Volume 22 Number 09 Sep2022

SCA Computer Club notes

Classes for the Month of Sep

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

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

Monitor Training-Refresher: Refresher course for **current** Monitors. Monitors are required to attend this course once every twelve (12) months to stay qualified, as well as perform a minimum of ten (10) shifts per year.

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

Apple Mobile Calendar App: Account configuration, making and using multiple calendars, creating events including repeating events and the use of alerts. Sharing Calendars and subscribing to public calendars will be covered. ***Prerequisites:*** Introduction to iPad or familiarity IOS operating system.

Photoshop Elements: Do you have a digital camera? 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.

Monitor Training-New: Monitor training for **new** monitors.

Buying a Computer: In order to make an informed decision when buying a computer, there are a things to consider. Learn the basic terms in this class so you can make an informed decision on what to purchase.

Apple Mobile Contacts App: Account configuration, using groups to organize contacts, integration with the Mail app, the phone, the Message app and Facetime. ***Prerequisites:*** *Introduction to iPad or familiarity with IOS operating system.*

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

Apple Mobile Mail App: How to use the Mail app to send and receive mail from multiple email accounts on iPhones, iPads and iPod touch. Topics will include basic account setup, creating and using mailboxes, attachments, and signatures. We will also cover sending attachments including pictures by email. Avoiding Spam and phishing schemes will be explained. ***Prerequisites:*** *Introduction to iPad or familiarity with IOS operating system*.

Classes continued:

If you are an Apple user, **Apple Talk** meets monthly to investigate Apple products. Did you recently buy a Mac, an iPad or MacBook Air? Do you have questions regarding specific Apple products or applications? Meets Sat Sep 10th at 10 AM in the classroom.

Computer Talk is designed as a "question and answer" session. This group is for computer related discussions and not limited to any specific product. Bring your Android, Apple, Chromebook, Windows, etc. questions and we will try to answer them. Meets every Thursday at 9 AM in the classroom.

Photoshop Elements Advanced Topics: discusses monthly topics based upon skills learned in the Photoshop Elements class including color and light adjustments, removing objects, combining photos, adjustment layers, etc. ***Prerequisites:*** *Basic Photoshop Elements class or some experience using Photoshop Elements or Photoshop*. Meets Friday, Sep 30 at 9:30 AM in the classroom.

Mark your calendar:

Many folks have cut their cable due to the expense. Find out how to still enjoy watching TV and movies now that one doesn't have cable anymore. Join us at 1PM in the Delaware Room on Sep 1st.

** **Important** ** **New computers will be installed in the Computer Club to replace older ones. We will be auctioning off the older machines as the new machines are configured and placed. Check the website for upcoming details**.

What is a modem? What is a router? Is there a difference between them?

Many of us have our computers hooked up to a modem and/or a router, but do you know the difference between them? Well, basically, a modem translates data from one's Internet Service Provide (ISP), e.g. Cox, Century Link, etc. and converts that data into a format that one's computer and devices understand. A router, on the other hand, acts to distribute the data from the modem and sends it to one's device. It can also receive data from the devices and send it back to the modem and on to the ISP. Simply put, a modem handles communication between one's home and ISP and the router handles communication between one's home and its devices inside the home.

Normally a modem will sit between the router and the line to one's ISP and listens to one's computer and devices sending data and then converts it into something that is sent to the ISP. If a signal isn't digital that is sent to one's PC, the modem converts it to a digital format because that is what computers understand...digital signals. Most homes connect to their ISP via copper cables or phone lines. Copper cables use electricity and phone lines use analog signals, hence the need for a modem to convert these signals into a digital format. We refer to the act of turning something digital to analog (or vice versa) as modulating.

A router on the other hand specializes in transferring data. It can do so via an Ethernet cable or connect via Wi-Fi (2.4 or 5 Ghz). The router supplies Wi-Fi channels to one's devices to use and many routers automatically select the best channel for one's network. But one can manually set up one's router to use a specific channel, if desired. Some routers even have firewalls to help keep connections secure.

It addition to copper cables and phone lines connecting to one's ISP, today fiber optic is available. Fiber optic sends data using light on/off pulses (similar to a digital signal). But most fiber optic connections don't go directly to one's house. They may go to a nearby utility box (e.g. FTTC or Fiber-to-the-Curb) or to a neighborhood hub (e.g. FTTN or Fiber-to-the-Node) and either copper or phone cable covers the remaining distance to one's home. In these cases, one still needs a modem to translate the data coming down the cable to one's home. If one is fortunate enough to have FTTH or Fiber-to-the-Home) one will also have a box within the home or an Optical Network Unit (ONU) somewhere installed in the house that decodes the signals. If one has FTTH, a modem is not required.

Today some folks may not have a separate modem and router, but instead a combination device. They are becoming more popular and if you rely on a device that you rent from your IPS, chances are you have a combo device. This may all sound "too complicated" for some because all they want to know is that they turn on their computer and go to the Internet and shop online or receive their email.

But for those of you who wondered what a modem or router does, we hope this basic information provided some insight. Let us know.

Do you use an Apple device? If so, it is recommended that you install the latest updates because hackers could exploit security flaws and then gain control of one's affected device. Apple has pushed out operating system (OS) updates to patch the vulnerabilities for iPhone, iPad, Mac and Safari users. The identified flaws may allow the execution of a code with kernel privileges thus affecting one's device and allowing a hacker to control one's device.

Identified flaws include users of IOS/iPadOS specifically, iPhones 6 and later, iPad Pro (all models), iPad Air2 and later, iPad 5th generation and later, iPad mini4 and later and iPod touch (7th generation). Users are urged to update their systems to version iOS/iPadOS 15.6.1. To do so, go to ***Settings> General> Software Update***. If one's OS is up to date it will display that, but if not, it will display a prompt to update to the latest update.

For macOS users, macOS Monterey 12.5.1 is the latest and for those using Safari, it is recommended to update macOS Big Sur and macOS Catalina to version 1.5.6.1. Mac users should click on the Apple icon in the upper left-hand corner of their screen> *select About this Mac> click the button for Software Update*. If your Mac is up to date it will display that or one will be asked to download and install the latest update. For Safari users running macOS Bug Sur or macOS Cataline, updating the operating system to the latest version automatically updates Safari. Stay up to date and stay safe.

Do you video conference using Zoom? If so, take note. A reported flaw was discovered in Zoom for macOS, specifically in the Zoom installer, that could let a cybercriminal take control of one's entire operating system by allowing a local low-privileged user to escalate their privileges to root. Then they could modify, delete or add files to one's system. Zoom acknowledged this flaw, deeming it High in severity and released an update to fix the problem. One needs to update to Zoom v5.11.5 to patch it. Or one can go to the Zoom app on one's Mac and select "***zoom.us***" from the menu bar (at the top of the screen). Next select "***Check for updates***" and if one is available, select "***Update***" to begin the download.

And not to leave out our PC users, if one is a Windows-based computer user, Microsoft urges one to install its latest update as soon as possible, which fixes 121 vulnerabilities for August (17 of which are considered critical). The three Microsoft Windows 10 files (KB5016616, KB5016623 and KB5016629) fix 64 elevation of privilege flaws, 31 Remote Code execution exploits, 12 flaws that can reveal information and two (2) zero-day flaws. That's why it is important to update immediately.

One of the flaws could allow hackers to exploit a coding error in Microsoft's Support Diagnostic Tool, placing a malicious executable in the Windows Startup folder. Malware gets onto one's computer through opening an infected email attachment or by one downloading a file from a spoofed website. The other zero-day vulnerability may allow hackers to bypass security protocols and read one's email. Always check regularly for Microsoft updates, as they periodically release smaller patches that correct additional flaws. Here is how to do it:

To Update Windows 10:

- Right click on the Start button in the bottom left corner of your screen
- Click on ***Settings> Update & Security***
- The next screen should display your Windows Update status
- Click on ***Check for Updates*** and if one is available, ***Download and install.***

To Update Windows 11:

- Click on the ***Start icon*** and select ***Settings***
- Click on ***Windows Update > Check for updates***
- If an update is available, select ***Download and install now***.

And for our Google Chrome users, multiple security bugs have been patched as well. Chrome's update should automatically apply to one's browser IF one relaunches Chrome regularly. But is you never close out (e.g. just minimize the tab and pull it up again to use) or IF you want to double-check, here's how:

- ***Open Chrome*** and ***click the three little dots*** in the top right hand corner of your screen
- Click "***Settings***"
- Click "***About Chrome***" (on the left side of the page)
- On the next page, Chrome will tell one if one's browser is up to date. If not, one should see a button to Relaunch Chrome.
- Click the **Relaunch button.** Chrome should close and restart and now one's browser should be updated.

Did you know that Chrome has an Enhanced Safe Browsing feature for extra security? Since the number of data breaches increase each year, Chrome offers additional protections to keep one's personal data safe from malicious activity online. There might be a trade-off with being safe and loosing some of one's privacy. Using Google's Enhanced Safe Browsing provides Google with access to more in-depth information about one's browsing habit. Perhaps this is why these protections are not enabled by default. That being said, if one wants to added protections, one must turn them on and here is how to do it:

- ***Open Chrome*** and ***click on the three dots*** in the upper right corner of one's screen or browser.
- ***Click on Settings***.
- ***Click on Privacy and Security.***
- ***Click on Security > Enhanced protection. (On an Android device, click on Safe Browsing at this step).***

If one enables Enhanced Safe Browsing, Chrome will check in real time whether or not a site one is about to visit might be a phishing site. This could prevent users from accidentally giving away their information to nefarious actors and possible saving them from being tricked into losing their money. Also if one is about to download a new Chrome extension from the Chrome web store, Enhanced Protections will let one know if the extension is trusted or not.

Additionally, Chrome also scans file before one downloads them and blocks suspicious files. If the files are deemed risky, but not clearly unsafe, the user has the option of sending the file to Google for a more thorough analysis. This extra precaution may be worth it to keep folks safe. And Google will scan usernames and passwords associated with data breeches to see if one's information is compromised. A notification from Google could warn one before one gets hit with fraudulent charges.

While all of these features of Enhanced Safe Browsing seem great, just remember there are a few drawbacks on privacy. For example, if one is using Enhanced Safe Browsing, one is signed into Chrome and one's Google account is also temporarily linked to one's browsing data. Although Google says it is to "tailor protections to one's specific situation" and the data is supposedly anonymized after a short period of time, studies implicate anonymized date (including search histories) can be linked to social media profiles using publicly available data. In other words, one has to determine for oneself if enabling Enhanced Safe Browsing outweighs the possible of Google knowing one's search histories or other privacy information.

Why do we provide our readers with articles on recent security flaws anyway? It certainly is not to scare our members but to make them aware of just how compromised the use of computers can be in their everyday lives. That certainly doesn't mean: stop using one's computer. It merely points to the fact that we all should be AWARE and not just assume that our operation systems (one whichever computer we use) and/or our browsers, etc. are not infallible. As a computer user, one should try to do whatever one can to keep one's system up to date and periodically check it to ensure the latest update is employed. We need to be aware of the multiple phishing attacks, the unscrupulous emails (enticing us to click here or there) and the other nefarious tricks that abound to compromise our personal information, bank accounts, etc.

Computers, tablets, phones, laptops, etc. are all wonderful instruments that have empowered many of us and allows for us to keep in communication with our loved ones, learn about upcoming events, watch videos, listen to music, read books, etc. in a convenient way from sitting right at home in our recliners. But with this technology, there remains risks and we should try to keep informed so as not to fall prey to those who seek to hurt us.

Remember to:

- keep your system (whatever it is) up to date and check it periodically

- be suspicious and avoid clicking on links that are embedded withing emails (e.g. attachments, files, photos, etc.) especially if you do not know who the sender is

- Never submit personal information (account numbers, passwords, credit card information) especially if asked by someone, even if they say they are with your bank or store you frequent AND you did not initiate contact with them originally.

- Check the URL (uniform resource locator), e.g. the address of the sender or the website, to ensure it is legit. For example, if you bank at Wells Fargo and receive an email from them, check the URL. If it does not read as https://www.wellsfargo.com, but instead reads something like (*lcgmfxtbnv@lcgmfxtbnv.net or xjxqsziisk@pkjsfhdzl.onmicrosoft.com* or anything other than what you think it should look like) **DELETE** it immediately.

- AND IF you are still unsure, call whom you think the sender is to see IF they are really sending you something. This includes your bank, your friends, a family member, etc. Just because you recognize the person's name or the institution, doesn't mean they weren't hacked and someone is using their contact list to send out emails.

- Be safe on line. Enjoy your computer. Enjoy your Computer Club and let us know how we are doing.

Want an alternative to Google Search? There are many various search engines available and the most common ones that come to mind for PC users are Microsoft Edge (which uses Bing) and Google and for Mac users, Safari or Mozilla Firefox. Although we've listed other search engines in past articles, here are some alternatives to Google.

- **Brave Search**: a relatively new search engine (delivers fast and accurate results) using community-made data from the Web Discovery Project. Touted for its privacy policy, it doesn't collect location data or search history or doesn't track one.

- **DuckDuckGo**: mentioned previously, it is a popular option that doesn't collect personal information or use targeted advertising.

- **Swisscows**: it pulls accurate results from Bing, doesn't track its users and block porn, violence and other explicit content. It is considered to be family-friendly search engine. More than just a browser, Swisscows offers a secure mail system with custom addresses and sells a VPN subscription for $10/month. Switzerland has some of the strictest data privacy laws and Swisscows is based in Switzerland, owning its own servers and datacenter.

Do you use another search engine, other than these we mentioned? If so, let us know how you like it and why. Perhaps other members of our club would be interested in trying it out. Contact us via our website at: https://computer.scaclub.org and from the main menu, select "***Contact Us***". Select "***Newsletter***" and give us your opinion. We would live hearing from you. Also let us know what you would like to see in future editions of our club Newsletter. And if you are interested in writing articles for our club newsletter, let us know that too!

Many of us still use Windows 10 (and that is perfectly fine, especially if our computers can't or won't support Windows 11). Microsoft might just be preparing to release a 22H2 update for Windows 10 in the second half of 2022 (which coincidentally is now). Although Microsoft ended most feature developments on Window 10 (after Windows 11 was released) the update could bring some new changes as the last significant update was the November 2021 Update (21H2). Remember, Windows 10 will remain supported until Oct 2025.

Even with that said, Windows 11 users can expect its first major update, Windows 11 22H2, starting this month around the 20th of Sep (so it is speculated). Microsoft is also working on new Surface products to arrive before the end of the year. Did you now that this is the 10th Anniversary of the first Surface tablet? The new products should ship with Windows 11 22H2.

So what is in Windows 11 22H2? To begin with, it is supposedly a huge update with a redesigned Task Manager, drag and drop in the taskbar, improvements to window snapping, folders in the Start Menu, Live Captions for an Audio (just like Android) and much more. Let's hope that with its large size, it rolls out seamlessly and doesn't cause other issues like other large updates in past years have caused. Keeping our fingers crossed.

We have mentioned previously that backing up one's files is advisable in case the originals get corrupted or lost or a major update crashes one's system. And even though there are third-party backup programs available, Windows itself has a built-in tool for doing so, aptly named, **File History**.

File History is available in Windows 10 and Windows 11 and can automatically back up files from specific folders on one's PC to an external storage device (e.g. USB drive, external hard drive, network location, etc.) and the backups can run in the background based on the interval one sets. To restore a file, just open and browse through one's previous backups and find the right version.

By default, File History backs up specific folders under one's User account (e.g. Documents, Music, Pictures, Videos and Desktop). It also allows one to remove (or add) folders to make sure all the files one wants backed up are backed up (regardless where they reside). But unfortunately, its days may be numbered as Microsoft may force its users to use OneDrive as a backup method. Take advantage of it now.

In Windows 10

- go to ***Settings> Update & Security> Backup*** and connect the device you want to use as the backup location.

- Click on ***Add a drive*** and select the drive you wish to use to turn on File History.
- Click the link for "***More options***" and then the dropdown menu for "***Back up my files***".

- You can set the interval from 10 minutes to daily. Click the menu for "***Keep my backups***" and decide how long you want to retain each backup.

- Now you can set which folder to include and exclude in the backup. If a folder is not listed, then click the ***Add a folder button*** and select that folder. If the list displays a folder you don't want to backup, select it and then click ***Remove.***

- To exclude any folder not displayed in the list (e.g. a sub-folder) click the ***Add a Folder*** button in the section for ***Exclude these folders*** and select the folder.

- Depending on the backup schedule you chose, the File History backup may have already started by itself. If not, then scroll to the top of the screen and click the ***Back up now button***.

- You can continue to use your computer as the backup runs. After it is completed, the overview section will display the date and time of the last backup.

In Windows 11,

- first make sure the drive you want to use as the backup is connected.

- Open the ***Control Panel*** in icon view and select the ***File History icon*** (or click the Search icon and type in File History and select the result).

- The File History window should be pointing to the backup destination under "***Copy Files to***". If more than one backup drive is connected, click the link on the left for ***Select Drive***. Select the drive you want to use for backing up your files and click ***OK***.

- You can add other folders (besides the default ones). In Windows 11, to add another folder, open File Explorer and ***right-click on the folder*** you want to add and select "***Show more options***".

- From the full context menu, select "***Include in library***" and ***then add it to an existing folder*** **OR** create a new library. I hear you, this is kind of clunky but this is how it works in Windows 11.

- To exclude a folder, click the link for ***Exclude Folders***. Click the ***Add button*** and select the folder you wish to exclude from the backup.

- Return to the main **File History Control Panel window** and click the link for ***Advanced Settings.*** Now Click the dropdown menu for ***Save copies of files*** and set the backup interval.

-Click the dropdown menu for ***Keep Saved version*** and set how long File History backups should be retained. When all done, click "***Save Changes***".

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

that we made up ourselves

Q. I don't want to pay for Microsoft Office. Are there other alternatives other than Mac pages, numbers, etc. as I am not an Apple user.

A. Funny you should ask. **LibreOffice**, is a free alternative to Microsoft Word, Excel and PowerPoint and just recently, LibreOffice 7.4 was released and considered to be a significant update. LibreOffice is a free, open-source office suite now available in 120 different languages. The new release touts improved support for borders and clearing breaks from Word docs and fixes for embedded media and shapes from PowerPoint files. LibreOffice 7.4 is now available for Linux, Windows 7 SP1 and later and macOS 10.12 and later. One can download the newest version from its official site at: https://lireoffice.org/download-libreoffice/

Q. I am running out of space on my PC. I use Windows 10 and would like to see if I can delete any large files that I may no longer need. Is there an easy way to do this? And in easy, I don't mean writing code or buying third party software. I am a basic user, not a geek.

A. The short answer is yes. But a word of caution. Once you identify a "large file" that you want to delete, be sure you know what it is. If you don't, you might just delete an important Windows file that affects your PC's performance. You have access to File Explorer and that makes it easy to manage all of the files and folders on your Windows PC. Using the search tool, you can find all of the files and here's how:

- ***Open File Explorer*** (from the taskbar icon or press the Windows key & E simultaneously.

- Select "***This PC***" on the left hand side pane or select any folder that might have large files that you know of.

- Type an ***asterisk*** (e.g. *) in the File Explorer's search bar and this will display all of the files of your PC.

More specifically to answer your question regarding LARGE files,

- Click the ***Search tab*** in the top-left corner of the screen

- Next, click the ***Size*** drop-down menu (e.g. the arrowhead to display options)

- Depending on your preferences, select Large (128MB-1GB), Huge 1-4 GB), or Gigantic (<4GB) from the options.

OR you can specify your own size limit in the File Explorer's search bar (e.g. if you want files larger than 100 MBs, type "**size:>100MB**" in the search bar (without the quotes) and press Enter.

Lastly, don't forget about hidden files in case you can't find something that you think you had. To check for hidden files, open Windows File Explorer or press the Windows key & E simultaneously.

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

that we made up ourselves (continued)

- Click the View tab at the top-left corner.

- Check the ***Hidden items*** box to show all files and folders that are hidden. We hope this helps you clear up some of your storage space. Let us know if it did.

Q. What is scareware? I heard the term used but don't know what it is.

A. Scareware is just another name for a cyberattack tactic that scares folks into visiting a spoofed or infected website or download malware. Many times scareware comes in the form of a pop-up add or through spam email attacks. Scareware tries to take advantage of one's fears, using threatening tactics or FUMO (fear of missing out) of the latest new thing. It is malware and it may claim to get rid of one's computer virus (when there isn't really a virus on the computer). For example, one may be searching the Internet and all of a sudden a pop-up add appears. It could be a flashing red image saying your computer is infected or a message in all CAPS using exclamation points encouraging one to act fast or right now or it could be a screen shot of a (supposedly) infected file on one's computer urging one to call the number or click on the link. The purpose behind it is to get one to panic and make irrational decisions such as buying worthless software, downloading "a fix" (which instead actually infects one's computer with malware) or calling a number on the screen "for help" (which normally goes to the scammer who then tries to get money out of the caller). If a pop-up suddenly appears on your screen indicating you have a virus, turn off your computer. It may also be helpful to turn off your router to prevent the malware from sending data to the perpetrators. When you turn your router and computer back on, check to see that you have the latest OS updates for your computer and also for your browsers. If you have a browser setting to enable pop-up blockers, then enable it. And don't panic, just take a breath and use common sense and be careful on what you click on or the sites you visit in the future.

Q. Is it safe to use money transfer apps like Apple Pay, Zelle, Venmo, etc.?

A. Many of the money transfer apps are supposedly safe to use, but recently Citi Bank put out an advisory regarding wire transfers and using Zelle. Specifically it warned against using Zelle to:

- send money to anyone claiming to be from a government agency or any stranger (regardless of the reason),

- any telemarketer trying to sell something or anyone claiming that one's account is compromised

- unauthorized/unverified cryptocurrency sites or salespeople or anyone asking one to send money to oneself. Basically it is a general reminder that when using such apps, one needs to be very careful about who one is sending their money to. When using Zelle, money is sent quickly and often times the funds are hard to trace and recover if one is scammed. So be vigilant, be aware and make a conscious decision before clicking. And ***if in doubt, don't***.