BITS AND BYTES

JANUARY 2023

https://mcc.apcug.org/

ARTICLE INDEX

GENERAL CLUB MEETING - VIA ZOOM

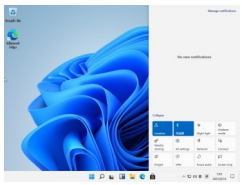
Wednesday, January 25, 2023
6:00 P.M.

Android Apps on Windows 11 – Well, I'll be!

By Phil Sorrentino, Secretary and APCUG Rep, Sun City Center Computer Club
https://scccomputerclub.org/ - philsorr (at) yahoo.com

Many apps that run on Android smartphones and tablets may soon be running on Windows 11 machines. As of February 2022, only in the US are Android apps available for Windows. A new addition to Windows 11, "Windows Subsystem for Android," will enable your Windows 11 device to run Android applications that are available in the Amazon App store. That may sound a bit confusing since Apps for Windows usually come from the Microsoft store. Be that as it may, this feature may eventually prove useful.

On



If your computer meets the requirements for Windows 11, it meets the requirements for Android Apps. (Make sure to check for any Windows 11 updates, and install them before proceeding with Android Apps.) Additionally, Windows 11 must have hardware virtualization enabled. Windows 11 essentially runs Android in a virtual machine, which is why this is necessary. (A Virtual Machine is a computer image-based software that can run programs and Apps.)

To check if your computer has virtualization enabled, go to the "Performance" tab in Task Manager (Ctrl+Shift+Esc). Then, open Task Manager, and click "More details" if you don't see the Performance information. If virtualization is not enabled for a computer using an Intel CPU, you can enable Intel VT-X in your computer's UEFI firmware (BIOS). If your system uses an AMD CPU, look for AMD-V in the UEFI firmware settings.) Four of the six computers that I checked had virtualization enabled.

If you are part of the Windows Insider Program, you may have already experienced Android apps for those more technically inclined. So far, the Windows Insider Program has been testing the capability with fifty or so popular Android Apps. Eventually, you will see the "mobile" Apps in the "new" Microsoft store, though currently, the download will come from the Amazon App store. Articles in the literature indicate that once downloaded, you can run these apps side-by-side with the help of the new Snap Layouts feature of Windows 11. And you'll be able to pin them to your Start menu or Taskbar and interact with them via a mouse, a touch screen, or an input pen. Also, you will be able to share your clipboard between Windows and Android Apps, and you will be able to see notifications from Android Apps in the Windows Notification Center, which sounds like a pretty comprehensive integration into the Windows 11 environment. Why would you need a mobile App when you have plenty of Apps on your desktop computer? Well, there may be some mobile Apps that don't have a desktop equivalent. Early results of the Windows Insider Program highlighted a few areas that may be interesting, such as Games, Reading books with Kindle, and content for kids, such as teaching math, reading, and writing skills. The Windows Insider Program encourages developers and creators to develop Apps for this new Windows 11 environment.

For those of you who would "lean in" to a technical discussion, this paragraph is for you; others might want to skip this paragraph. Just a little "techno-talk," Windows 11 will soon be enhanced by adding a new component. This new component will be a subsystem that will essentially ride on top of Windows 11 and will be called the "Windows Subsystem for

Android." The subsystem will include the Linux kernel and an Android OS based on the Android Open Source Project version 11. It will be distributed through the Microsoft Store as part of the Amazon App store installation, allowing users to stay updated over time as the software evolves. The subsystem runs in a Hyper-V Virtual machine, allowing multiple Operating Systems to run simultaneously. End of 'techno-talk," suffice to say it will be a relatively sophisticated and complex software product. For example, one of the icons for Android on Windows looks like this:

So, for those who might be more adventurous, how do you install Android Apps on a Windows 11 computer? As always, there are YouTube videos on the subject which would be an excellent first step. After the videos, the first thing to do is open the Microsoft Store on your computer. Click the start button, find the Microsoft Store in the alphabetical Start Menu list, and click it to open it. In the App Store, search for Amazon App Store". If the Amazon App Store is not installed, you will have to install it. (Note that this could take a while. A pop-up will appear and guide you through the process; click "Set up" and continue through the steps down to the App Store installation. The last thing to do will be a computer restart. After the restart, the Amazon App Store will automatically open. If it doesn't, you should find it in the Start Menu.) When installed, the first thing to do is to sign into your Amazon account if you have one. If you don't have an Amazon account, you can create one at this point. Once you are in the Amazon App Store, you will see that it works like all the other App stores you have used. (When I first installed the Amazon App store, I didn't find any App that I needed, but that was expected because, at that time, there was a limited number of Apps available, though we are told that many Apps are soon to come.) In the store, you will find free and not-free Apps. The free Apps will have a "Get" button; the not-free apps will have a button with a price. Navigate to an App you want and click the appropriate button. Click Install, and the App will download and then install. You can click "Open" to use the App when the installation is finished.

If you followed the directions and everything worked out, you have just installed your first Android App on a Windows device. The Android apps you downloaded can now be found in the Start Menu, just like Windows Apps. They can even be pinned to the Taskbar like regular Windows apps. But what about Android Apps that are unavailable in the Amazon App Store? Well, you can always "sideload" Apps, but that's a subject for another time.

Bluetooth Adapters – Do I need one?

By Phil Sorrentino, Secretary and APCUG Rep, Sun City Center Computer Club
https://scccomputerclub.org/
philsorr (at) yahoo.com

The short answer is no if all your devices have Bluetooth incorporated in them, but yes, if you have a non-Bluetooth device that you would like to use with other Bluetooth devices. A Bluetooth adapter allows a non-Bluetooth device to work with a Bluetooth device. The adapter does this by providing Bluetooth electronics for the non-Bluetooth device. Bluetooth is a wireless communications standard for interconnecting electronic devices. It allows devices to connect wirelessly over a range of about 100 ft. This wireless connection can be

beneficial if devices are in separate rooms in a house. But that's the technical side of Bluetooth. Most of us know Bluetooth as how our smartphones connect to the radio system in our cars to provide "hands-free" phone conversations. This is probably one of the most extensive uses of Bluetooth today, but there are other uses. Two other uses of Bluetooth that come to mind involve listening to music; wireless headphones or earbuds and wireless (Bluetooth) speakers.

As implied above, Bluetooth is included in Apple and Android smartphones. Bluetooth is a convenient way to connect a smartphone to a listening device like headphones or a speaker. (In fact, some smartphones like the Apple iPhone XS, the Google Pixel 3, and the Motorola Moto Z3 don't even have a 3.5 mm wired headphone jack, making Bluetooth the only way to connect these devices to headphones.) Headphones are a convenient way to take advantage of a smartphone being used as a music player. Start the phone's music app, put on the headphones, and enjoy the music. Apple wireless headphones are very noticeable. Apple AirPods, as they are called, are typically white and look like someone cut the wires going to each individual headphone. Besides Apple, many other wireless headphones are available from Sony, Bose, LG, Jaybird, Optoma, Beats, and others. Using Bluetooth headphones, you replace the wires needed with standard headphones with the wireless Bluetooth connection. That way, no wires are going from your head to your phone, which might be in your hand or in your pocket, which might get in your way. (With some of these wireless headphones, there is still a wire going from one headphone to the other that usually goes behind the head.)

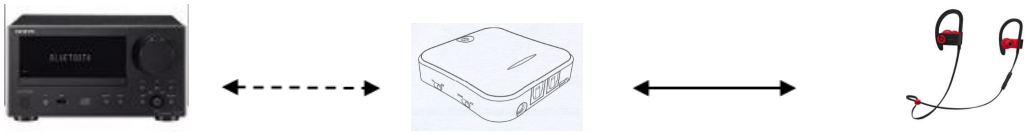
Bluetooth Speakers - the other use for Bluetooth. Speakers that have Bluetooth included are sold as Bluetooth or Smart Speakers. There are many of these available from Sony, JBL, Sonos, Bose, and others. Most of these speakers are powered by batteries, so they are portable, and you can use them anywhere. Many are waterproof, encouraging their use at the beach or around the pool. These speakers contain Bluetooth electronics, which allow them to connect to a device such as a smartphone or a computer and be used in place of the speaker(s) on the device to provide the sound. So, if a Bluetooth speaker is connected to a smartphone and a music player app on the smartphone is started, the music will be heard on the Bluetooth speaker. A Bluetooth speaker is usually much more powerful than the small speaker on the smartphone, and the quality of the Bluetooth speaker is typically much better than that of the smartphone speaker, so the listening experience may be more enjoyable. And if the Bluetooth speaker is powerful enough, it may even be used to fill a large room and entertain many people.

Wireless headphones and Bluetooth speakers are quite helpful when used with a smartphone or a computer with Bluetooth electronics embedded, but what about those devices that don't have Bluetooth electronics included, like an older stereo receiver or a radio? Well, this is where Bluetooth adapters come into play. Bluetooth adapters allow you to listen to your non-Bluetooth stereo or radio using your wireless headphones or Bluetooth speakers. The adapter provides the Bluetooth electronics needed to connect to other Bluetooth devices. Bluetooth adapters from Logitech, Taotronics, Trond, 1Mii, and others should cost less than $50. Except for the inexpensive items, most adapters can be used as a Bluetooth Transmitter or a Bluetooth Receiver. When the adapter is used with a non-Bluetooth source of audio (like a stereo), it is being used as a Transmitter. When the adapter is used with a non-Bluetooth device that receives the audio (like a powered speaker), it is being used as a Receiver. Adapters are powered by wall power or battery, or both. If your stereo is not portable, you probably don't need a portable adapter. (Be aware that some less

expensive portable Bluetooth adapters cannot charge their battery and operate as a transmitter at the same time.)

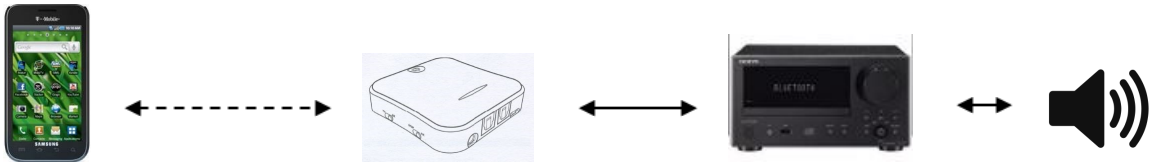
Setting up the adapter to function as a transmitter is pretty straightforward. First, the audio output from your non-Bluetooth stereo gets connected to the adapter's input, typically with a 3.5 mm stereo cable. (Some more expensive adapters even support optical audio.) Then when you go through the pairing and connecting process, the audio from the non-Bluetooth stereo will be audible in the wireless Bluetooth headphones. (In the diagram, a Bluetooth speaker can be substituted for the headphones, and you would have audio as loud as the particular speaker could provide.)

Bluetooth Adapter used as a Transmitter



Non-Bluetooth Stereo Bluetooth Adapter Bluetooth Headphones

Many adapters can also allow a non-Bluetooth device to operate with a Bluetooth audio device as the audio source. In this arrangement, the adapter is used as a Receiver. The non-Bluetooth device receives the audio from a Bluetooth device via the Bluetooth Adapter used in the Receive mode, as shown in the following.



Bluetooth Device Bluetooth Adapter Non-Bluetooth Stereo

So now, do you need a Bluetooth Adapter?

Are Free Public Phone Charging Stations Safe?

'Juice Jacking' Might Load Malware on Your Phone or Tablet as It's Charging

by Kurt Jefferson, Kurt Jefferson, Editor, Central Kentucky Computer Society
https://ckcs.org/ lextown2 (at) gmail.com

You're on a layover at a major airport when you realize your iPhone or Android smartphone's battery is draining fast, and the battery power is down to single digits.

The battery icon has just turned from green to red, meaning your phone is nearly drained. Soon it will be as useless as an electric kettle in a cave.

There's a convenient public charging station nearby. You're in a bind. Your jet leaves in half hour. And yet you've read about the dangers of charging your phone or tablet at a public charging station. So what's a person to do?

How can you be sure the public charging station is safe? Reviewed.com reports, "As the latest security alerts prove, USB cables and chargers are like chewing gum—if you find it lying around in public, don't use it. It's not free candy. The Los Angeles District Attorney recently warned that charging your phone via

those public USB ports can lead to "juice jacking." That's when hackers use the connection to transmit dangerous malware onto your device and steal your personal information or data."

Reviewed.com's executive editor, T.J. Donegan, recommends an alternative. He recommends you buy a USB portable battery pack, "many of which can even charge laptops on the go–so you don't have to crowd around the one outlet with 15 other people."

Reviewed.com recommends what's called the Jackery Bolt portable battery pack. It says the portable battery pack "has an incredibly high capacity that can charge your phone three times over (!!) before the charger needs to be recharged. Plus, it's slim and compact, so it's easy to tote around and has multiple ports so you can charge more than one device at a time." Amazon currently sells the Jackery Bolt for $32.99.

The Wirecutter, a website that reviews and tests nearly everything (and purchased by The New York Times), gives high marks to the Zendure SuperMini 20w Power Bank. Amazon currently sells this model for $45 (using the Amazon on-page clipped coupon.) The Wirecutter writes in its Zendure review, "about as small and lightweight as a power bank can be while still offering enough capacity to juice up most smartphones up to three times. Its USB-C Power Delivery (PD) port can charge most handheld devices (and recharge the power bank itself) at top speed with the included USB-C cable and a compatible wall charger (the one that came with your phone will work). The USB-A port can handle any older, non-USB-C devices you might have kicking around, too."

The HyperJuice 18W USB-C+ Lightning Battery Pack also gets a good Wirecutter review. It contains built-in cables, so you don't have to mess with cables that can easily get lost, tangled, or misplaced. It's currently $60 from the Hyper website.

The Wirecutter also gives thumbs up to the TravelCard Charger, which sells for $30 from TravelCard. "It has the lowest capacity of any power bank we've tested," writes The Wirecutter, but the review claims it's the best portable charger "for someone who wants to have an emergency boost of power always on hand."

Reviewed.com:
Here's Why You Should Never Use A Public Phone Charger
Public charging stations for your phone: Are they safe? - Reviewed (usatoday.com)

The Wirecutter:
The Best Portable Chargers and Power Banks for Phones and Tablets
The 4 Best USB Power Banks for Phones and Tablets 2023 | Reviews by Wirecutter (nytimes.com)

FBI Issues Warning Over Public Charging Stations
The FBI says don't do it even if you're tempted to use a public charging station so your phone or tablet won't die on you.

It's a risky business, according to the team at the FBI, watching malware spread on mobile devices throughout the U.S. and abroad:

"Cybersecurity experts have warned that criminals can load malware onto public USB charging stations to maliciously access electronic devices while being charged. Malware installed through a dirty USB port can lock a device or export personal data and passwords directly to the perpetrator. Criminals can use that information to access online accounts or sell it to other bad actors."

FBI tech experts add, "Don't let a free USB charge wind up draining your bank account." Here are some tips to help you avoid becoming a juice-jacking victim:

- Avoid using a USB charging station. Use an AC power outlet instead.
- Bring AC, car chargers, and USB cables with you when traveling.
- Carry a portable charger or external battery.
- Consider carrying a charging-only cable from a trusted supplier, which prevents data from sending or receiving while charging.

Fixing a Nasty Computer Hack

David Kretchmar, Hardware Technician
Sun City Summerlin Computer Club - https://www.scscc.club - dkretch (at) gmail.com

I recently completed a repair on a club member's computer after he allowed a "helpful" technical representative, probably from the other side of the world, to remotely access his computer. Unfortunately, the victim in this case apparently failed to read or heed my article in the November 2021 *Gigabyte Gazette* (https://www.scscc.club/Gigabyte/gg_2021-11Nov.pdf) warning that these types of scams were becoming increasingly prevalent.

The "bait" in this instance was an official-looking email, supposedly from Cox, stating that the victim had been substantially overcharged on his Cox bill and he was due a refund of $400. The victim telephoned the scammer using the phone number in the email. Next, he went online and downloaded and installed remote access software at her instruction. He then allowed the purported technical representative to initiate a remote access session and log into his system. The victim began to feel uneasy when he saw that things were being done on his computer that had nothing to do with Cox. He finally became alarmed and hung up on the scammer when she asked for his bank account information "to process his refund."

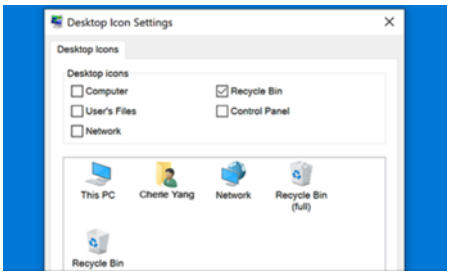
Unfortunately, this victim did not immediately shut off his computer, so the scammer could continue to mess with his system remotely, I suppose as a departing coup de grace for a failed scam. The victim could no longer access his computer, which displayed the Windows 11 "Gray screen of death" right after he entered his PIN during login. Microsoft has finally replaced its famous "Blue screen of death," which provided a bit of mostly useless information, with a "Gray screen of death," which provides no information.

The victim, who runs an online business, called me in a panic. This was especially interesting to me since I have had minimal experience working with pooched Windows 11 machines. I was curious to see if there was a substantial difference in addressing issues in Windows 11 versus Windows 10 (there was not, at least for this user's issue).

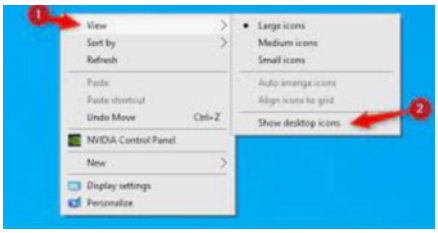
I researched the gray screen issue online and did not find much helpful information. Many writers suggested the problem was bad video drivers or a bad hardware connection. I knew there was no physical issue since the miscreant obviously never had physically assessed the victim's computer. And I doubted the graphics card drivers were the problem since messing with them would cause an immediate catastrophic system failure, even if it could be done remotely on the fly. After providing answers that did not solve the issue, many sites did offer to sell me their software, which they said would fix the problem. No thanks.

I finally decided to approach the Windows 11 system the way I would Windows 10. Getting past the gray screen of death was straightforward; I booted into Safe mode and repaired the Windows

startup. When I finally got into the victim's computer, I removed the remote access software. Then I did a system refresh, keeping all of his original data files and programs but replacing all of the system files. I wanted to assure the club member that there were no nasty surprises on his system due to his encounter with the scammer.



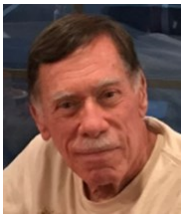
Yet when I could finally boot to the victim's desktop, I saw something very strange. The victim's desktop icons, files, and folders had disappeared. I considered that the scammer could have put the victim's computer in tablet mode, which messes up the desktop. I learned that Windows 11 does not have a dedicated tablet mode. Again, an online search for the problem was mostly useless. Most writers suggested going to Personalize themes, Icons and checking the icons I wanted to appear on the desktop. This did not address the issue of nothing showing on the desktop, files, folders, and icons. Naturally, many of those offering useless advice online had a software package to sell, which they assured would fix any problems. Again, no thanks.



I found an article that suggested I right-click on the desktop, left-click on View (#1), then make sure "Show desktop icons" was checked (#2). Yes, that sneaky scammer had hidden everything on the victim's desktop with three clicks of her mouse. However, when I left mouse clicked on "Show desktop icons," the victim's desktop appeared normally. This was the first time I had seen a scammer throw two problems onto a victim's computer.

When contacted, a scammer will often state that to help you, they must remotely access your system. They will try to get you to download remote access software that will give the scammer access to your computer. Just say NO! There are few legitimate reasons someone needs to access your computer to provide assistance.

I mentally divide computer hacks/scams into two categories: tarantulas and scorpions. Tarantulas are big and scary looking, yet their bite is virtually harmless to humans. The most dangerous scorpions are the tiny ones you are likely not to see until they have stung you, and they can send you to the emergency room or at least to bed for a day or two. The unfortunate victim in this story ran into a scorpion that stung him twice. The sting would have been even worse had he allowed them access to his bank account.



Freshly Squeezed Reviews

Freshly Squeezed Review: Podcasts That Uncover Buried Treasure | YMP Now
By Frank Petrie, Jr. - June 1, 2022

In this review, I want to tell you about three podcasts I have found indispensable. They range in length anywhere from 7 minutes to 15 minutes. However, they have in common one thing: revealing hidden, extremely productive features cloaked in Apple's apps. Features turn what you thought was a basic, mundane, unimaginative app into a tiny, powerful gem.

And that's the reoccurring theme that draws me to all three of these podcasts. You'll find that Apple has quietly "borrowed" features from other third-party apps and incorporated them into

their stable of included apps to make them much more valuable. You only have to know where the treasure is buried.

1) ScreenCastsOnline. (DISCLAIMER: I'm a contributor to their monthly magazine.) ScreenCastsOnline has been around forever. Every Tuesday, they produce short tutorials; on Fridays, they produce half-hour deep dives. In addition, ScreenCastsOnline has numerous presenters who will walk you through apps that you never heard of and show you how they could possibly fill a hole in your everyday computing life.

But I would like to focus on the short-length Tuesday episodes. These cover a range of topics. For example, many episodes introduce you to apps you weren't aware of that are included in your Setapp subscription. Once introduced to said app, you're taken through its paces and how it could benefit your daily routine. And when Apple releases a new macOS, they like to point out new features added to some apps as basic as Notes.

(ScreenCastsOnline requires a subscription that avails you of a back catalog of their podcasts and magazines. It also has its own Mac, iOS, and Apple TV apps for consumption.)

2) Macmost. Hosted by Gary Rosenweig, Gary takes this idea and gives it a slight twist. He'll not only show you things you didn't know you could do with something like Number's tables but proposes simple yet innovative ways to incorporate them into your professional or personal workflow.

The fun part is he starts with, "I was wondering if… ". He then tells you what he's setting out to achieve, explains his thought process on accomplishing his objective, and finally, the solution he arrived at to make it a reality. Even if you don't wind up using the formula he figured out, it's fascinating to simply watch his process of sussing out the problem. He reminds me of Bill Nye, the Science Guy, only with a keyboard.

3) Proper Honest Tech (YouTube). I stumbled on this channel a month ago but was immediately hooked. So much so that after one episode, I started in with binge-watching. The host uncovers so many buried features in Maps alone; I have watched that episode alone numerous times with my iPhone firmly in hand, learning every uncovered function available.

It's not unusual for me to finish an episode of these podcasts and start deleting apps that can be accomplished with Apple's provided apps once you know how to achieve the same outcome you had procured the third-party app for. One less app means more space on your drive and possibly one less thing to irritate your collection of apps or your OS.

Take part of your afternoon and check them out. You won't regret it.

Interesting Internet Finds -- May 2022

By Steve Costello - scostello AT sefcug.com

While going through more than 300 RSS feeds, I often encounter things I think might interest other user group members. The following are some items I found interesting during May 2022.

Amazon Dropping MOBI Support On Send To Kindle Apps
https://blog.the-ebook-reader.com/2022/05/03/amazon-dropping-mobi-support-on-send-to-kindle-apps/
Kindle users do not panic! MOBI files on your Kindle will still be readable. All this means is that you will no longer be able to use 'send to Kindle' apps to send MOBI files to your Kindle.

I Lost My Phone With My Second Factor For Authentication. How Do I Recover?
https://askleo.com/i-lost-my-phone-with-my-second-factor-for-authentication-how-do-i-recover/
I know some people are hesitant to use two factor authentication for this reason. Leo explains how he would recover from that scenario. (Note: I use 2FA everywhere I can, and have not had a problem. The key is to think about how to handle this and prepare for it before it ever happens.

Gas Prices In Google Maps: Here's How To Find Them
https://9to5google.com/2022/05/13/how-to-find-gas-prices-with-google-maps/
With the price of gas on the rise, it is even more useful to be able to find the best price. This post shows how to find gas prices while using Google Maps. (Note: This knowledge came in handy during a recent road trip. Prices differed by over twenty cents a gallon within a hundred miles during the trip. Without being able to see the prices in Google Maps, I would have almost surely spent a lot more for gas.)

Android Cellular Data Not Working? 8 Ways To Fix
https://helpdeskgeek.com/help-desk/android-cellular-data-not-working-8-ways-to-fix/
It is not a question of if, but when your android cellular data will stop working. When it does, refer to this post for cures most likely to work. (Note: I lose my android cellular data at least once a month for some reason but usually get it back in minutes using one of these fixes.)

Is It Dangerous To Use Free Stock Photo Websites?
https://www.plagiarismtoday.com/2022/05/18/is-it-dangerous-to-use-free-stock-photo-websites/
This is an interesting article for the editors and bloggers that use photos from stock photo websites. Just because it is free from a stock photo website does not mean it is safe to use. Check out the advice in this post before using just any stock photo website photo.

****

Most of Us Get It Wrong: Not Just Teenagers Depend Upon the Internet

By Kurt Jefferson, Editor, Central Kentucky Computer Society
https://ckcs.org/ - lextown2 (at) gmail.com

70% of seniors are now online and using technology, reports the World Economic Forum in July 2019. When it comes to the Internet, the website claims it's – No Longer Just For the Young.

"Young people may roll their eyes at older people who can't use technology as fast as they do, but it's wrong to say that older Americans can't use technology. Remember, a baby boomer, Tim

Berners-Lee, invented the World Wide Web, so why should we be surprised that they continue to create, adapt, and use new technology?" reports the World Economic Forum.

In January 2022, Pew Research revealed its latest technology poll results. It discovered: "When it comes to internet use, virtually all adults ages 18 to 29 now say they use the Internet (99%). A similar share of those 30 to 49 (98%) say the same. And 96% of those 50 to 64 use the Internet, compared with 75% of those 65 and older who report being internet users."

So, if you're over 50 and depend on the Internet, how do you protect yourself against the onslaught of cybercriminals who want your money? Let's start with good advice from Reviews.org.

First off, don't share your information online. I'm amazed at the number of folks who scream to the world on Facebook or Instagram that their baby is due on a specific date. Isn't that an invitation to a burglary? I mean, mom and dad are obviously at the hospital. Who's at home watching the turf? Just don't make major personal announcements on social media. You're visiting New Zealand over the summer? Keep it to yourself. Why in the world would you list your departure and return dates online? Talk about an opportunity for burglars.

Before clicking on a web link, hover your cursor over it. You should see where the link takes you in your browser's status bar. This prevents you from visiting a rogue website disguised as a legitimate one.

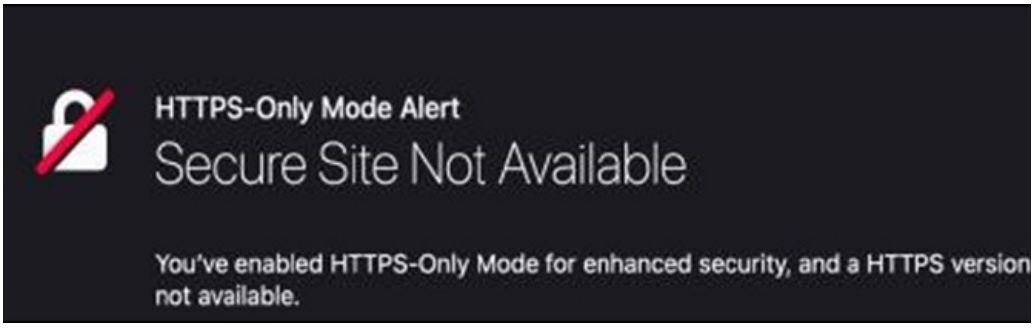
Use only secure public websites and a trusted VPN (virtual public network.) Logging onto unsecured Wi-Fi at a motel, restaurant, library, or airport is just crazy. If you must log onto an open wireless network, ensure your VPN is up and running. (I use a VPN even when a Wi-Fi password is required.)

Experts say you should only log onto websites that begin with https:, but this isn't always possible. For example, if I visit a specific school from the home page of the largest school district in central Kentucky, the page won't automatically load on my version of Firefox. I have a Firefox add-on installed called HTTPS Everywhere, which blocks the page and tells me it's not secure.

A button allows me to continue to the http-only site, but the browser add-on is a red flag alerting me to a possible security problem.

There are plenty more basic security tips on the Reviews.org page. Check them out if you want more security suggestions.

Just because you're over 50 doesn't mean you have to fall for traps designed to steal your money. Be smart. Be safe. Be vigilant. Scammers are out there, even if you cannot see them.



QR Code Scams – Be careful where you point that smartphone

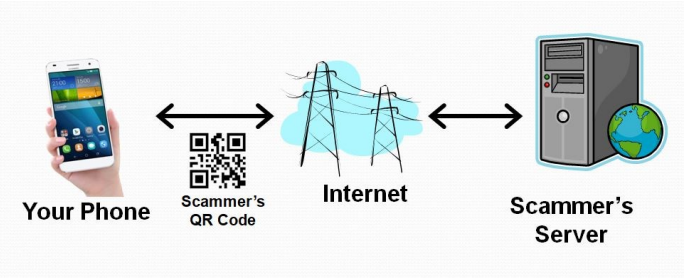
By Phil Sorrentino, Secretary and APCUG Rep, Sun City Center Computer Club
https://scccomputerclub.org/ - philsorr (at) yahoo.com

QR Codes seem to be everywhere today. You'll find them anywhere someone wants to give you more information than is possible by other means, like a sheet of paper or a machine-readable standard bar code. Initially, QR codes were created to track manufacturing processes where barcodes couldn't store enough information. However, a bar code has one dimension. A QR code is 2-dimensional and can store significantly more data than a bar code. Roughly speaking, a QR code may contain as many as 7,000 characters as opposed to a bar code that may contain up to around 40 characters. That's over 170 times the amount of data. This increased amount of information makes the QR code so worthwhile.

QR codes were invented in Japan in the 1990s. They were first used by the automotive industry to manage production but have spread everywhere. There are even websites and apps that let you make your own. A QR code is a machine-readable, 2 dimension matrix of black and white squares. A QR code may represent many different data types, such as text, a hyperlink to a website, a telephone number, an email address, or a text or email message. QR codes, like billboards, clothing labels, walls, TVs, and even tattoos, can be placed on almost anything. QR stands for Quick Response. Quick Response comes from the manufacturing industry and deals with how fast a product can be replaced on the seller's shelves. Quick Response is *"the rapid replenishment of a customer's stock by a supplier with direct access to data from the customer's point of sale." A QR code is merely a data storage representation of some information using the binary code. (For example, the letter A is represented by "01000001") The little squares and patterns of the QR code represent the binary information. The actual QR code is read-only, so it cannot record or steal any personal information on its own. Nowadays, the smartphone's camera app can scan the QR code when the camera is directed at it. (Most smartphones no longer have to download a separate app from the App store for reading QR codes.)*

A QR code with an embedded hyperlink to a website can connect you to a specific website quickly and easily using your smartphone. There is very little one needs to know to take advantage of a QR code. But a lot of the latest technology is being used to accomplish the task. The three major technology components are your smartphone, the internet, and a server (on the internet, or "in the cloud"). This collection of technologies goes by the name "Client-Server Technology," and all three components have been developed to work together. For example, your smartphone has a camera App that connects the smartphone, as the client, to the server website whose URL was embedded in the QR code. (URL is the Universal Resource Locator, the term for a web address on the internet.) This allows the provider of the QR code the ability to connect your phone with the QR code provider's server when you scan the QR code. Once connected to the server, the smartphone can access all the information that the server can provide.

QR codes take people from the physical world to the online (cyber) world. They let smartphones connect to an enormous world of information quickly and easily, but unfortunately, they also allow smartphones to connect quickly and easily to a scammer's website. This is why scammers have started using QR codes in attempting to get in touch with potential victims. It gets people online with the scammer's server. It is similar to "phishing" emails and telephone calls. QR codes are another way for scammers to get in touch with potential victims.



Many scammers (aka cybercriminals) have started to exploit the technology's convenience. Scammers create malicious QR codes to connect unwitting consumers to the scammer's server and dupe them into divulging their personal information. Anytime new technology comes out, cybercriminals attempt to find a way to exploit it. This is especially true with technology like QR codes. It seems like most people can figure out how to use them, but they probably don't really know how they work, and it's always easier to manipulate people when they don't understand their technology. Scanning the scammer's QR codes won't do anything malicious to your smartphone, such as installing malware. Still, it probably will take you to a website designed to try to get personal or financial information from you.

Like any other phishing scheme, it's impossible to know precisely how often QR codes are used for malicious purposes. Experts say they still represent a small percentage of overall phishing, but numerous QR code scams have been reported to the Better Business Bureau. As a result, many people know they need to be on the lookout for phishing links and questionable attachments in emails that purport to be from your bank. But thinking twice about scanning a QR code with your smartphone camera isn't second nature for most people yet.

Recently a QR code scam was uncovered in a Texas city. Drivers were led to a scammer's website after scanning a QR code sticker on a parking meter. Eventually, around 30 such stickers were found. The QR code was supposed to help the motorist pay for online parking. However, instead of being taken to the city's authorized website, the motorist who scanned the fake stickers was led to a fake website that collected their credit card information. With a warning of the parking meter scam, officials in another city issued a warning to motorists after spotting similar stickers on parking meters.

Fake QR codes have even shown up in emails. Scammers may like using QR codes in phishing emails because they often aren't picked up by security software, giving them a better chance than attachments or bad links to reach their intended targets. It boils down to QR codes being just one more way for cybercriminals to get what they want and yet another threat for people to be on the lookout for.
So be careful when scanning QR codes. Here are some tips from security experts. Think before you scan. Be especially wary of codes posted in public places. Take a good look and determine if the sticker is part of the sign or display. If the code doesn't look like it fits in with the background, it may have been put there by a scammer. Be suspicious of any QR code that comes in an email. If you scan a QR code, look at the website it led you to and determine if it looks like what you expected. If it doesn't look appropriate, then leave the website. If it asks for personal information you don't think is appropriate, don't provide it. And, in the words of one of the Computer Club's past presidents, Matt Batt, "Be careful out there!"

Microsoft Windows in "S Mode"

News and/or Opinion from the SHCC Editor
By Paul Baecker
September 2022 WYSIWYG issue - http://www.SterlingHeightsComputerClub.org
Newsletter (at) sterlingheightscomputerclub.org

Someone recently asked me for my opinion on a sale-priced laptop at a local store and whether I'd recommend its purchase.

An HP laptop with an Intel i5 CPU with a Passmark rating of 691, 8GB of RAM, 256GB SSD, 17" screen, Windows 11, backlit keyboard, and full HD display. All in all, a decently powered mobile PC on sale for only $399, advertised as "$300 off their regular price."

What could be wrong with this selection?

Windows 11, that's what could be 'wrong' with this selection. However, looking closely at the specifications of this offering indicated that the version of Windows 11 that came installed on this laptop was "Windows 11 Home in S Mode."

I had never heard of "S Mode," so this would be a new education for me. "S Mode" (Windows 10 or 11) basically limits you to accepting applications only from Microsoft. However, they say that "S mode is designed for security and performance, exclusively running apps from the Microsoft Store. So if you want to install an app that isn't available in the Microsoft Store, you'll need to switch out of S mode".

But this laptop isn't such a bad purchase after all (if you are on a budget and accept the small drive size and the middle-of-the-road Passmark CPU score) because you can "leave" Windows S Mode at any time. This will result in your new PC having the full Windows Home edition. The only caveat is that you cannot reverse this decision. But I suspect that for most PC users, this would be the right permanent direction to go anyway.

See below links to review articles about Windows S Mode (for Windows 10 and 11) — what it is and how to leave it.

When shopping for a new PC, always study the specifications sheet for each of your purchase candidates so that you don't encounter unexpected surprises after your eventual choice. But be aware that the specifications list for a PC on any particular store's website may not be complete, and some of the spec info listed there may also be inaccurate (which happens too often!), so double-check the information about your potential purchase, perhaps on the PC manufacturer's web site.

Also, purchase from a retailer that offers a return policy without any restocking fee. In my opinion, if you can't test-drive your selection in the store, you should be able to do so at home and return it at no charge if it doesn't meet your expectations. (Be sure to delete all your files and footprints before returning the device! Maybe even re-install the Operating System on it to accomplish that entirely.) Most retailers offer a free 14-day return policy. Costco offers a very generous 90-day return policy (as well as great sale prices on equipment).

Switching out of Windows “S Mode” results in a full Windows Home edition and cannot be reversed.
https://support.microsoft.com/en-us/windows/switching-out-of-s-mode-in-windows-4f56d9be-99ec-6983-119f-031bfb28a307#WindowsVersion=Windows_11

Windows 10 and Windows 11 in S mode FAQ - Microsoft Support
Some low-cost Windows PCs and tablets ship with Windows 11 Home in S Mode. Here is the process for switching out of S Mode.

https://www.pcworld.com/article/545076/how-to-switch-out-of-windows-11-in-s-mode.html