Volume 24 Number 06 Jun 2024

SCA Computer Club notes

Classes for the Month of Jun

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

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 you day to day life with your devices easy as pie.

Monitor Training-Refresher: Refresher course for current Monitors.

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.

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.

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.

Monitor Training-New Monitors: Training for new Monitors. 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.

Your Computer Club Board will meet on Tuesday, Jun 11, 2024 in the Classroom at 1:30 pm. Any member in good standing may come and listen to the Board's discussions. Attend and maybe you will become interested in running for the Board next year. We always welcome new ideas to improve our Club.

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 meetings are on **Saturday, Jun 8** from 10 am-noon and **Tuesday, Jun 18** from 10 am-noon.

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

Reading Mode

Are you tired of seeing all those ads on a website page when you are just trying to read an article of interest? If so, why not invoke "Reading Mode"? Reading mode eliminates the ads and is enabled on a per-page basis. So how do you invoke it? Depending upon which browser one is using, here are some suggestions:

Chrome browser: open a web page and point to the web page you'd like to view in Reading Mode. Right-click on a blank section of the page and select "***open in reading mode***" from the context menu and a sidebar appears with the content in reading mode.

Safari browser: open Safari and point it to a web page you'd like to view in Reading Mode. On the far left side of the address bar, there should be a small icon (like a page of paper). Click on it, but be aware that the icon may disappear after a few seconds, so you have to be quick. A nice thing about the Safari browser is that with certain sites, one can automatically open pages within Reading Mode.

Edge browser: open Edge and point to a page you'd like to view in Reading Mode. It is called **Immersive Mode in Edge**. Near the right edge of the address bar there should be a small book icon. Click on it.

Firefox browser: open Firefox and point to a page you want to view. Near the right side of the address bar edge, look for the "***Reading View***" icon and click on it. ***Note:*** *the difference between Firefox and Safari is that the icon in Firefox* ***does not*** *disappear after a few seconds.*

Data Tracking

Companies use “data tracking”, the collection of information about a user’s online activities such as browsing history, location data, messaging information, app usage, etc. How is it used? The company uses it (or shares it with third parties) to tailor advertising to you, even though they may claim they use if tor “improving services” to you. If may look different from one company to the next, but let’s just look at mobile carriers, as they collect quite a bit of information (and most folks have and use a cellphone).

T-Mobile analyzes personal data to predict user preferences and behaviors which can influence future services and marketing strategies. They share data to aid both public and scientific research initiatives (claiming that personal identifies are removed). But they also track how often and how long an app is used to gain insight into a user’s preferences and all of this is used to tailor advertisements closer to the user’s interests.

Verizon uses data like web browsing and app usage to offer additional services or upgrades and to offer a more “personalized” service experience. Combining user data with external data, they can generate insights into consumer behaviours and trends to personalize marketing efforts and service offerings.

AT&T collects both user browsing and location data to customize offers and ads. Employing algorithms, they are able to collect data to make automatic decisions regarding which ads or content is presented to the user. They also collect demographic info to better understand their user base and share certain data with third parties to facilitate identity verification and fraud prevention measures.

If this bothers you, you can better manage your privacy and data and disable data tracking. How?

T-Mobile: Log into your account and click on ***Profile***. Scroll to the bottom and select ***Privacy and Notifications***, then ***Privacy Dashboard***. Toggle off the various options such as *Share Data for public and scientific research, analytics and reporting, advertising options, profiling and automated decisions* and opt out of *data usage for profiling purposes*. Also, be sure the *Do Not sell or share my personal information* is checked.

Verizon: Log into your account, go to ***Account> Account Overview*** and select ***Edit Profile and Settings***. Choose ***Manage Privacy Settings***. Opt out or disable *customer proprietary network info, business and marketing insights, custom experiences and custom experience plus*. Resetting the *Custom Experience settings* will also stop Verizon from using previous collected browsing and location data.

AT&T: Log in and go to ***Profile> Privacy Choices***. Toggle off *Personalized Plus, Personalized, and Share or Sell my personal information*. It is recommended to keep identity verification active for security purposes.

Customizing Windows 11

Did you know you can customize Windows 11 to make things more accessible? Most folks know about realigning the Start Button from the center to the lower-left corner and using the Widgets button to see newsfeeds, weather, top stories, etc. But here are a few others one might be interested in.

Windows 11 Phone Link app: lets one wirelessly connect one's phone so that any phone notifications appear on one's PC, as well as allowing one to reply to text messages, make calls on the computer, etc. With an Android phone, one can access photos on the phone, use it as a Wi-Fi hotspot, play music or even run phone apps on one's computer screen.

Are you writing your club's minutes or emailing your friends or family and messages or video chats pop up? What a distraction, right? Well, how about using ***Focus Sessions*** which allow you to set aside an amount of distraction free time? ***Start the Alarms & Clock app, select Get Started and pick a number of minutes for your Focus Session.***

Add tabs to File Explorer by right-clicking on a folder choosing ***Open in New Tab***. You can also drag a file between tabs by dragging it to the desired tab and then down into the file list for that tab.

Customize your Start menu. Go to ***Settings> Personalization> Start> Folders***. You can then add File Explorer, other folders, network icons, etc. to your Start menu. The icons will appear along the bottom edge next to the Power button.

Looking to see information regarding your ***battery usage***? Go to ***Settings> System> Power & battery*** and open the Battery usage tab to see a chart that show how much power has been used. It also shows power usage by individual apps so that if an app is using too much power, you can shut it down or put it to sleep.

Have you discovered other tips using Windows 11? If so and you want to share them, contact us via the website. Select Newsletter and let us know so we can pass it along to other members of our Club.

Checking to see if a Link is Safe or not

Before clicking on a link, it is wise to see if it is really safe or not. Ransomware is spread by people unwittingly clicking on dangerous links in email, texts, social networks, etc. where ransomware was embedded. So how can one be sure a link is safe? Here are a few tools that can help.

ScanURL, an independent website, that uses a secure HTTPS connection, polls Google Safe Browsing Diagnostic, Phish Tank and Web of Trust to indicate whether a site is safe or not.

PhishTank, operated by OpenDNS, lets you know if a link is safe or if it will send you to a phising site. Enter the URL and if the link is "already in the tank" you'll get instant results.

Google Transparency Report can identity phishing risks as well as malware. Phishing is potentially a greater concern than malware.

VirusTotal URL Checker offers a browser-base multi-function scanning tool that analyzes suspicious files and URLs to detect types of malware.

SiteCheck can scan websites for security issues including malware, viruses and malicious code. Minimal or Low Security Risk means the site is safe.

Psafe Dfndr Lab will check a URL and if found in their database, it will display whether or not one can trust it. If the site is not found, you'll be encouraged to exercise caution and if you are not 100% confident in the URL or website, you should NOT click on it.

Voice Authentication and why you might not want to use it

Voice authentication (aka voice recognition) is a form of identifying someone based on one's voice, a biometric characteristic. It requires one to repeat a passphrase, multiple time to enable the system to establish a unique voiceprint. Once established, the characteristics of one's voice, e.g. pitch, tone, pronunciation, etc. is analyzed to determine whether the speaker is authentic. One's voiceprint can then be used like a password to enter certain websites, accounts, etc. Instead of typing in a password, one simply speaks a phrase, the system checks it against one's stored voiceprint and if it's a match, one is in.

Sounds like a good deal, eh? A lot easier than remembering an eighteen (18) alphanumeric password or passphrase, right? Well, here is something else to consider. While it sounds like it is an easy way to authenticate in order to log into one's account or specific website, the introduction of artificial intelligence (AI) has made it susceptible to deepfakes and synthetic media attacks. Hackers can leverage machine learning-enabled deepfake software in order to generate copies of a victim's voice using minimal recorded audio that is convincing. Imagine, an AI generated voice that sounds just like you and it is used to fool most voice authentication systems.

An example of a deepfake or synthetic media is a digitally manipulated video, text, image and sound (e.g. one's voice) that is used to replace one's likeness. In other words, a deepfake can be created to sound just like one's voice and then used to compromise one's log in credentials. And although currently, deepfake creators are spending more time on creating fake video images, more and more are focusing on fake audio as a means of stealing a person's account information. And AI generated fraud is harder than ever to detect and stop.

So what can one do to protect one's self? First of all, be aware. Now that you know voice cloning exists, and one's voice can be recorded during a phone conversation, be cautions when sharing personal information or speaking to strangers on a call. Some folks always answer their phones whether or not they recognize the caller. The caller could be recording one's voice, asking for personal information or verification codes or stating they are from a known company, e.g. IRS, USPS, Amazon, one's banking institution, etc. And it could just be a scam, trying to get one to speak so their voice can be recorded. Better not to answer calls from unknown callers (or numbers) and let them leave a voicemail. If it is someone that one knows, the caller will probably leave a message and one can call them back.

Two-factor authentication is an added layer of security because it requires a second form of verification, e.g. a code sent to one's phone, in addition to a password/passphrase. It has been around now for a while and a good idea to use it, if you don't already.

And of course, use strong passwords/passphrases and don't use the same one for multiple accounts (just because you think it is so strong). Also, remember to keep your software up to date. One should regularly update one's operating system, antivirus software, web browsers and other applications one uses to ensure one has the latest security patches and protections. Many browsers will update automatically, as well as operating systems, if one chooses to allow that. Check your settings for automatic updates. Lastly, one can also invest in identity theft protection services that will monitor one's personal information, social security number, phone number, email address, etc. so that if one's information is breached, one will be notified. That may not be necessary if one takes precautions (such as those mentioned above) but that is a personal decision.

As technology advances, so do the hackers, so be safe. Keep your systems up to date and stay aware of current threats and how to protect yourself. Utilize your Club membership privileges to stay informed via Computer Talk, Apple Talk, the various classes offered and your monthly newsletter.

Is your Microsoft OneDrive Storage getting low? Want to free up space?

Do you use OneDrive to store your files, photos, email attachments, etc. How much storage are you getting? Have you received a message indicating your account is running our of space? What can you do? Here are some suggestions to help if you need more storage capacity.

First of all, if you use the web version of Microsoft OneDrive (or the free cloud storage) you are offered 5 GB of storage space for your email attachments, files and photos. If you use Outlook.com, you get 15 GB of free mailbox storage for your emails, contacts and calendar items.

If you have a Microsoft 365 subscription, it depends.

- For a Microsoft 365 Basic, you get 50 GB of free mailbox storage for your Outlook.com emails, contacts and calendar items and 100 GB of free cloud storage for your email attachments, files and photos in OneDrive.
- As a Microsoft 365 Personal subscriber, you get 50 GB of free mailbox storage for your Outlook.com emails, contacts and calendar items AND 1 TB of free cloud storage for your email attachments, files and phots in OneDrive.
- A Microsoft 365 Family subscriber (you and up to five (5) other people) get 50 GB free mailbox storage for your Outlook.com emails, contact and calendar item AND you each get 1 TB of free cloud storage for your email attachments, files and photos in OneDrive.

If you are running out of space, your can either buy more storage or clear space by deleting unused files, or removing large email attachments, or emptying the recycle bin or relocating data.

If your subscription expires, your account will automatically revert to the free version 5 GB of storage) and you'll get a notification about low storage. To check your account, log in and go to "***Services and Subscriptions***" on the left sidebar to see if your account is still active. If it isn't, you'll need to reactivate it by clicking the "***Resubscribe***" button and following the instructions.

Since the storage space used for Outlook attachments **ALSO** counts towards your overall quota in Microsoft 365 (free or paid), it might be using a lot of your space. You can check to see how much it is using by logging into your Outlook account and clicking on the gear icon in the top-right corner to open "***Settings***". Then go to the "***General***" tab on the left sidebar, click on "***Storage***" to see how much space your Outlook attachments are using. If it is a lot, click on the "***Outlook (Attachments)***" link and you will see the emails with large attachments. You can delete them or download them to local storage to free up space.

How about deleting files from your OneDrive storage that you no longer need? Once deleted, they go to the OneDrive Recycle Bin (and stay there for 30 days). If you change your mind, you can restore them during that time . Remember that they still count towards your storage space while in the Recycle Bin, so if you don't need them, delete them from the Recycle Bin to free up more space.

When you make changes to a document stored in OneDrive and save it, OneDrive saves that version (e.g. it does not overwrite the original). Each time you make changes, a new version is saved, so deleting older version can free up space. But you need to do so using File Explorer. Go to your **OneDrive folder**, right-click on the file, select "***Show More Options***" to open the classic context menu and then select "***Version History***" to manage the file's versions. You'll need to click on the three vertical dots next to the version you want to delete and select "***Delete***" to free up space.

Is your Microsoft OneDrive Storage getting low? Want to free up space?

(continued)

Do you automatically configure your OneDrive to back up standard folders, e.g. Documents, Pictures, Desktop, Music, Videos, etc.? That can take up a lot of storage space, especially if they contain large files and you frequently add new data to them. You might consider moving their content to another location on your computer OR downloading then to a local storage device OR stop automatically backing them up. To stop the backups, click on the OneDrive icon, select the gear icon and click on "***Settings***". Go to the "***Sync and Backup***" tab, select "***Manage Backup***" and then turn off the toggle next to the folder you no longer wish to back up. Lastly, click on "***Stop Backup***" to confirm your choice.

How about just deleting unused data from your OneDrive? To locate large files and folders go to the "***My Files***" tab and click on the "***File Size***" column header to sort files from largest to smallest. Delete those large files you no longer need. You can also open folders that have the most space, arrange the files within by size and determine if you really need to keep them. If not, delete them. And don't forget your Photos tab. You might choose to delete those you no longer want, or duplicates, or blurry ones you saved (and didn't realize it), etc. Once deleted, remember to go to your Recycle Bin to empty it to free up space.

Lastly, if you've identified large files (and you decide you do not want to delete them) you can move them to your local storage or transfer them to another cloud storage service. To download them, ***click on the three dots next to the file or folder***, then select "***Download***". After downloading, double-check to ensure you have them and ***THEN*** delete them from your OneDrive and your Recycle Bin to free up space.

There you have it; a few suggestions to try to free up space on your OneDrive account if it is getting full. Let us know if any of these suggestions help. Contact us via the Computer Club website. Choose Contact Us from the main menu, select "Newsletter" and provide your input. We appreciate hearing from you.

Pushing advertisements to Windows 11 users is something Microsoft started doing in its Start Menu. The ads are "recommended" software encouraging one to download more apps onto one's PC and/or tablet. But what if one doesn't want this? Well, here's how to disable them. Simply go to ***Settings> Personalization> Start*** and toggle off the button next to "***Show recommendations for tips, app promotions and more***".

Night Shift on the iPad. What is it? If you use your iPad at night, you might want to consider using Night Shift, which has warmer colors and supposedly makes it easier on one's eyes to read when one is in low light environments or when it's dark out. To see what it is, go to ***Settings> Display & Brightness> Night Shift***. Here one can manually turn it on, schedule it to turn on during certain times and adjust how warm one wants the display to be.

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

that we made up ourselves

Q. I have an iPhone and when I charge it, it never fully charges 100%. Normally, it charges to about 80%. What is wrong with it?

A. Actually, nothing. It could be because it has a feature that is called "Optimized Battery Charging" that is intended to prevent over-stressing the battery. This could also extend one's battery life because it prevents the battery from reaching a full 100%charge. It is effective if one maintains a regular charging cycle (like when plugging in one's phone every night when going to bed) because it ensures the phone is fully charged right before one wakes up, reducing strain on the battery. Some even say that charging one's device to 100% stresses the battery. We don't know if that is true or not, but batteries do go bad after a period of time. Unplug your devices after they charge (to 80% or 100%) and don't leave your laptops, phones, tablets, etc. continuously plugged in as that too can affect your batteries performance.

Q. I recently updated my iPhone to iOS 17 and now I get a notice to update to iOS 17.5.1. It is really necessary to update so soon?

A. Apple updates (as well as other OS updates) range from adding new features, updating or improving features to installing needed security patches/updates. Regardless what phone type you use, it is a good idea to update (especially security patches) when they become available. It the case of iOS 17.5.1, it provided important bug fixes and addresses a rare issue that was discovered where photos that experienced database corruption could reappear in the Photos library even if they were deleted. In simple terms, some folks experienced having old photos (that they had previously deleted) show up in their Photo library all of a sudden. This didn't happen to everyone that updated to 17.5, but enough that Apple rather quickly put out 17.5.1 to fix it.

Q. Is there a way to preview a file in File Explorer without opening the file? Sometimes I name my files similarly and forget which is which. Then I go to File Explorer and have to open each one to find the one I want. It would be much easier if I could just see the files first without having to open each one to find what I am looking for.

A. Actually, yes there is a simple way to do that. File Explorer has a built-in file viewer called the preview pane. To use it, open ***File Explorer*** and go to the file you want to view, whether it is a Word document, Excel Spreadsheet, Power Point presentation, PDF or image. If no preview pane appears, simply click on the "***View***" tab and select "***Preview pane***". Now you can click on the file you want to view, as it appears in the preview pane. Drag the separation bar left or right to increase or decrease the size (or width) of your file to see it better.

Q. Is there a way to check if a link or URL (Uniform Resource Locator) is safe or not? So much has been written about not clicking on unknown links or links in

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

that we made up ourselves (continued)

altogether. So how can I check to see if a link is "safe" or not?

A. You are correct. It is stressed over and over **NOT** to click on links if one isn't sure and especially those that appear in unsolicited emails or texts because they could contain malware, or steal one's login credentials if the link is impersonating a banking site requiring login, etc. So do we just not click on anything? That is pretty hard to do. Here are some suggestions you can try to see if a link is safe before clicking on it. Some basic things you can do is to make sure the link starts with **HTTPS** or **https** as this indicates using a secure socket layer (SSL) to transmit and encrypt data. Also check to see if there is a padlock symbol at the far left of the URL address. You can hover your mouse over the link if it is truncated or to check the spelling. Some imposter sites look like the real thing but checking the link reveals different spellings of the real site. For example, amazon.com may appear as amzon.com or wellsfargo.com may appear as wellfargo.com. There are other ways to check that are a little more involved:

- Use a link checker tool. We mentioned some on page 4 of this newsletter, but here are a few more:
  * Norton Safe Web (https://safeweb.norton.com).
  * Google Safe Browsing (https://transparencyreport.google.com/safe-browsing/search)
  * Kaspersky Threat Intelligence Portal (https://opentip.kapersky.com/?tab=lookup)
- If you did go to a website and had doubts about it, check to see if the website itself provides an email, phone number, or real address in its contact information. Many "imposter" sites look just like the real thing, but lack contact information or customer support information at the bottom of the main page.
- Check reviews on the website. Do they all sound the same? Are they templated? Are they unusual? This could be an indication of an imposter website.
- Check the website's domain information, e.g. its age and ownership? If a domain hides these details, it may be an unsafe site. How do you check it? You can do a **WHOIS** search by going to (https://hostinger.com/whois) and entering the domain name.

These are just some of the ways to check to see if a link is legitimate. Don't rush through and just click on links indiscriminately. And if you are not sure (and you don't have the time or don't want to check, simply don't click on the link). Stay safe online.

Q. Can I change my username on my local account in Windows 11?

A. Yes. Open ***Control Panel> User Accounts*** and select the profile whose username you want to change. Then select **Change your/the account name**. If your Windows 11 device is connected to a Microsoft account, you'll have to edit the name on an external webpage. On your device, go to ***Settings> Accounts> Your info> Manage my accounts***. When the webpage opens, expand the ***Your info tab*** and then select ***Edit name***.

As the weather gets hotter, don't forget to hydrate, especially if you are outside. Summer is coming, along with the 100 degree days. Stay safe and frequent your air-conditioned Computer Club. Enjoy your summer!