Volume 25 Number 01 Jan 2025

SCA Computer Club notes

Classes for the Month of Jan

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.

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.

Mastering the iPhone: Discover the full potential of your iPhone in this engaging one-hour session designed for all levels of expertise. Join us as we explore the latest iOS updates, exciting new apps, and enhancements to Apple's suite of tools like Photos and other key apps. This interactive session will include a lively Q&A, where you can get answers to your specific iPhone questions and learn tips and tricks to make your device work smarter for you. Whether you're looking to stay up-to-date or simply want to get more out of your iPhone, this class is for you. Don't miss this opportunity to connect with fellow club members and gain valuable insights from our trusted Apple guru. Bring your questions, your curiosity, and your iPhone—let's unlock its full potential together!

A Basic Introduction to AI (Artificial Intelligence): Keep up with today's technology. Have you ever wondered what all the hype is about AI? What is it? What does it do? How can you use it? Join us in this basic introductory class on AI, its uses, why it might be important for you and what you can use it for in everyday life.

Mac Safari Browser: Macintosh Safari Browser Using the Safari browser including using multiple windows or tabs, creating, organizing and using bookmarks, downloading and using plug-ins and extensions, removing unwanted malware, and setting preferences. Prerequisites: Mac for Beginners or familiarity with Mac operating system.

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.

Mac Mail App: Macintosh Mail App – How to use the Mail app to send and receive mail from multiple email accounts.

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 discussion of all products Apple. It will include presentations 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, Jan 11** from 10 am - noon.

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

Your Computer Cub Board will meet on Tuesday, Jan 14 at 1:00 pm in the Classroom. Any member in good standing is welcomed to attend and listen to the Board discuss Club operations. A Member Comment Period is held near the end of the meeting for members to address the Board. Have comments, questions, suggestions for the Club? Attend the meeting and address the Board.

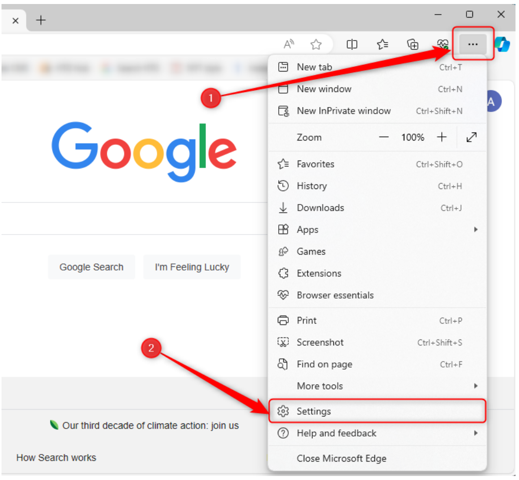
Do you ever drag your cursor over words to highlight the text? Maybe you are just cutting and pasting or copying something? Did you know that if you simply double-clicked on any word, it will select it instantly? Do you want more than one word, perhaps an entire paragraph? Then try triple-clicking anywhere in the paragraph and voila...all of its is highlighted. This little trick works in most browsers, word processors and even emails. So give it a try save some time and skip the click-and-drag struggle.

Did you know you could control your App permissions? Apps need access to certain things in order to function properly, but sometimes apps might request permissions that have nothing to do with its core functionality. For example, why would a calculator need your location? It doesn't. So, it is essential to manage your app permissions. To enable or disable permissions for a specific app on your PC, press **Windows + I to open Settings**. **Go to Apps> installed apps.** Click on the three-dot menu icon next to the app and select **Advanced Options**. Use the toggles under App permissions to mange permissions for that app. NOTE: Changes should take effect immediately, but if the app is already in use, you might need to restart for changes to take effect.

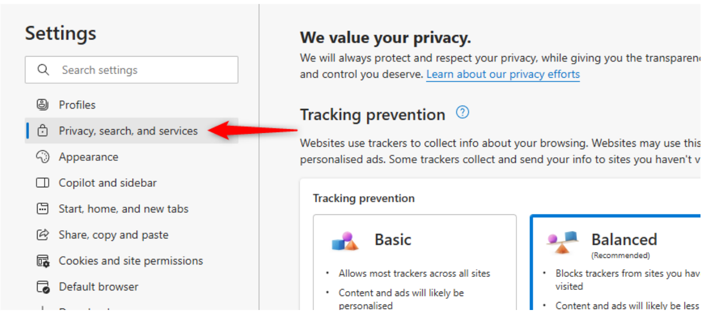
Another way to control your app permissions is via "**Privacy & Security**". **Open Settings> Privacy & Security** and scroll to **App permissions**. Select a specific permission e.g. Camera. Use **Let apps access your camera** toggle to enable or disable for all apps at once. If you want to use it for a specific app, click the down arrow next to **Let apps access your camera**. Scroll through the list and use toggles next to each app to enable or disable camera access as desired. You can do the same for location, microphone, photos, videos and more. This way you can be sure that your device only grants access to those apps you decide upon.

Change your default search engine in the Microsoft Edge browser

If you use the MS Edge browser, then by default your searches are using Bing. If you want to use another search engine (e.g. Google or DuckDuckGo, etc.) as your default browser instead, you can. Here's how: First, open an Edge browser window. Click the menu button (three dots) in the top-right corner and select "Settings." (Fig 1)



(Fig 1)



We value your privacy.

We will always protect and respect your privacy, while giving you the transparen
and control you deserve. Learn about our privacy efforts

Tracking prevention

Websites use trackers to collect info about your browsing. Websites may use this
personalised ads. Some trackers collect and send your info to sites you haven't v

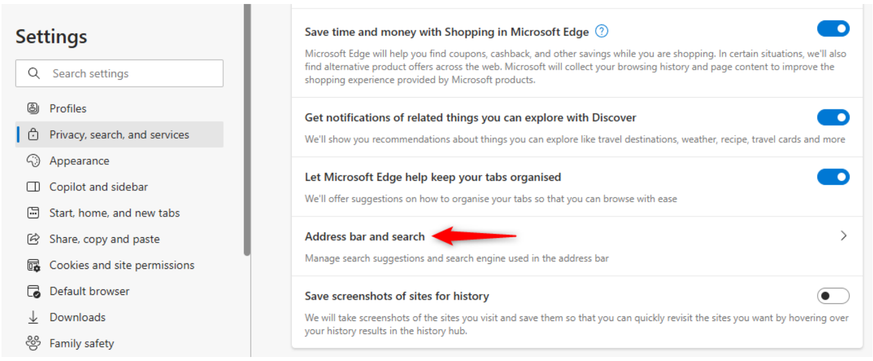
- Allows most trackers across all sites
- Content and ads will likely be personalised

- Blocks trackers from sites you hav visited
- Content and ads will likely be less

(Fig 2)

In the left sidebar, click "Privacy, Search, and Services." (Fig 2)

Scroll down to the bottom of the right pane and look for the Services section and then select "Address Bar and Search."



Save time and money with Shopping in Microsoft Edge

Microsoft Edge will help you find coupons, cashback, and other savings while you are shopping. In certain situations, we'll also find alternative product offers across the web. Microsoft will collect your browsing history and page content to improve the shopping experience provided by Microsoft products.

Get notifications of related things you can explore with Discover

We'll show you recommendations about things you can explore like travel destinations, weather, recipe, travel cards and more

Let Microsoft Edge help keep your tabs organised

We'll offer suggestions on how to organise your tabs so that you can browse with ease

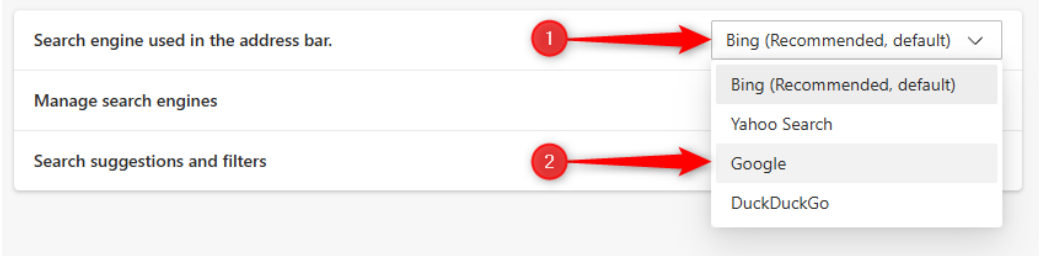
Address bar and search

Manage search suggestions and search engine used in the address bar

Save screenshots of sites for history

We will take screenshots of the sites you visit and save them so that you can quickly revisit the sites you want by hovering over your history results in the history hub.

From there, use the "Search Engine Used in the Address Bar" dropdown and select your preferred search engine. By default, you can choose between Bing, Yahoo, Google, and DuckDuckGo.



Search engine used in the address bar.

Manage search engines

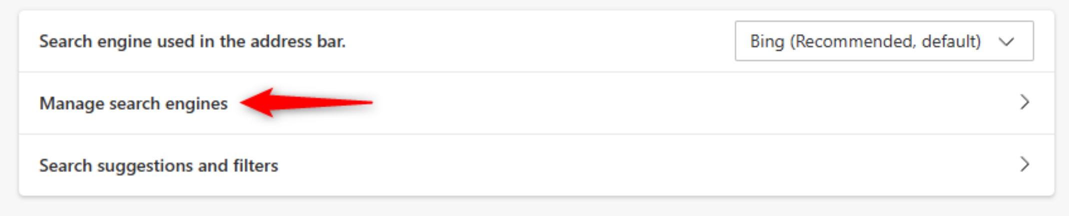
Search suggestions and filters

Change your default search engine in the Microsoft Edge browser (continued)

The next time you search from the address bar, or right-click text or images on a web page and select the "Search the Web" option, Edge will use your chosen search engine.

How to Add Other Search Engines

If you want to use a different search engine and not one of the four, click "Manage Search Engines."

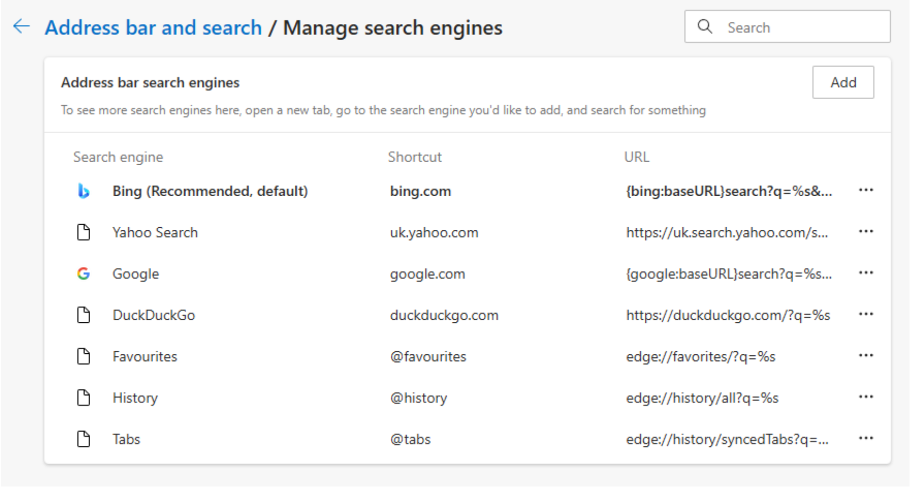


Search engine used in the address bar. Bing (Recommended, default)

Manage search engines

Search suggestions and filters

You'll see a list of search engines.



Address bar and search / Manage search engines

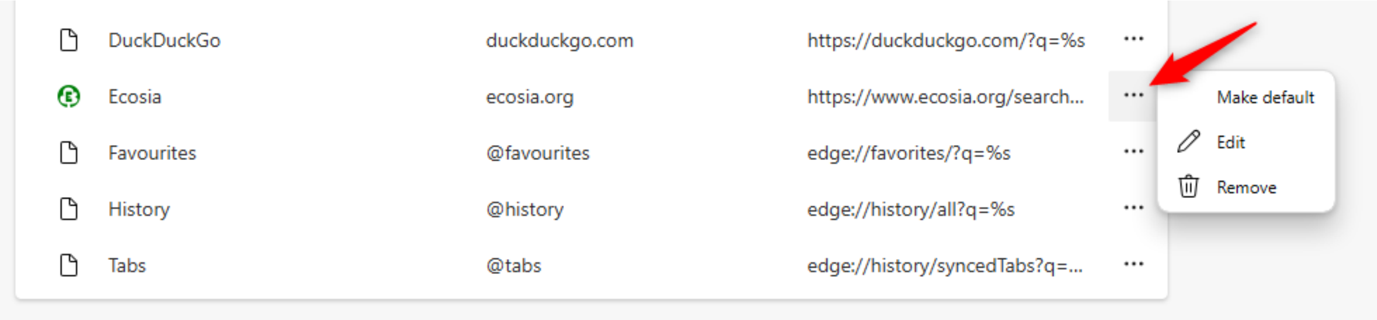
Address bar search engines

To see more search engines here, open a new tab, go to the search engine you'd like to add, and search for something

Search engine	Shortcut	URL
Bing (Recommended, default)	bing.com	{bing:baseURL}search?q=%s&...
Yahoo Search	uk.yahoo.com	https://uk.search.yahoo.com/s...
Google	google.com	{google:baseURL}search?q=%s...
DuckDuckGo	duckduckgo.com	https://duckduckgo.com/?q=%s
Favourites	@favourites	edge://favorites/?q=%s
History	@history	edge://history/all?q=%s
Tabs	@tabs	edge://history/syncedTabs?q=...

While you can click the "Add" button to add a search engine manually, this requires knowing that engine's URL structure. Instead, as Edge instructs at the top, "open a new tab, go to the search engine you'd like to add, and search for something." It will then appear as an option in the list, assuming the search engine is configured to offer this.

Once this happens, click the three horizontal dots next to the engine and select "Make Default." You can also use the same menu to delete an engine by selecting "Remove."



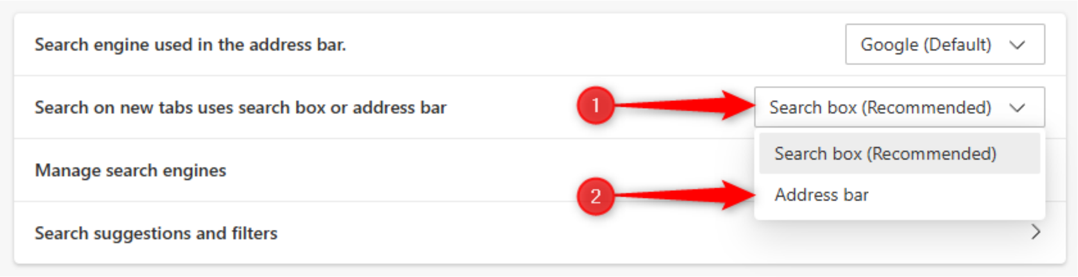
DuckDuckGo	duckduckgo.com	https://duckduckgo.com/?q=%s
Ecosia	ecosia.org	https://www.ecosia.org/search...
Favourites	@favourites	edge://favorites/?q=%s
History	@history	edge://history/all?q=%s
Tabs	@tabs	edge://history/syncedTabs?q=...

Change your default search engine in the Microsoft Edge browser (continued)

How to Change the New Tab Search Behavior

Even after you change your default search engine, the search box on Edge's new tab page uses Bing. You can instead use the address bar to search with whatever engine you've set as the default.

To do this, return to Edge's Address Bar and Search page (for quick access, input **edge://settings/search** into the address bar and press Enter) and set the "Search on New Tab Uses Search Box or Address Bar" to "Address Bar."



Search engine used in the address bar. Google (Default)

Search on new tabs uses search box or address bar Search box (Recommended)

Manage search engines

Search suggestions and filters

Fake AI video generator called EditPro

Bad actors are infecting both Windows and Mac devices with malware called EditPro which claim to let the viewer download a fake AI video tool. Cybercriminals are using social media ads and deepfake videos to trick users into downloading EditPro, which actually installs malware known as **AMOS** and **Lumma Stealer** on Windows and MacOS devices.

AMOS stands for Attack Management and Operations System and helps bad actors with minimal technical skills manage and automate large-scale cyber attack. Lumma Stealer is a malware-as-a-servive tool that captures sensitive information (e.g. login credential and credit card data). It is difficult to detect and combat due to its usage of advanced technologies such as process injection (a method of executing arbitrary code, hiding malware in normal computer processes that often slips past common security tools like antivirus programs).

Here is how it works:

Data Collection: The software collects a large amount of video footage of the target person, often from social media or other public sources.

Training: Using machine learning algorithms, the software analyzes the collected footage to learn the person's facial expressions, movements, and voice patterns.

Synthesis: Once trained, the software can generate new video content by superimposing the target person's likeness onto a different body or background, making it appear as though they are saying or doing things they haven't actually done.

Output: The final product is a highly realistic video that can be difficult to distinguish from genuine footage.

These fake videos can be used for malicious purposes, such as spreading misinformation, scamming people, or even blackmailing individuals. These malicious programs steal sensitive information like login credentials and credit card details. The file for Windows users is called "Edit-ProAI-Setup-newest_release.exe" and for macOS it is "EditProAi_v.4.36.dmg". If you've downloaded EditPro, it's recommended to reset all your passwords and enable multi-factor authentication to protect your accounts.

What’s an alternative to passwords?

Passwords are hacked daily. Why? There are several reasons: easy to guess (e.g. 123456, password, qwerty123, etc.) and/or perhaps there was a data breech, phishing attack, malware, etc. So what can be used instead of a password? A passkey.

What’s that? It is a way to log in to apps and websites without using a username and password combination. A passkey is a form of multifactor authentication that uses public key cryptography in combination with biometrics like fingerprint and facial recognition or a device PIN to verify an account owner’s identity. It's a pair of cryptography keys generated by your device. A public key and a private key combine to create a **passkey** that unlocks your account.

While the public key is stored on the server of the service one is using, it is not considered sensitive as it cannot be used to access one’s account without the corresponding private key. A private key is securely stored on one’s device within one’s operating system and remains hidden from the service provider. This is also known as asymmetric cryptography, a type of encryption. Apps or websites store your unique public key and passkeys act as a replacement for traditional passwords. They are becoming the future proof alternative to traditional passwords and they don’t require any resetting.

Maybe you have seen the option to setup and use a passkey. In a 2024 survey, 53% of respondents have enabled passkeys on at least one of their online accounts (FIDO Alliance). Google, Microsoft, Apple, PayPal, GitHub and more have adopted the technology because of the security benefits. Know how some “experts” recommend changing your passwords every so often? Well, with a passkey, that is no longer necessary.

How to enable passkeys? If you have a Google account, go to the Google Passkeys page and set up your passkey with your device. Go to “myaccount.google.com”. Choose “Security”, scroll down and select “Passkeys” (under “How do I sign in to Google”). Now select “Use passkeys”, then “Done” when it pops up. Tap “Create a passkey> Continue”. (NOTE: in case you’re only presented with “Use another device” after clicking “Create a passkey”, your current device or browser doesn’t support passkeys). If you get different pop up, select “Continue” and then you’ll be prompted to verify your identify. Once verified, a passkey is created and you click “Done”. You will find your passkeys under “Passkeys you created”.

You can set up passkeys on your Microsoft account and click on the “Manage how I sign in” button (under Security). Scroll down and select “Add a new way to sign in or verify” (next to the circled + sign). Choose face, fingerprint, PIN or security key, then follow the instructions that pop up to set it up. Once setup is complete, you’ll be asked to name your passkey. Then whenever you log in to any Microsoft service, just click “Sign in Options” and select your passkey, authenticate when asked and you are good to go…no password needed. If you want to remove it later go to the Security section of your account, scroll down to “Use a passkey” and click remove.

To set up a passkey on an Apple device, make sure your device is running iOS 16 or later, iPadOS 16 or later, macOS Ventura or later, or tvOS 16 or later. Go to Settings > Passwords > Password Options and make sure iCloud Passwords & Keychain is turned on. When signing up for a new account on a website or app, select the option to create a passkey. You can also create a passkey for an existing account by going to the account settings or management page. Select how you want to sign in with your passkey, such as Touch ID, scanning a QR code, or using an external security key.

Safari settings to consider

Do you use the Safari browser? Have you ever gone through your settings to see what you may or may not be allowing or maybe you want to block certain actions from occurring? Here are a few to consider:

- **Pop-up Blocker**: Stops annoying pop-up ads from appearing. **How to enable**: Go to Safari > Preferences > Websites > Pop-up Windows. Set the option to "Block and Notify" or "Block". This prevents those pesky ads that pop up when you visit certain websites.

- **Prevent Cross-Site Tracking**: Keeps websites from tracking your activity across different sites. **How to enable**: Go to Safari > Preferences > Privacy. Check the box for "Prevent cross-site tracking". This stops advertisers from following you around the web with targeted ads.

- **Block All Cookies**: Stops websites from saving small files on your device that track your activity. **How to enable:** Go to Safari > Preferences > Privacy. Check the box for "Block all cookies".

- **Disable Auto-Play**: Prevents videos from playing automatically when you visit a website. **How to enable**: Go to Safari > Preferences > Websites > Auto-Play. Set the option to "Never Auto-Play". This stops videos from starting on their own, which can be annoying and use up data.

- **Fraudulent Website Warning**: Alerts you if you're about to visit a suspicious site. **How to enable**: Go to Safari > Preferences > Security. Check the box for "Warn when visiting a fraudulent website". This helps protect you from phishing scams and malicious websites.

- **Disable JavaScript**: Stops some website features that can be annoying or harmful. **How to enable**: Go to Safari > Preferences > Security. Uncheck the box for "Enable JavaScript". This can make some websites load faster and reduce the risk of certain types of attacks, but might also break some website functionality.

- **Block Notifications**: Prevents websites from sending you notifications. **How to enable**: Go to Safari > Preferences > Websites > Notifications. Set the option to "Deny". This stops websites from asking to send you notifications, which can be distracting.

- **Disable Location Services**: Stops websites from knowing your location. **How to enable**: Go to Safari > Preferences > Websites > Location. Set the option to "Deny". This helps protect your privacy by preventing websites from tracking your location.

- **Reader Mode**: Simplifies web pages for easier reading by removing ads and other distractions. **How to enable:** Click the Reader button in the address bar or go to View > Show Reader. This makes articles easier to read by removing clutter like ads and sidebars.

Most websites have similar settings that one can select to disable/enable. Just go to Settings in your website start looking there for the various options.

Let us know if these are helpful or not or if you want to see articles like this. Provide your input by going to the club website and selecting “Contact Us”> Newsletter. If you don’t care to see articles like this, then please provide us some other recommendations on topics that you would like to see. We appreciate your candidness.

All you ever wanted to know about Firewalls

Before we dive into firewalls, it is essential to understand how data travels between Internet networks. Data moves across the Internet in the form of information-filled packets. A firewall inspects these packets, analyzing:

- Content: what each packet contains, e.g. image, text, video, etc.
- Protocol: language of the packet, e.g. HTTP (hypertext transfer protocol, the foundation of data communication for the World Wide Web and a standard between web browsers and web servers to establish communication) or TCP (transmission control protocol, a collection of standards allowing systems to communicate over the Internet). It works with IP (Internet Protocol) which defines IP addresses used to identify systems on the Internet, providing instructions for transferring data and TCP creates the connection and manages the delivery of packets from one system to another. You might recognize them as TCP/IP.
- Port: the medium that the data travels through, e.g. email, web, social media network, etc.
- Source: where the data comes from e.g. the IP address or hostname of incoming traffic.
- Destination: where the data is headed, including the IP address, hostname and other info describing where the traffic is going.

After all of the this, the FIREWALL determines whether or not to let the data packet pass through and can block it based on a set of predefined rules. There are hardware firewalls, often integrated into routers or standalone appliances. These act as a barrier between a private network and the Internet and provide scalability and consistent performance often protecting an entire network without relying on the resources of individual devices.

Software firewalls are applications installed on individual devices that monitor and control network traffic at the endpoint level. Included by default in most operating systems, e.g. Windows and macOS, and some routers. These firewalls can be configured to block specific applications and provide alerts for suspicious activities.

So a firewall blocks threats coming from restricted sources or ports. They can block data packets that have malicious content. Think of it like a checkpoint for all data packets. It can protect your home Internet system from threats e.g. cyberattacks , malware, ransomware, etc. An example is if an application tries to access a location or photos on your device (even though you haven't allowed it to do so) the firewall will immediately act to stop it and inform you of unusual activity.

A firewall can also use rules to filter network traffic, thereby blocking unauthorized attempts to access your system or monitor your activities and can be configured to log information about such traffic. It can track timestamps, size, protocols, ports, IP addresses and other details of a given packet. Some firewalls can also scan for weaknesses in your network's connected devices, alerting you of outdated or misconfigured software.

Sounds, great, right? But what a firewall CAN"T do is provide 100% protection. It's a part of the security factors one needs, including antivirus software because while a firewall inspects the network traffic, it doesn't always identity malware hiding within applications, files or devices that might go undetected. Using a firewall in conjunction with a good antivirus software program is recommended. It's only one piece of network security strategies, which also involves the user making wise choices against clicking on embedded links, etc.

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

that we made up ourselves

Q. I am 70 yrs old and only started using computers a year ago to text and email my grandchildren. They always ask me why I don't use emojis. What is that?

A. An emoji is basically a pictogram, a graphical or digital image or icon to express an emotion, idea, etc. For example a face, a heart, a flag, an animal, food picture, etc. Think of using a picture instead of writing words to express something. Using them in texts and/or emails is pretty easy because most texts/emails have that option. Where one would input the text or email, look for a smiley face icon and click on it or look where the formatting options appear. Here one will see the options for emojis, stickers, GIFs, etc. Click on "Emoji" and a list of them will be displayed. Just click on the one you want to add/insert it into your text or email and it will appear within the text or email. Hope this helps; let us know if it does.

Q. Is it true that TP-Link routers may be getting banned?

A. Yes, and there are about 65% of American homes and businesses that use TP-Link routers, along with the U.S. Department of Defense (DOD) and other federal agencies. These routers have been linked to Chinese cyberattacks and lets security flaws slide, making them a huge target. Currently they are under investigation by the Commerce, Defense and Justice Departments in the U.S. and are being considered to be banned due to their vulnerabilities and potential national security risks. The potential ban is more about the company's ties to China than the specific security issues, some cybersecurity researchers say. It comes at a time in Washington when there is a growing bipartisan support for extracting Chinese products from US telecommunications. An October attacked, "Salt Typhoon", has been identified as the largest telecommunications hack in our nation's history. If you have a TP-Link router, be sure to keep your firmware updated and use unique passwords to protect it (not the default password that came with it). Stay tuned for more information as the investigation continues. At this point, it is not necessary to run out and buy a new router (unless of course you need one).

Q. *Is there a way to protect my cell phone, for example, to lock it if it is lost or stolen? If so, can you tell me how to do that?*

A. Both Google and Apple have built-in theft protection features. The latest Android 15 upgrade introduced Google's Theft Detection Lock, which uses AI to detect sudden movement (like if your phone is grabbed from you and the perpetrator runs off with it) and locks your phone in response. First, be sure you have a password on your lock screen. In your Settings, look for Security or Lock screen & security. Here you can set a password, PIN or pattern. To enable the new security feature open **Settings> Google> All services> Theft Protection. Turn** on Theft Detention Lock. This will work with phones running Android 10 or later. On iPhones, Stolen Device Protection kicks in when the phone is away from familiar locations, like home and adds extra security to prevent a

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

that we made up ourselves (continued)

thief from making changes to your account or device. Your phone will require FaceID sign-in (sorry, no password alternative so only YOUR face will unlock it). Security makes whoever has your phone wait an hour before they can change your Apple account password. That gives enough time to wipe your stolen phone remotely if you need to do so. If your iPhone runs iOS 17.3 or later, you can turn on Stolen Device Protection. Before doing so, make sure you have two-factor authentication on, Location Services enabled, FaceId or Touch ID on and Find My iPhone set up. Then go to **Settings> Face ID (or Touch ID) & Passcode** and **enter your passcode**. Tap **Stolen Device Protection** and turn it on. By default, Stolen Device Protection only works when your phone is away from your familiar locations (but you can override that for extra protection). Go to **Settings> Face ID (or Touch ID) & Passcode> Stolen Device Protection**. Under **Require Security Delay**, then **choose Always.**

Q. This might not fit the parameters of your newsletter or be worthy of consideration as a computer-related topic but I am going to submit it to you for consideration. This last year I've been saddled with health issues and my health insurance company has denied some of my submitted claims. I don't know what to do or where to seek help regarding them. Can you suggest anything?

A. Well, you are correct. We review computed related articles and information and pass along information that might be helpful to our members. We rarely make any recommendations regarding specific products or equipment. While your question is not necessary computer related, there happens to be an open-source platform that takes advantage of large language models to help users (like yourself) generate health insurance appeals using AI. So since AI is involved, along with computers, consider searching for Fight Health Insurance (fighthealthinsurance.com). Please let us know if that helps.

Q. We are new to SCA and recently joined the Computer Club. It has so much to offer. But we were wondering how the Club determines what classes it offers each month? Is there anyway to suggest topics for consideration?

A. Excellent question**.** Classes are offered depending upon what our members have indicated they are interested in or what our Instructors think might be helpful information that members might have an interest in. Some things, like Special Topics, are held on a regular basis. Classes are all geared to beginners unlike otherwise stated. If you have any recommendations, please, please share your ideas with us. Via the club website, **Contact Us** and **select Education.** We will consider all requests, dependent upon the amount of interest and available Instructors. If you would like to teach a class, be sure to let us know that also. We will provide Instructor Training (a prerequisite requirement) that will cover our operating procedures, etc. that will enable one to use our resources to conduct classes. Lastly, welcome to Sun City Anthem and our Club!