Volume 22 Number 04 Apr 2022

SCA Computer Club notes

Classes for the Month of Apr

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.

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.

Buying a Computer: In order to make an informed decision when you are buying a computer, there are a few terms that you need to be aware of so that the sales folks don't try to "snow' you. Do terms like gigabytes, hard disks, volatile memory, main board, Ethernet card, cable modem, etc. make you wonder which country you are in? Then, join us in helping you become aware of meaning of these terms and many others that you hear. Learn the basic terms in this class.

Photoshop Elements is for both Mac and Windows users who want to learn to organize and edit pictures. It provides a basic introduction to its photo-editing program. ***Prerequisite: comfortable using Mac or Windows OS.***

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?

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.

Photoshop Elements Advanced Topics builds upon skills used in the Photoshop Elements class, including enhancing photos, removing imperfections, combining photos, etc. Some fixes are easy, others use the power of adjustment layers. ***Prerequisite: basic Photoshop Elements class or experience using Photoshop Elements or Photoshop.***

Mark you calendar for our **Electronic Equipment Recycling Event** on **Saturday, April 16, 2022 from 8 am — noon at the Anthem Center East Parking lot**. Signs will be posted to direct traffic to the recycling truck. **DO NOT** drop off any equipment at the Computer Club prior to the event. Please, if for some reason you cannot make this April 16th date, contact **Sustain Vegas** at **702-248-7302** to arrange dropping off your equipment at their location (4660 W. Dewey Dr, Unit 145) or request they pick it up at your home. *Thank you in advance for your cooperation.*

List of unaccepted items: CRT TVs & Monitors, Thermostats or any device containing mercury, Medical devices, appliances, batteries, ballast, lightbulbs, microwaves, VHS/Cassette tapes, any item that contains a liquid (Freon, Mercury, etc.), smoke detectors

The next Board meeting is scheduled for Thursday, Apr 28 at 1:30pm in the classroom. Members are welcomed to attend and listen while the Officers and Directors discuss club operations. Have questions about why we do things the way we do? Want to recommend new practices? A member's comment period near the end of the meeting allows members in attendance to provide input, comments or ask questions of the Board. This is a good opportunity for members to observe the Board's discussions, recommendations, decisions, etc. especially if one is considering getting more involved with club operations and thinking about running for a position in the future. It also gives members the opportunity to provide the Board with input regarding our Club.

Windows 11 Tips

What is **Snap Windows**? A feature in Windows 11 that allows one to position multiple windows on one's screen simultaneously. Using a pre-defined layout, each window can be snapped into a specific place on one's desktop.

To try it, open four (4) different apps (or windows) in Windows 11. Now choose one of the four and place your mouse cursor over the maximize icon (upper right-hand corner that looks like a square (between the _ and X)). When you do so, you should see four (4) different layout patterns from which to choose.

If you want to snap only two (2) of the four (4) open windows, so they appear side by side, choose the corresponding side by side pattern. Clicking the figure on the left side (of the pattern) will position your current window on that side, while doing so on the right side will position your current window on the right side. After choosing a side, you should see a large thumbnail image of the other three (3) apps (or windows) that you originally opened. Decide which one of them you want to display on the other side of the side by side layout. Again, hover your mouse over the maximize icon and then choose the second layout (the one you didn't choose initially) of the side by side pattern, and click the thumbnail of the window you want displayed. You can snap up to four (4) apps (or windows) to display at a time.

Malware-does it ever stop?

We've talked about malware before and although it might seem like an old topic, it warrants reminding all of us about its dangers. **Why?** Because it is constantly evolving and the majority of those who create it do so for nefarious reasons, e.g., to steal one's credentials, personal information, etc. We all need to be aware and try to use good practices to avoid being "tricked" into something that might inadvertently make us a victim.

So what exactly is **Malware**? Malware is any software that has been intentionally created and designed to cause havoc to one's computer (or to a server or network). The intent could be to steal or gain unauthorized access to information on one's computer or even an entire network. Malware can consist of ***viruses, worms, trojan horses, spyware, adware or ransomware*** and over a half-million pieces of malware are detected daily. And while companies have evolved to address malware, it is unlikely that malware will ever go away.

The ***best defense*** we can use to try and prevent malware from affecting us is to *be aware* and *take precautions* when using our computers, phones, etc. Having some type of anti-malware software (and there are free, as well as, paid applications) that identify, isolate or delete malware when identified is key. The Windows OS has "Windows Security" built-in and it includes an antivirus program called Microsoft Defender Antivirus. But *if one installs* another antivirus app and turns it on, Microsoft Defender Antivirus turns off automatically. Having two (2) or even three (3) different antivirus applications does not always mean one is better protected. To customize or see one's settings in Windows, select ***Settings> Update and Security> Windows Security***.

A dangerous and evolving strain of malware called Qakot (aka Qbot or Pinkslipbot) initially was a banking Trojan (in 2007). It is still around causing havoc, stealing passwords and credit card information, installing ransomware, backdoors and mapping out company networks. Now it has been found to hijack email accounts and then look for threads and inject itself by adding reply messages to those threads. Mail recipients might not even realize that the infected information is installing ransomware, backdoors and mapping out company networks. Now it has messages were not part of the original ongoing conversation between multiple parties. These messages often contain links to download a file and if clicked, the link delivers a zip file that then unpacks to create a Word or Excel file on one's machine that is malware. The identified malware is capable to steal user credentials for several banking and financial websites including Bank of America, Citibank, Wells Fargo, TD Ameritrade and Schwab, PayPal and Microsoft.

So how does one protect against such possible email injections? Well, as we've said before, **don't click** on links embedded in emails that you are ***unsure of,*** unsure of *who* sent it, unsure of *why* it was sent, unsure of *what* it is. *Don't let your curiosity get the best of you.* If someone you know sends you a file, but you weren't expecting it, contact that person first to ask **IF** they actually sent you something (to be sure it was not a spam email from their account with an attached payload).

Now, **IF** you do download and open the file and the file displays that you need to ***"Enable Content"*** or ***"Enable Editing"*** to view the file, **BEWARE**. That file just might be malicious.

And of course, make sure you use some type of antivirus software on your system at all times, whether it is the built-in Microsoft Defender Antivirus or another. Remember, you can always ***scan*** any downloaded file **before** opening it. Just select the file, right-click and scan with Microsoft Defender.

Malware-does it ever stop? (continued)

With tax season at our door, cybercriminals are once again impersonating IRS and sending out emails that could infect one's system with malware. The criminals spoof actual companies and/or government agencies using bogus W-9 tax documents as a delivery method. And now they are using email using the IRS logo and attaching a password-protected file (supposedly a copy of one's completed 2021 income tax return indicating one needs to retain the copy for next year). The ***IRS does not initiate contact*** with taxpayers by email, text messages or social media to request personal or financial information. Normally, if they want to contact you, it will be through a letter via the USPS.

And yet another federal agency, the Federal Trade Commission (FTC) has indicated that they too are being used in fraudulent scam emails with subjects that claim you have won a prize, ready to be collected (for a fee) or that there are some outstanding COVID-19 issues requiring one's immediate attention. These emails are supposedly from the FTC Commissioner Rebecca Slaughter or the FTC staff. The FTC won't email, call, text or message anyone and ask for money or information e.g. bank account, credit card, social security number, birthdate, etc. The FTC doesn't give out awards or funds related to Covid-19.

Remember, anyone requesting payment from you in the form of gift cards, cryptocurrency or even money transfers should be viewed with extreme caution as it is likely to be a scam. If you get an email asking for money or personal information, you can report it to the FTC at: ReportFraud.ftc.gov

There are many examples of malware and scam emails and people in their mature years (70s and 80s) are often targeted, so that includes us here in SCA. The reason is that many are financially stable and have good credit. It used to be easier to detect scam emails due to misspelling and grammar errors but today, many have become more sophisticated and even use commercial logos. And of course, embarrassment plays a big part in why older folks get scammed, some, multiple times. One is unwilling to admit it, or ask for help because one is too embarrassed and think that if one of their friends knew they had been taken advantage of, their friend might think poorly of them. The best thing one can do IF they are scammed (or think they may have been) is to tell someone….a friend, a family member, a trusted advisor, etc. It bears repeating:

* Don't click on links in an email or text (e.g. SMS message) unless you know it is safe (e.g. is from someone you know, you were expecting it, etc.) If you are unsure, don't.

* If you receive an email from a company or your bank and you are unsure if it is real, go to the company's website or go to your banking institution and check your account. Don't click on the link in that email to do so. Or call the business and ask to speak with someone there about the email you received.

* If you get an email or a phone call asking for financial information, don't get scared. Stop and think about what is being asked. Many times scammers will try to scare or intimidate potential victims by threatening them. Tell them you want to do more research before answering and then hang up, OR just hang up, or just mark the email as Junk and delete it.

* Sign up for fraud alerts on your credit cards and bank accounts. Don't fall victim and don't be too embarrassed to let someone you trust know if you have been scammed. Many times the scammers will come back again, especially if they were successful the first time.

Tips for Android Users

NOTE: not all Android devices use the same operating system (OS) due to the Android model and/or manufacturer. With this in mind, some of the settings may be different on your particular Android device.

Need to **find your device**? Here are a few options:

* Protect yourself by using a password (or pin or pattern) on your device. Go to ***Settings> Lock Screen>*** (some devices may display *Security or Security & Location or Security and Screen Lock*)> select the desired option. Using the default option is not advised as it is only a Swipe option and it provides no protection. Some newer Android phones allow "***Smart Lock***", which allows one to keep one's phone unlocked in certain situations such as when one's phone is in one's pocket or if one is near their resident, etc. Smart Lock is an additional feature.

* **Find my device app**. That's right, it is not just for iPhones anymore. Android devices also have a find my device app. One needs to have "location" turned on and then go to play.google.com/settings where it will display one's device. NOTE: the visibility box must be checked or it will not show Find My Device.

* Don't want to use the app? No worries. Find your phone using the Android website. Go to android.com/find and sign into your Google account. Now the last known location will display on a map, along with your device's battery life. One can also have the phone ring (for five (5) minutes) even if the sound was set to silent. Better yet, if one is concerned that someone stole the phone, one can Erase Drive. ***This option will erase all content on the phone***. *A drawback is that if Erase Drive is used, then one cannot Find MY Device anymore.*

* Use google.com to "Search" for one's missing phone. Type in "find my device" or "find my phone" in the search window and its last know location will be displayed. An option, Recover, provide more information, e.g., recent security activities.

* **Lookout Security & Antivirus app** is another option, available from the Google Play Store. If one thinks one's phone has been stolen, this app can not only locate one's phone, but sound and alarm. AND using its **Signal Flare** feature, it can send one an email with the phone's location, along with a photo of whomever may have it (even after the phone dies). Hopefully one will not need any of the above tools to find one's phone, but if so, there are several options available.

Protect your device using **Google Play Protect**

Enabled by default, this Android feature is a real-time malware scanner that monitors every app on one's phone. It even does so with any application one is going to install. Here's how to check to see if it is enabled. Go to ***Settings> Biometrics and Security***. Under Security, click on ***Google Play Protect***. A display of one's system's app should appear.

Two-factor authentication

This has been around for some time now and adds another layer of security to your phone because it requires one to verify. Go to ***Settings> Google> Manage Google Account***. Scroll through the menu until you find ***Security*** and choose ***2-Step Verification***. Open your browser (not Chrome) and tap ***Get Started*** and follow the steps displayed.

Tips for Android Users (continued)

App permissions

When installing new apps, we sometimes overlook the fine print that indicates the new app needs permission to a host of information. So, periodically, one should probably go through and check one's app permissions to see what all the app has access to. Go to ***Settings> Apps***. Click on the *three (3) dot menu* (in the upper right-hand corner) and select ***App permissions***. Now look at any app to see what secondary apps or services it is using. When installing new apps, it is always good to remember to read app reviews closely before downloading them, and check the review count to make sure you're not seeing a bunch of phony testimonials. Several five star reviews out of a small pool is a big red flag.

Lastly a note about using Location settings. Although it is needed in order to use some apps, like finding one's device, it also provides a lot of information about where you are (e.g., home, store, friend's house, Anthem Center, etc.). Sometimes this information provides targeted advertisements, so one might want to review which apps have access to one's location. To review, go to ***Settings> Biometrics and Security***. Scroll down and find **Privacy** and turn Location on. Now tap **Location** again to see which apps recently requested your location. Now one can adjust accordingly.

What is a Browser in the Browser (BITB) Attack?

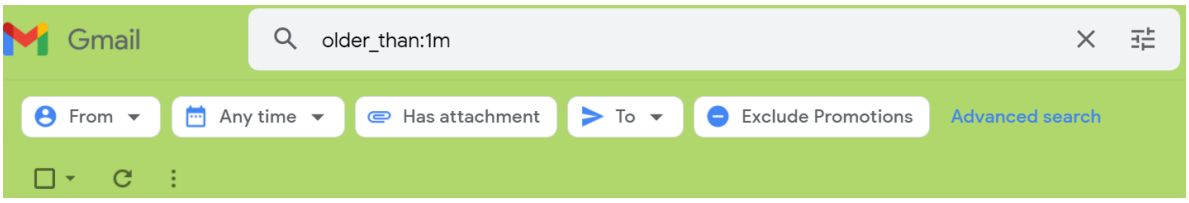
It is s phishing technique used to simulate a browser window within a legitimate browser in order to spoof a legitimate domain. Sometimes when a user authenticates to a website through Google, Microsoft, Apple, etc., one is presented with a pop-up window requesting one to authenticate, e.g. put in one's email or phone and then one's password. The problem is, it is basically indistinguishable from the real one, even if one hovers over the URL. So be extremely careful when a website you normally use (and doesn't ask you to login again), suddenly asks you to login in. It may just be a spoofed website and if you do login, your credentials can be stolen. There are some software able to tell if the "fake" window is real or not. For example, some password manager software might recognize the "fake" browser window and therefore NOT autofill your credentials like they normally would. Fortunately, while credentials may be compromised, there is not an immediate monetary reward and criminals would need to either sell those credentials or use them to get other data. Another reason why one should not use the same password for multiple accounts, especially banking and social media accounts. Passwords should be unique for each account and strong, for example, characters should be varied (e.g. upper/lower case, numerals and special characters) as well as lengthy passwords. Today, pass phrases are encouraged to be used since they are longer. The old eight (8) character password recommendation is outdated, with some suggesting that the minimum length for passwords should now be at least 16 characters long, hence the recommendation for pass phrases. What do you use?

Need help cleaning up your Gmail Inbox?

Of course you do! How long did that New Year's resolution to keep your Inbox manageable (by deleting unwanted/unneeded/outdated emails last? One month...two months...well if you are already behind, don't give up. Gmail has features that can assist. Let's start with the Search feature. At the top of your Gmail Inbox, there is a Search box. One can use it to search for old emails by day, month or even year. For example, if you have an Inbox with several years worth of emails (yes that is possible) we know you are not going to take the time to look through then all one at a time to determine which one you want or need to keep, right? So why not make it easier. In the search box, enter "**older_than:2y**" without the quotes. This will search and display any emails in your Inbox that are older that two (2) years old. If you've been semi-consistent about deleting emails out of your Inbox, you might want to change that search term to: older_than:3m (or even just a number of days, e.g., older_than:60d Whatever length of time you use, it can be a start to emptying your overcrowded Inbox to make things more manageable, right? Once your results display, you can either delete them all (or you can keep only the ones you really need).

Maybe you use (or started to use folders at one time to organize your emails) but didn't keep that up. You can do the same thing to clean up those folders also. Let's say you have saved every email from one of your club activities. You could input your search term as follows: **label:nameoffolderolder_than:2y** *The "name of the folder" would be whatever you labeled it.* So if I had saved all of my Veterans Club emails into a folder that was labeled Veterans Club, the search term would look like this: ***labelVeteransClubolder_than:2y*** The results would yield any emails in my folder labeled Veterans Club that were older than 2 years. I really don't need to see what the meeting subject was about two (2) or more years ago, so I can select them all and delete them.

Want to make it easier still, if you are getting a large number of resulting emails from your search? When your results display, you will see several buttons across the top. You can use these to further filter your search results, e.g. emails from a certain sender, emails with attachments, etc. Simply click on one of the buttons to further filter the results.



Let's say you want to further filter your results by displaying only those emails older that 1 month that have attachments. You would click on "Has attachment". You can again further filter those results by the *type* of attachment.

Need help cleaning up your Gmail Inbox? (continued)

Once again, select the button you want to filter the results (of emails with attachments) by type e.g. Image, Document, PDF, etc. Once you have the results, you can determine whether to keep or delete them. Then you can delete those you truly do not want or need. By clicking on the empty square box next to the email you want to delete to select it. To select all of them at one time click on the empty square box above the displayed search results. Notice that a check mark will now appear in each box next to all of the emails. IF you select "All" of the displayed emails, but want to limit the selection by read, unread, starred, Unstarred, etc. you can do that too by selecting the down arrowhead next to the empty checkbox. Once you've made all of your choices, select the trash can icon to DELETE them. You are on your way to cleaning up your over-filled Inbox. But wait, there's more.

What if you accidentally delete something and realize that you should have kept it. No worries. Emails that you have deleted should still be in your Trash can for 30 days. After that, they are permanently deleted from your mail account. So if you made a mistake, simply go to the left-hand sidebar and look for the "Trash" folder. (Note: you might have to expand "More" if you don't initially see the Trash folder.

If you have thousands of emails in your Inbox, don't try go through them all in one sitting. Do a little each day, using the time filters and before you know it, you will have a manageable Inbox and you can once again tell yourself you are NOT going to let it become unmanageable again. Your next task will be to remove the junk emails, but that's for another time. Let us know if this works for you. Login to our website at: https://computer.scaclub.org and select "Contact Us". Now select "Newsletter" and send us a message. Your Editors would like to hear from you.

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

Q. What is Personal Vault in "OneDrive"?

A. Personal Vault is a protected area where one can store important or sensitive files and/or photos. The folder, "Personal Vault", will automatically lock after a period of inactivity and to gain access, one must unlock it. But, one can change how long OneDrive waits before it locks. Its easy access via onedrive.com makes it ideal to store one's important documents because it is protected by an extra level of security. The one drawback however is that one can only store three (3) files in Personal Vault, **UNLESS** one has a Microsoft 365 Family or Personal subscription. With the subscription service, one can add as many files as one wants. To learn more go to: Protect your OneDrive files in Personal Vault (microsoft.com)

Useful things you may want to know, or Frequently Asked Questions (FAQs)
that we made up ourselves

Q. I am not sure but I think that my email has been hacked. Are there ways to check it?

A. Yes, there are a few ways in which you can check. These "flags" if you will, may indicate your account has been hijacked, either by malware or someone. And if this happens, your account may be used to spread phishing or spam to others, e.g. those in your Contacts. Here's some things you can look for:

* **Check your Sent and/or Drafts folders** to see if there are any emails in there that **YOU** didn't write. When checking your Sent mail, look at the recipients too, as well as WHEN the mail was sent. Also see if any of those emails include attachments. Attachments are a primary way to spread phishing malware. If you can't remember sending any of these emails, it's quite possible that your account has been compromised. Another indication may be from your friends who ask you if you sent them strange emails.

* If your account has been hacked (or if you suspect it has been) it is usually a good idea to **CHANGE** your password. ***Also look to see if your password was changed without your knowledge.*** To check, search your inbox for terms like "password reset", "password verification", "password successfully changed", etc. Look at the date and time and if you didn't change it, someone else might have.

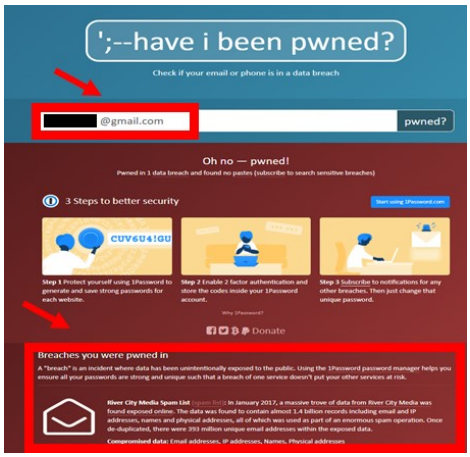
* You can sort through messages read or unread. If the emails are unread, they normally appear in **bold**. If you notice that your inbox (that was full of unopened emails, e.g., many were in bold print) now appear as if they have been read (unbolded) and you know you hadn't read them, that could be an indication too that someone else has accessed your email account.

* Have you received login alerts for accounts associated with your email? In many cases, if you log into a site from an IP address (that is not one you usually log in from) you automatically get an email notification, designed to prevent fraud and notify you of an unauthorized login. For example, if you login to your bank from your home and now you received an email location that indicates you have logged into your bank from another state, that can be a **RED FLAG** that your email account has been compromised. Hopefully, you have not experienced any of the above indications.

If you are still unsure, change your password and it is a good idea to set up two-factor authentication (2FA) as well, as it will provide you with an extra layer of security on your email account.

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

that we made up ourselves (continued)



Once set up, you will get an alert any time someone tries to log in from an unknown device. When choosing a password, be sure to make it as strong as you can. For example, use a long pass phrase and alternate between numbers, letters and symbols.

Don't use your birthdate, phone number, pet's name or anything else that is easy to associate with you via your social media accounts **AND** don't use a password that you use for other accounts (no matter how strong you think it is). One last thing, you can also check to see if your email account has been hacked or involved in a data breach by going to Have I Been Pwned: Check if your email has been compromised in a data breach If your email address has been compromised, you will see a list of sites that may have exposed your data and what exactly was leaked. The website is: haveIbeenpwned.com **NOTICE** the Spelling…**pwned** and **NOT** pawned! Always double-check the URL before launching.

Q. What is a Browser in the Browser (BITB) Attack?

A. Excellent question! It is s phishing technique used to simulate a browser window within a legitimate browser in order to spoof a legitimate domain. Sometimes when a user authenticates to a website through Google, Microsoft, Apple, etc., one is presented with a pop-up window requesting one to authenticate, e.g. put in one's email or phone and then one's password. The problem is, it is basically indistinguishable from the real one, even if one hovers over the URL. So be extremely careful when a website you normally use (and doesn't ask you to login again), suddenly asks you to login in. It may just be a spoofed website and if you do login, your credentials can be stolen. There are some software able to tell if the "fake" window is real or not. For example, some password manager software might recognize the "fake" browser window and therefore NOT autofill your credentials like they normally would. Fortunately, while credentials may be compromised, there is not an immediate monetary reward and criminals would need to either sell those credentials or use them to get other data. Another reason why one should not use the same password for multiple accounts, especially banking and social media accounts. Passwords should be unique for each account and strong, for example, characters should be varied (e.g. upper/lower case, numerals and special characters) as well as lengthy (e.g., more that 8 characters). Today, pass phrases are encouraged to be used since they are longer.