opportunity, they need it now or they'll miss that opportunity. There's a sense of urgency with their request and they need you to respond right away. Pig-butchering scams cost Americans $4 Billion a year and the scammers are all over Facebook, LinkedIn, WhatsApp and dating apps like Tinder and Bumble.

**Other scams** to watch out for include:

**Phishing** scams that are designed to appear urgent and timely, imposing deadlines or even threats. An email might say that your bank account has unusual activity and asks you to "click here" so that you can change your password. Don't do it! You could be sent to a fraudulent website that attempts to capture your login details.

**Shopping website** scams continue to rise and some might even trick you to install malicious software on your device. Check the website's domain name; look for misspelling, hyphens, etc. Search the Whois database at: https://www.whois.com/whois/ to check its authenticity and if the domain is newly registered, or if the website has suspiciously low prices, be suspicious.

**Virus and tech support** scams: ever get a pop-up that says "your computer has been infected" and to contact support? Think about it. If you call the support contact number a scammer will ask you to pay in order to "repair" your computer or to "remove" the virus. **Tech support fraud** was the **most reported cybercrime against those over 60 years old in the United States.** Over 18,000 complaints to the Internet Crime Complaint Center were reported in 2023.

**Lottery and Prize** scams get your hopes up. Scammers impersonate government institutions or well-known organizations to make it seem like you won. Again, there's that sense of urgency or limited-time offer in which you need to act. You might even get a fake check and then you are asked to return some of the money. Don't deposit that check. Contact your bank immediately.

Keep these tips in mind so you do not become a victim:

- Double check the sender's email address. Scammers often have strange email addresses or slight variations or misspellings of legitimate domain names. Don't trust caller ID either.
- Ignore unsolicited texts from an unknown social media account or number. If you answer them, they'll keep contacting you and 9 times our of 10, it's a scam. If that happens, block the number. Better yet, don't answer. Just delete the text.
- If you do text with someone new, don't overshare personal information, especially if they are quick to profess their strong feelings for you. Seniors especially are taken in by scammers pretending to "care" or "really like" you (when they don't even know you).
- Scammers take advantage by creating a sense of urgency or frightening older folks, e.g. "we think your bank account has been comprised and you need to move your money now or lose it all". Never overreact. Call or go to your bank. Don't trust any number they ask you to call.
- Use email filters to help detect and block phishing attempts.

## **Be aware of these latest Scams** (continued)

If you have any doubts, discuss it with a trusted friend, neighbor, son/daughter and get their opinion on the situation or the “opportunity” before “being scammed”.  And if you do become a victim, don’t be ashamed to report it!  You can file a report with the FBI through the Internet Crime Complaint Center (IC3).

There are multiple ways to stay informed and educate yourself.  Besides reading articles you can learn things right here at your Computer Club.  We offer classes (check our monthly calendars on our website).  There are also discussion groups such as Computer Talk and Apple Talk where you can ask questions and learn things.  Take advantage of your membership and use these benefits.  And of course, there is the House Call program if you need assistance.  Don’t be a stranger.  Come to the club and use our equipment and learn a thing or two.

## New in iOS 18

There’s a new **Passwords app** that was recently introduced in iOS 18, used to simplify password management for Apple product users and allows users to store and manage passwords, authentication codes, and passkeys in one place.  It offers biometric authentication for added security and syncs passwords across multiple devices, e.g. iPhones, iPads, Macs, and Apple Vision Pro. This ensures that passwords are easily accessible and auto filled when needed.

Apple's Passwords app is designed to simplify and secure password management on your devices. Here's a quick overview of how it works:

- ***Centralized Storage***: The app pulls together all your login information, including passwords, passkeys, Wi-Fi networks, and more, into one place.
- ***Biometric Authentication***: For added security, the app uses biometric authentication like Face ID or Touch ID to ensure that even if someone else has your unlocked phone, they can’t access your passwords.
- ***Sync Across Devices***: Passwords syncs across all your Apple devices (iPhones, iPads, Macs, Apple Vision Pro) making your passwords accessible and auto fillable wherever you  need them.
- ***Security Alerts***: The app alerts you to potential security vulnerabilities, such as easy-to-crack passwords or reused passcodes across different platforms.
- ***Password Generation***: It can create randomly generated passwords to help you avoid reusing the same login information for multiple accounts.
- ***Verification Codes and Passkeys:*** You can also store verification codes and passkeys for two-factor authentication.

**To get the Passwords app,** you'll need to update your device to iOS 18 or later. Once updated, you can find the Passwords app on your *Home Screen* or by using the *Spotlight Search*.

**To start using it:**

- Open the Passwords app from your Home Screen or Spotlight Search.
- Authenticate using Face ID, Touch ID, or your passcode.
- Enable Notifications: The first time you open the app, you'll be prompted to allow notifications for password changes or breaches.
- View and Manage Passwords: You can see all your saved passwords, passkeys, Wi-Fi passwords, and verification codes. To add a new password, tap the "+" icon, enter the website and username, and iOS will suggest a strong password.

## Things you might want to know (or not)

Do you use an Echo device? Are you ever annoyed when it repeats what you said? Well, good news. You can turn off that default setting by going to your Alexa app, tapping More> Settings> Voice Responses and then turn off Brief Mode.

Do you get tired of apps asking for ratings? If you use an iPhone, go to Settings> App Store and toggle off In-App Ratings and Reviews. Using an Android phone? Don't be upset, but there's no fix for that right now.

Don't you love auto-correct when trying to type an email to your family or friends? It's especially fun when it keeps correcting words that you *actually* want to use, right? NOT! But did you know that you CAN add custom words that you use that won't get autocorrected? On an Android device, go to Settings> System> Keyboard> Personal dictionary. Using an iOS device, go to Settings> General> Keyboard> Text Replacement.

Ever put apps on your mobile phone's home screen. Is it now cluttered? Why not just create folders by categories? You can do that on a phone's home screen. Just drag one app on top of another to make a new folder. You might have one for shopping apps, Google apps, productivity, social media, etc. Give it a try if you need to clean up your home screen.

Ever spend minutes typing away on your keyboard and all of a sudden poof! Everything just goes away? Oh, no. What just happened? Try to hit undo that to see if it returns. How? On a Mac, use the combination keys of Cmd + Z and on Windows, use Ctrl + Z.

Did you know that there has been a major update to Microsoft Copilot, which includes a radical redesign and several new features? Why? The update aims to make Copilot more intuitive and competitive with other AI platforms like ChatGPT.

Some of the key updates include:

- Copilot Voice: This feature allows for smoother and more natural conversations with the AI, making it feel more like talking to a person.
- Copilot Daily: A new feature that provides daily summaries of news and weather, with plans to include reminders and personalization options.
- Think Deeper: Designed to help with complex decisions, like choosing a city to move to or the best type of car for your needs.
- Improved Windows Search: Enhanced search capabilities for more detailed answers to user queries.
- Card-Based Design: A new user interface that offers options based on the time of day and more.

# Deepfake Technology: what is it?

Technology is embedded into our lives whether we want it or not. You probably use it to converse with your children/grandchildren, friends, etc. via a mobile phone, computer, laptop, etc.? Do you Facetime your relatives? Do you put appointments on your calendar on your phone?

By now you have heard about Artificial Intelligence (AI) and it is getting a lot of publicity everyday as it is used in just about everything from logistics, medicine, banking, shopping, technology, etc. Please don't take the attitude that AI "is not for me" and just ignore it as it is being embedded in everything you do. It is not just for those "other generations" so you need to at least be aware of what it is, how it is used and most importantly, repercussions from its use that can affect you.

Which leads us to ***Deepfake Technology***. Deepfake technology uses advanced artificial intelligence (AI) to create realistic-looking, but FAKE images, videos, or audio recordings by manipulating existing media. It works by training algorithms on vast amounts of data, allowing them to replicate a person's likeness or voice convincingly. It manipulates visual and auditory elements to make it seem like someone said or did something they never actually did. Think about a digital puppet show where someone's face or voice can be convincingly mimicked to say or do things they never actually did.

Deepfakes can be used for various purposes, from harmless fun like creating entertaining videos to more serious, deceptive uses such as spreading false information or manipulating people. So there are potential dangers associated with deepfakes, notably their use in misinformation, identity theft, and political manipulation. And this is why you need to be aware, so it doesn't take advantage of you.

What possible malicious purposes can deepfakes be used for? Seniors are particularly vulnerable to scams and misinformation. Deepfakes can be used to trick them into believing false information, manipulating them into giving away personal information or even convincing them to send money.

While deepfake technology can be used for entertainment (as in movies and television) to enhance storytelling or digitally recreate performances of actors, or used in social media (to create humorous or parody content by swapping faces in videos, for fun or satire ) or, even in education and research for training simulations and educational purposes, there is the potential for manipulation for nefarious purposes. Here are some examples:

***Misinformation***: False news reports can be created, making it difficult to discern fact from fiction. Don't believe everything you hear on the news.

***Fraud and Identity Theft:*** Deepfakes can impersonate individuals to deceive others, potentially leading to identity theft or you might have heard about someone receiving a fake call from a "grandchild" asking for emergency financial help to get out of jail or to fix their car or to continue their college education. What about someone impersonating a healthcare provider giving false medical advice or asking for your Medicare number to send you a cane or walker that you need?

***Harassment***: Individuals can be targeted with fabricated content that could damage reputations.

***Scams***: Fraudsters use deepfakes to impersonate people, such as family members, friends, bank employees, or government officials, to trick victims into giving them money or sensitive information. They can also use deepfakes to create fake identities, such as phony ID credentials.

Fraudsters can use deepfakes as an extortion gimmick by creating phone calls that sound like a family member in distress, and then use that to exploit the victim's emotional state.

And this is why **you** need to be aware. Again, ***seniors are particularly vulnerable to scams and misinformation.*** Don't be that senior who gets scammed. So **how do we protect ourselves?**

## **Deepfake Technology: what is it?** (continued)

***Be Skeptical*** and ***Verify Sources***: Always check the authenticity of information from trusted news outlets. Verify unexpected or unusual requests for money or information, especially from phone calls or videos.

***Double-Check Sources***: Cross-reference information from trusted sources before believing or acting on it.

***Use Technology***: Install security software and use services that help verify the authenticity of emails, calls, and videos. Security software and emerging detection tools can help identify deepfake content.

***Education***: Keep learning about the latest technology and scams to stay ahead. Take advantage of the classes offered at your Computer Club. Let us know if you want classes on a certain topic. If enough members request it, perhaps we can provide instruction or it might be a topic for discussion at Apple Talk or Computer Talk.

***Look for Inconsistencies***: Pay attention to unnatural movements, audio mismatches, or discrepancies in visual quality that might indicate manipulation.

***Promote Awareness***: Educate others about the existence and potential risks of deepfakes to build a more informed community. Tell your neighbor or friend if you hear about a scam being circulated. Or ask your neighbor or friend about their opinion if you suspect a scam email or text you received, especially if it involves you providing money or providing your credentials or letting someone remote into your computer in order to help you.

By staying informed and cautious, we can protect ourselves from being manipulated by deepfakes. Understanding deepfake technology is essential, as it presents both innovative possibilities and serious challenges that require vigilance and critical thinking. Don’t ignore it; become aware and stay safe.

## Is 4G better than 5G? And what does that even mean, 4G, 5G?

**5G** is the fifth (5th) generation of the technology standard for cellular networks; the technology that provides connectivity to most mobile phones. 4G technology became commercially available around late 2009, offering significantly faster speeds and better mobile web access compared to 3G. And 5G technology began its rollout in 2019. Some of the key differences between them include:

- **Speed**: 5G offers significantly higher speeds compared to 4G, with potential download speeds up to ten times faster.
- **Latency**: 5G has much lower latency, meaning data is transmitted with minimal delay, which is crucial for real-time applications like online gaming and video calls.
- **Bandwidth**: 5G can support more devices simultaneously due to its higher bandwidth, making it more efficient in crowded areas.
- **Coverage**: 5G uses a combination of low-band, mid-band, and high-band frequencies to provide more reliable coverage, even in rural areas.
- **Energy Efficiency:** 5G is more energy-efficient than 4G, which can lead to longer battery life for devices.

And 6G? It is still in development. Industry experts estimate it may be available in 2030 and of course it will include yet faster speeds, lower latency and more advanced features that we currently have in 5G.

So, is there a difference between 5G and Wi-Fi 5? Excellent question. Yes, there is. See the next page.

## 5G and Wi-Fi 5. Are they different?

As we mentioned, 5G is a **cellular network** used by mobile carriers, that offers wide-area coverage so that mobile phones have connectivity to the Internet. It allows mobility, allowing one to stay connected whether in a car, train, or just walking around the neighborhood.

***Wi-Fi 5* on the other hand**, is a ***wireless network technology*** we use in our homes, offices and other public places (although it's best to think twice before connecting to the Internet) using a coffee shop's network or a café's network, or the airport or other venues in public places.

Wi-Fi 5 (802.11ac) as it is called, provides local-area coverage with the range of a single building or a home for instance. If offers speeds up to 1,300 Mbps, which is pretty fast, but generally slower than 5G. Additionally, it has a lower latency compared to older Wi-Fi standards but higher latency that 5G and one needs to stay within the range of the Wi-Fi network to maintain connectivity. So in essence, 5G is designed for wide-area, high-speed mobile connectivity and Wi-Fi 5 is optimized for high-speed local-area access in more confined spaces.

And Wi-Fi 6? That is now available and it started rolling out in 2019. It offers improvements over previous Wi-Fi standards, like higher speeds, better performance (in crowded areas, like apartment buildings, etc.) and improved battery life for connected devices.

Depending upon your carrier, you might be able to get it. AT&T offers it through their Fiber multi-gigabit plan (if you have fiber available in your neighborhood). Verizon now provides Wi-Fi 6 routers to their Fios Internet customers, including a Wi-Fi 6 home router. And Comcast recently announced plans to offer Wi-Fi 6 as part of its network upgrades as it wants to provide multi-gigabit symmetrical speeds to its customers. Don't forget about Cox. It too offers Wi-Fi 6 through its Panoramic Wi-Fi service. It's gateway is an all-in-one modem and router that supports Wi-Fi 6. So if you are interested in getting W-Fi 6, check with your carrier to see if it is available.

Wi-Fi 6 works better in congested areas with a large number of users, e.g., airports, stadiums, or educational settings. These areas sometimes inhibit a user's ability because they are competing for bandwidth and multiple overlapping networks interfere with each other. Wi-Fi 6 is supposed to improve throughput by up to four (4) times over that of Wi-Fi 5 in such areas. And at home, one might have competing devices, like smart devices, phones, tablets, television, etc. that compete for bandwidth too. So Wi-Fi 6 handles that well, and of course if you stream movies or use video conferencing, Wi-Fi 6 will support that too. And now you know.

---

## Something new to try? Try this

- Ever have your monitor just go blank? Try this before shutting it down and restarting it. Use the combination keys of the Windows key + Ctrl + Shift + B to see if it brings it back. Why? Because this tell your computer to refresh or reset your graphics driver and that may be all you need to do.
- On a Mac, here's a quick way to close a window or even quit an app. To close a window, simple use the combination keys of Cmd + W and to close an app, use Cmd + Q. No more having to move the mouse cursor to the red dot and click on it to close or quit an app. Such a time saver.
- Do you write articles for the Spirit magazine? Do you provide product reviews where there is a limited word count? Do you use Google Docs? If so, use the combination keys of Ctrl (or Cmd if using a Mac) + Shift + C to check the word count of your article/review/document. The pop-up also has a checkbox to show the word count on your screen permanently.

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

that we made up ourselves

***Q. I have a Windows 10 PC and I heard that it is no longer supported and I have to go and buy a new PC. Is that true?***

**A.** No, not exactly. Microsoft will *officially end support* for Windows 10 on November 14, 2025. This means that there will no longer be any more "free" updates, security fixes or tech assistance. You can pay Microsoft for extended support, or upgrade your computer to Windows 11 (if it is capable of doing so), buy a new computer (if yours cannot be upgraded) or continue to use your computer as is. If you continue to use your computer with Windows 10, (which is fine) you will continue to get support until Nov 2025. After that date, it is recommended that if you continue to use your computer, use it offline, e.g. don't shop online or bank online as you may become susceptible to malware, viruses, etc.

***Q. I recently tried to purchase a bicycle for my grandson from an online website. When I went to finalize the purchase, I got a message that said "card declined". I know my card was good, but instead of checking it out with the card issuer, I used a different card and the purchase went through. This month I received my statements and BOTH of my cards were charged for that bicycle. How does this happen?***

**A.** Unfortunately, you were scammed. The Better Business Bureau (BBB) recently warned the public of this scam which is increasing, especially now that the holidays approach. One tries to buy something online, but one doesn't realize that the website was faked. When one gets the "card declined" or "your card did not go through for some reason" message, one simply pays with another card. Then the charges appear on both cards. When shopping online, be sure the website is legitimate. Check its URL (it may be off by a letter or two) and make sure it is secure (look for the closed lock symbol) and/or that the URL begins with "https://" in front of the website name. One can check a website by searching for it on BBB.org. If you are scammed, report it through the BBB.org website. Look for the "***BBB Scam Tracker***", so others aren't scammed.

***Q. My daughter recently gave me a new iPhone that she said she got really cheap on the Facebook Marketplace for only $50. I suspect something's wrong but I don't want to hurt her feelings as her intention was good. How can I check to see if the iPhone is legitimate?***

**A.** Excellent question! Before you use the phone, check its International Mobile Equipment Identity (IMEI) number. Dial *#06# on the phone to display the IMEI number. Copy the number and go to "stolenphonechecker.org/spc/consumer" and enter the number to see if the phone was reported lost, stolen or blocked by the carrier. When something is really cheap or too good to be true, it usually is not the real product one thinks it is. Always better to check, than to be taken advantage of. Don't be fooled!