PATACS is a member of
apcug
Association of Personal
Computer User Groups
www.apcug.org

PATACS Posts

Club info: Call
703-370-7649
www.patacs.org

Newsletter of the Potomac Area Technology and Computer Society

My turn……

In the December 2024 issue, I edited John Krout's article in a way he felt was unwarranted—in that I put registered trademark (®) symbols next to the phrase "At-a-Glance". In my defense, I was trying to protect the Society from having Acco come after us for trademark infringement. There were a couple of problems with my logic—or more precisely—a lack thereof. The main one was that Acco no longer holds the trademark on the phrase. The second was that I couldn't reach John and published the unapproved changes anyway. He was not a happy camper with me, which I understand and he asked me to publish an apology. So this is it. **John, I'm sorry I published your article without checking with you first**. I have assured him it won't happen again.

In re-reading, the published version of the January's issue, I see that somehow the phrase "ISO" entered the description of the image on page 14. It should have been "Canon", not "ISO".

And now we know about the Commanders. Josh Harris said the name will stay. ☹ Their fantastic run stopped at the NFL's NFC championship game against the Philadelphia Eagles, as I somehow knew in my heart, it would. The Commanders were good, but they're not good enough to overcome Philly...yet. By the time this is published, we'll know how the Super Bowl finished. In case you missed it. Kansas City was crushed by the Eagles, denying them a 3-peat (which is a trade-marked term: https://www.wikiwand.com/en/articles/Three-peat!)

The Society continues to look for anything you might want to publish. If you have something, please email it to me at editor@patacs.org.

Some of you expressed interest in my travels.

My wife and I were in Minnesota in mid-February to visit her family. We waited until the coldest week of the winter. High temps each day were just above zero. Fortunately, for them, by the time the weekend came they had a heatwave with temps in the 40s. We were home by that time, just in time for the 1st heatwave here.

Me? I'm headed to the Lofoten Islands in Northern Norway for a photo workshop in mid-March. All I know for sure is that it takes 2 days to get there and the weather is "changeable"!

Next printed issue: Late April, 2025

Table of Contents

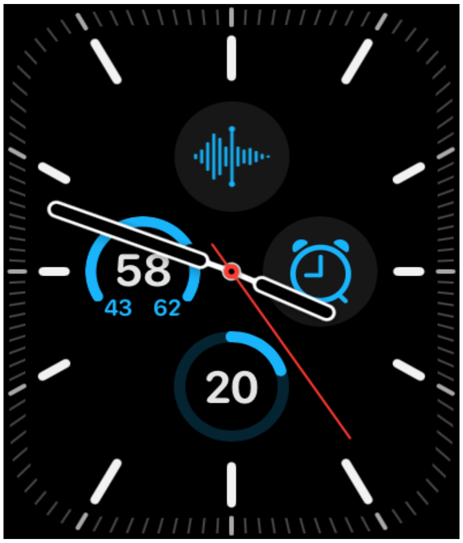
My turn...... 1
When Four Apple Watch Complications Just Aren't Enough.......... 2
Microsoft Windows 11 Copilot: How Not To Remove It.......... 2
Another Day. Another Scam. Don't Fall for it.......... 6
Do You Use Two-Factor Authentication? 7
Stop installing unwanted software. 9
Printing your photos.......... 11
Burned By Another Security Breach?..........13

Thank this issue's proofreaders: Jon Bernstein, Paul Howard, Lynda Soady, Nick Wenri, Henry Winokur

When Four Apple Watch Complications Just Aren't Enough

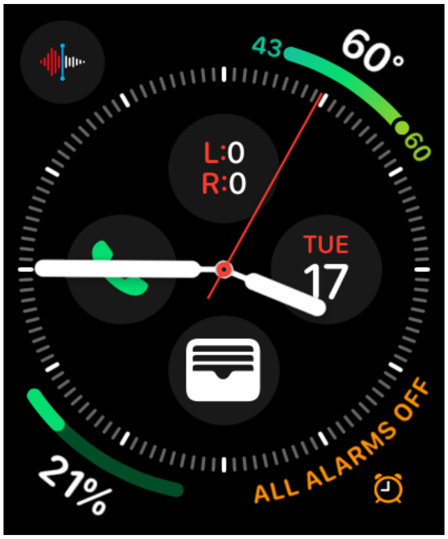
Gabe Goldberg, gabe@gabegold.com
Potomac Area Technology And Computer Society (www.patacs.org)

Apple provides many faces (designs) for its watches, ranging from simple to elaborate and functional vs. elegant. Icons on the watch face are called "complications" and provide quick access to Watch apps such as (shown on the Meridian face—left): Battery, Voice Memos, Temperature, and Alarms. For several years, four complications sufficed for me—especially since I didn't know that more could be accommodated—until I heard someone mention that. So I switched from the **Meridian** face to **Infograph**, adding Hearing Devices, Phone, Today's Date, and Wallet. Even in small Watch-face screen real estate, complications are easily accessed to conveniently invoke functions.



← **Meridian**
watch face

Infograph
watch face →



###

Microsoft Windows 11 Copilot: How Not To Remove It

by John Krout, Potomac Area Technology And Computer Society (www.patacs.org)

Introduction

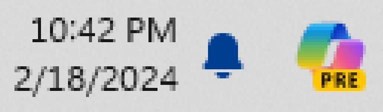
Automatic installation of un-requested software is a behavior I don't like.

Microsoft forced a double whammy on my Windows 11 desktop computer in February 2024. During the February 17th PATACS+OPCUG joint monthly meeting, which was Zoom-only, Zoom froze and a minute later, it was apparent the entire computer was frozen. I pulled the power plug and then re-plugged it. As the computer rebooted, it installed a Windows 11 operating system update. The download of that update probably caused the initial freeze.

After about 10 minutes, I was able to rejoin the Zoom meeting.

After the meeting, I checked Settings on the computer. I found what I expected: long ago, I had used Settings to create a "NO UPDATES" time range of 9 AM to 2 AM daily. Microsoft led me to have faith in that setting and then clearly ignored it.

One day after the meeting, I found an unfamiliar icon in the right corner of my Windows 11 taskbar. You can see it to the right. The icon is on the right and includes the letters PRE.



A click on the icon revealed a "preview" of Microsoft **Copilot**, their generative Artificial Intelligence (AI) brand. Either a left-click or right-click on the icon opened a tall, thin dialog window, inviting me to ask a question.

I also found a scalable Copilot logo graphic in the C:\Windows folder tree: Obviously, Microsoft wants to beat its generative AI competitors to desktops. The competitors include mega-firms like Google, Adobe, and Autodesk and startups like OpenAI.

Where does AI do its work?

In a nutshell, today (Ed's note: *early*-spring, 2024) and for the indefinite but no doubt long future, AI will be executed on servers, not your computer. Personal computers just don't have the hardware for storage and execution of generative AI.

Consider the following consequences of that situation.

First and foremost, those servers will capture and retain EVERYTHING you use AI to accomplish, and maybe a lot more (see third consequence). The owners of that AI service and servers will seek to monetize that valuable information about you.
(I am against such monetization.)

Second, AI services won't be available everywhere because the Internet isn’t available everywhere. Certainly not where cell towers are blocked by terrain or are overloaded. And laws may prohibit the use of generative AI in some locations, especially overseas.

The **third** consequence is speculative, I admit. I wonder if Copilot will be running behind the scenes, invisible to the user, monitoring the use of non-Microsoft apps, listening to conversations through microphones, and watching through webcams. Microsoft sees profit in such behaviors.

I see violations of privacy and unwarranted use of bandwidth that I pay for.

My first interactive generative AI experience

You can see my dialog with Copilot below. My input is identified as ***You***. I added the italics to clarify the two major sub-headings in the generative AI answer.
As you will see below in the dialog, the answer was incomplete. Perhaps I should have asked how to remove the Copilot preview *from my computer*. Maybe I should be glad that the AI could not read my mind.

You:
how to remove the Copilot preview

Copilot:
Certainly! If you'd like to remove the Copilot preview from your Windows 11 taskbar, there are a couple of options:

Remove Copilot from Taskbar (Temporary):

This method will hide the Copilot icon from your taskbar without completely deactivating it.

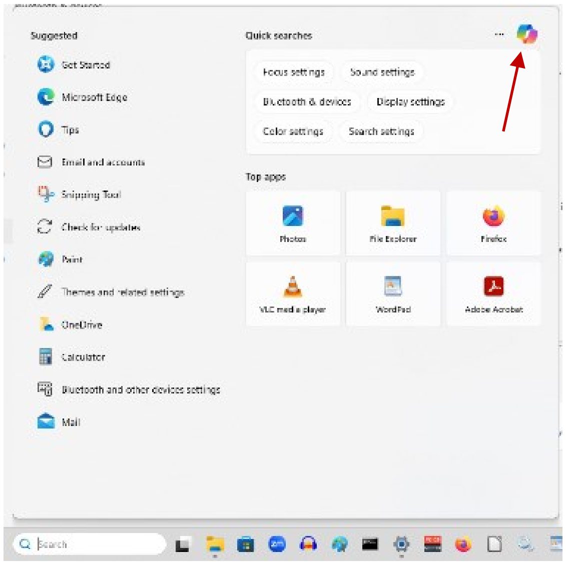
Follow these steps:
Open the Settings app (you can search for it in the Start menu).
Click on **Personalization**.
Scroll down and select **Taskbar**.
Toggle off the Copilot option.

Disable Copilot Completely (Permanent):

If you want to **permanently disable Copilot**, follow these steps:
Click on Start and **search for gpedit** to open the Group Policy Editor.
In the left-hand panel, navigate to User Configuration > Administrative Templates > Windows Components > Windows Copilot.
Double-click on Turn off Windows Copilot in the right-hand panel.
Click Enabled, then click Apply and OK.

Remember that if you ever want to enable Copilot again, you can follow the same steps and choose "Not configured" or "Disabled" instead of "Enabled" in the last step.
That's it! If you need further assistance with Windows, feel free to ask. 😊
<end of dialog>

I did try the permanent removal option. I encountered a problem: **gpedit** was not found on my Windows 11 computer. I searched on the Windows Store and did not find it there. It appears to be part of Windows 11 Pro only. I am disappointed that Copilot did not say so. I searched the Web and found a page of scripts for installing **gpedit**, one for Windows 10 and one for Windows 11. When the script is finished, I can start **gpedit** by typing **gpedit.msc** in the Windows 11 search field.



Using the remaining instructions, I could find and complete the steps. Alas, the icon remained active after that, so I assumed a restart was also required, which was also not mentioned by Copilot. When the computer restarted, the icon was indeed no longer in the taskbar corner.

Copilot is also found elsewhere on the computer.
A day later, I found the Copilot icon in another place, the popup that appears when the Search field in the taskbar is clicked. You can see that second icon in the upper right corner of the illustration at the bottom of the previous page. The second icon does ***not*** contain the letters PRE.

And yes, that second icon is active. Using **gpedit** to disable Copilot, as described by Copilot, did not remove or disable the second icon.

I decided not to include the URL for **gpedit** installation scripts in this article because using **gpedit** did not remove the Copilot icon anywhere other than on the right end of the taskbar.

More Web research followed. I found a page on which a registry edit was described to disable Copilot. I tried that registry edit method. It did not work for me.

I opened Windows Settings and used Search to find references to Copilot in Settings. None were found. The same not-found result happened in the Windows Control Panel.

Is removal from a computer not possible?

My Web research also turned up a Microsoft forum page on removing Copilot. A Microsoft rep posted an answer repeating the **gpedit** technique and reiterated a familiar refrain:

Copilot is now a part of the Windows 11 OS and *cannot be removed*.

In court many years ago, Microsoft sang that same song about an earlier version of Windows and the Internet Explorer (IE) Web browser. Microsoft claimed IE could not be removed without seriously harming the Windows OS. An outside expert demonstrated in court how to remove IE without impacting the Windows OS. In short, Microsoft may have believed that the company made IE removal from Windows impossible, but the company was proven wrong.

Microsoft may have learned much since then, but so have outside experts who use critical thinking skills to test and challenge Microsoft's claims. Perhaps the story of Copilot and its removal of it is just beginning.

(*Copilot AI, did not answer my how-to-remove question accurately or completely.*)

Microsoft has demonstrated that it is willing to install what the company considers the latest Microsoft killer app **without giving its Windows customers a choice before or after the installation**. Giving customers a choice might limit Microsoft's profit potential.
That lack of a choice shows that Microsoft does not treat customers respectfully.

###

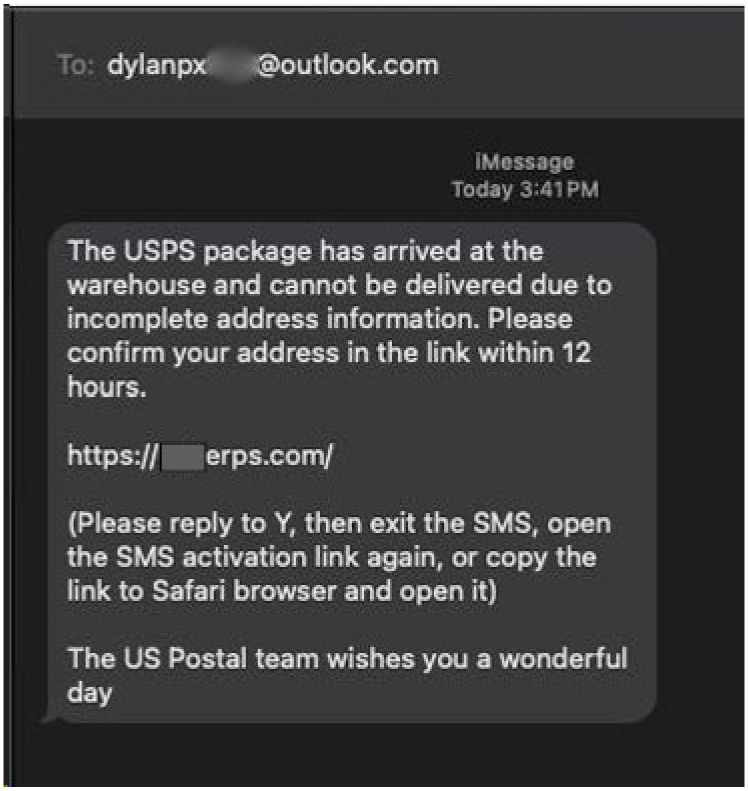
Another Day. Another Scam. Don’t Fall for it.

By Kurt Jefferson, Editor, lextown77@mymetronet.net
Central Kentucky Computer Society https://newsite.ckcs.org

I wonder how many Americans this very minute are being taken for a ride and giving away their personal information to a criminal. You might be surprised. At all hours of the day, people are turning over credit card numbers and more to thugs.

As Aura writes, “When Mary Anne May received a text from UPS on the day after Mother’s Day, she assumed a family member sent her a gift that she wasn’t home to receive. But when she clicked on the link in the text to reschedule the delivery, and was asked for her credit card number, she started to get suspicious.

While Mary Anne’s caution was well-founded, millions of Americans have fallen victim to package delivery scams like this one.”



To: dylanpx[redacted]@outlook.com

iMessage
Today 3:41PM

The USPS package has arrived at the warehouse and cannot be delivered due to incomplete address information. Please confirm your address in the link within 12 hours.

https://[redacted]erps.com/

(Please reply to Y, then exit the SMS, open the SMS activation link again, or copy the link to Safari browser and open it)

The US Postal team wishes you a wonderful day

In recent days, I've received a number of bogus text messages on my phone. I simply report them as junk and delete them.

Here's an example. The bogus text message alerts me that the US Postal Service (USPS) is holding a package at its "warehouse" and cannot deliver it because it lacks complete street address details. Look who supposedly sent the text. It's from a guy named Dylan. This is the ***first*** red flag. Think about it. USPS will never text you using a bogus email address starting with "dylan."

Second, the letter carrier has been delivering mail and Amazon packages to my house for years. USPS doesn't have my address? Then who's the guy who's been delivering junk mail to my mailbox for years?

Third, the USPS doesn't have "warehouses." They don't use that phrase. The USPS has distribution centers. And I'm very glad to know that the bogus US Postal team is wishing me a wonderful day! Finally, the USPS doesn't use bogus web addresses, as shown in the text. A legitimate message would read usps.com or something similar.

(Ed's note: ***fourth***, the USPS isn't going to send email from anywhere but @usps.com.)

If I click on the link shown in the text, I'll get a website where I can easily enter my credit card number to be scammed by Dylan or whoever is trying to turn me into a victim. Hey Dylan, have a wonderful day!

###

Do You Use Two-Factor Authentication?

By Phil Sorrentino, Secretary & Newsletter Contributor, philsorr@yahoo.com
Sun City Center Computer Club https://scccomputerclub.org/

If not, you might want to consider it for specific accounts if it is offered. Two-factor authentication is a way of adding an additional level of privacy to a computer account. When you set up an account, typically on a computer server, you assign a "user name," which is not private, and a password, which you are advised to keep private. This provides a certain level of privacy because to access your account, you must provide the user name, and the password. This is probably all you need to do for most of your accounts. However, adding another level of privacy would be prudent to guarantee that

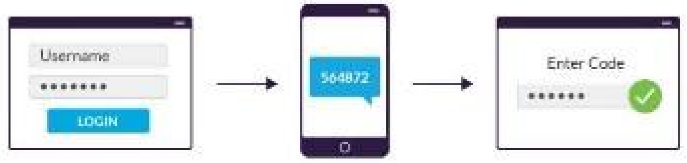
only you can access the account. These accounts would be those that you would be very unhappy if someone else, or some other computer, could access and download or manipulate its contents. An account that contains very personal information or an account at a financial institution might be just this type of account.

Keep in mind the internet employs a **Client-Server Architecture**. Using this architecture, your account is on a server computer, not your home computer, tablet, or phone. These (client) devices only provide the ability to connect to the server and manipulate the account contents. So if someone else knew your user name, which is not protected, and also knew your password, they could access the account and manipulate the contents. If it's a financial account, they could probably manipulate its value.

Unfortunately, no matter how diligent you are in protecting your password, sometimes passwords become known to the bad guys, such as "hackers." If hackers get into your financial account, they can possibly use it for fraudulent financial transfers or payments, or worse, and a password alone may not be enough protection. Even many services that don't offer two-factor authentication have instituted various checks on the computer attempting to use a particular server account, like sending an email to the email of record indicating a new computer is trying to access the account and asking, "Is this you?". If you are concerned about this, search "what happens if someone accesses my account" and see the possibilities. Nowadays, many services employ two-factor authentication to help guarantee that only the account owner can access a particular account. (Ed's note: this is why using a password manager helps. Only ONE password is assigned to each account and they can be complex. If one is stolen, not all are compromised.)

Two-factor authentication is not a new concept. Banks have used a second form of identification for years, from using ATMs, to secure access to safe deposit boxes. When a bank customer visits an automated teller machine (ATM), one authentication factor is the physical ATM card that the customer slides into the machine ("what you have"). A second factor is the PIN the customer enters through the keypad ("what you know"). When you want to get into your safe deposit box, you have to provide the account number ("what you know") and a key ("what you have") before they will let you into the box.

Fortunately, many, if not all, financial institution servers provide the ability to use two-factor authentication. Two-factor authentication requires a second form of identification, which you typically have. Two-factor authentication increases the probability that the requester is who he says he is. The more factors used, the higher the likelihood that the requester is the account owner. Two-factor authentication is sometimes confused with "strong authentication," but these are different strategies. Soliciting multiple answers to challenge questions may be considered strong authentication. However, unless the process also requires "what the user has" or "what the user is," it would not be regarded as two-factor authentication.



What you know + What you have/are = Positive Authentication

In general, authentication can be done by "what you know", like a password or pin, or "what you have", like a badge or a smartphone, or "what you are", like a fingerprint or iris eye-print. (Some highly classified systems may require all three for authentication, which would involve possessing a password and a physical token used in conjunction with biometric data, such as a fingerprint, a voiceprint, or a retina scan.)

For most typical internet servers, the second form of identification is "what you have." The "what you have" can be a code sent to you by text, email, or phone; the account owner usually makes the choice. The code is typically a one-time-use series of digits. Once the code is sent, you will have enough time to enter it into the screen that starts the authentication process. If email is selected, the server will send an email with the code to the email address of record on that server. Once you provide the correct code, you will be granted access to the account. If a voice phone call is selected, the call is made to the phone number on the record on that server. Once the phone call is answered, the digits are announced, and you can enter them on the screen that starts the process. If a text is selected, the text will be sent to the phone number of record on that server (ensure the phone number can receive texts). The code in the text can then be entered into the screen that starts the process.

Two-factor authentication adds an extra step to your login process, and depending on how the service has implemented it, it can be a minor inconvenience or a major annoyance. (And it also depends on your patience and willingness to spend the extra time to ensure higher security.) However, in the long run, using two-factor authentication improves the security of your private information, which is undoubtedly something we all want. So, take the time to set up two-factor authentication on at least all of your financial and very private accounts.

###

UNCHECKY

Stop installing unwanted software.

By Jasmine Blue D'Katz, cynthia.g.simmons@gmail.com
Lake County Area Computer Enthusiasts http://www.lcace.org/

I have been using several programs suggested by Bob Gostischa (www.techforsenior.com) and Judy Taylour (APCUG). Recently, I had to rebuild one of my computers, and the program **Unchecky** gave me lots of help reinstalling the software.

Unchecky is a free, open-source program that automatically unchecks unwanted, preselected boxes during software installation. It is a lifesaver for anyone who has ever been frustrated by the sneaky tactics used by some installers to trick users into installing additional software or signing up for unwanted services.

How it Works

Unchecky works by monitoring your computer for software installation processes. When it detects an installer, it automatically scans the installer for pre-selected boxes. If it finds any, it unchecks them for you. This way, you can be sure that you are only installing the software you want, without any unwanted extras.

Benefits of Using Unchecky

There are many benefits to using **Unchecky**. Here are some:

- Saves time: **Unchecky** can save you a lot of time by automatically unchecking unwanted boxes. No more clicking through endless installation screens!
- Saves money: **Unchecky** can help you save money by preventing you from installing unwanted software you might have to pay for.
- Protects your privacy: **Unchecky** can help protect your privacy by preventing you from installing software that tracks your activity or collects your personal information.
- Easy to use: **Unchecky** is extremely easy to use. There are no settings to configure, and it runs silently in the background.

Is Unchecky *Safe?*

Unchecky is entirely safe to use. It is a reputable program with a large and active community of users. It is also open source, so you can be sure its code is clean and free of malware.

Overall

Unchecky is an essential tool for anyone who wants to take control of their software installations. It is free, easy to use, and can save you time, money, and frustration. I highly recommend it to everyone.

*Here are some additional things to keep in mind about **Unchecky**:*

- **Unchecky** does not work with all installers. Some installers are designed to bypass **Unchecky** and other similar programs.

- **Unchecky** may not always be able to detect all unwanted boxes. Double-checking the installation screens yourself is always a clever idea before clicking "Install."
- **Unchecky** is not a replacement for common sense. It is important to be careful about what software you install, even if **Unchecky** can uncheck the unwanted boxes.

I would also like to add that **Unchecky** is an excellent program for anyone concerned about their privacy. By preventing you from installing unwanted software, **Unchecky** can help protect your personal information from being collected and used by third parties.

###

Printing your photos.

By Lynda Buske
Ottawa PC Users' Group, Ontario, Canada https://opcug.ca

Despite our digital world, it is really nice sometimes to print a photo that you can stick on your fridge, display on your wall, or even frame and give as a gift. The main thing to remember is that the print size for a digital image may be limited.

All digital cameras and cell phones have sufficient megapixels to provide the resolution for a 4”x6” or 5”x7” photo enlargement. Many would have enough for much larger prints (e.g., 8”x10” or 11”x14”). However, cropping in post-production will reduce your image dimensions.

The best starting point is determining what a good quality home or commercial printer will provide. In most instances, the gold standard is 300 dpi (dots per inch), which you can equate to 300 pixels per inch. That means if you want to print an 8” x 10”, the long side of your image would ideally be at least 3000 pixels (10” x 300). For 16’ x 20”, you would probably like the long side to have around 6000 pixels.

The table below provides a rough guideline for the maximum print size of good quality that you can expect based on the number of megapixels your camera has.

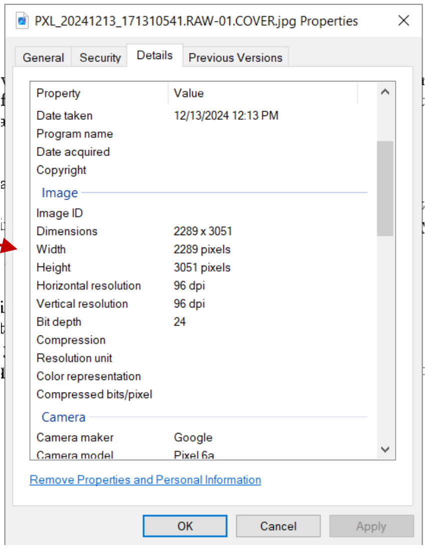
Camera resolution	File size at high resolution (pixels)	Max print size **in inches** at 300 dpi
2 megapixels	1200 x 1800	4 x 6
3 megapixels	1536 x 2048	5 x 7
	2448 x 3264	8 x 10
8 megapixels	2592 x 3888	8 x 14
	2800 x 4000	8 x 14
10 megapixels	3264 x 4920	11 x 14
	3744 x 5616	12 x 18
12 megapixel	4000 x 6000	16 x 20

(table continues next page)

Camera resolution	File size at high resolution (pixels)	Max print size **in inches** at 300 dpi
16 megapixels		
21 megapixels		
24 megapixels		

If you have a 24MP camera, your images will probably be 6000 x 4000 pixels. This means you can do a lot of cropping before going under the 3000-pixel threshold. If you shoot with a 12 MP camera and then crop your images significantly, you may not be able to print an 8"x 10". However, if your cropped image dimension is still around 1200 x 1800, based on the chart above, you could print a 4"x6". Some older cell phones have only 5 or 6 megapixels, so be careful when deciding what size to print. Unfortunately, many family pictures we want to treasure are taken at social events with cell phones, so get close to minimize the need to crop. Unless you are sure your cell phone has an optical zoom on the camera, don't "zoom" with the finger spread as that is just cropping and hence losing resolution. Even if cell phones tout 20MP or 100MPs, almost all only output 12MP due to pixel binning (https://en.wikipedia.org/wiki/Pixel_binning).

The easiest way to see your image's dimensions in the Windows environment is to go to *File Explorer* and right-click on the photo. Then click on *Properties*, select the *Details* tab, and find the dimensions.


PXL_20241213_171310541.RAW-01.COVER.jpg Properties
General
Security
Details
Previous Versions
Remove Properties and Personal Information
OK
Cancel
Apply

Property	Value
Date taken	12/13/2024 12:13 PM
Program name	
Date acquired	
Copyright	
Image	
Image ID	
Dimensions	2289 x 3051
Width	2289 pixels
Height	3051 pixels
Horizontal resolution	96 dpi
Vertical resolution	96 dpi
Bit depth	24
Compression	
Resolution unit	
Color representation	
Compressed bits/pixel	
Camera	
Camera maker	Google
Camera model	Pixel 6a

One final consideration when making prints is the viewing distance. If you print a 4"x6", there is a good chance it will be held in your hand or an album and, hence, very close to your discerning eye. If, on the other hand, you make an 11"x14" print for your wall, it may never be viewed at less than a few feet, and therefore the resolution does not have to be as good.

You may have to experiment as to which image dimensions produce an adequate enlargement for your viewing needs and which printing service provides the quality you want. I recommend printing one 8"x10" as a test before committing to a company. When submitting digital photos online, many services will warn you if the resolution is not adequate for the print size you requested.

I have found the quality of prints at Shutterfly and Photobook Canada to be very good, but there are significant delivery fees. On the other hand, Staples has the quality but no delivery fees if you pick up your print at the store. However, it takes five business days. If you want a quick turnaround of 4"x6" prints, a place like Walmart is probably all you need.

###

Burned By Another Security Breach?

By Kurt Jefferson, Editor, lextown77@mymetronet.net
Central Kentucky Computer Society https://newsite.ckcs.org/

If you're reading this, there's a fair chance your personal data has been compromised. Stolen. As Malwarebytes Labs reports, "Earlier this week, the data of over 70 million people was posted for sale on an online cybercrime forum. The person selling the data claims it stems from a 2021 breach at AT&T."

If you think you might be a victim, you can type the email address connected to your AT&T account on the Malwarebytes website. (Malwarebytes is a well-known company that produces anti-malware software and similar products.)

This security breach is especially troubling because, as Bleeping Computer notes, "AT&T says a massive trove of data impacting 73 million people did not originate from its systems after a hacker leaked it on a cybercrime forum and claimed it was stolen in a 2021 breach of the company."

The stolen personal data is from an alleged 2021 AT&T breach that hackers calling themselves ShinyHunters attempted to sell on the dark web.

You should note that the dark web cannot be reached through search tools such as Google, Yahoo! or DuckDuckGo.

It's comprised of websites where everything from drugs to guns to personal information are sold for the right price. Whether or not the stolen data came from AT&T, the wireless giant says it has started notifying millions of customers about the data thefts.

AT&T says it has already reset passwords of current customers and will be contacting others whose passwords, Social Security numbers, and possibly email and street addresses were compromised.

Prosecutors in New York are opening an investigation into the breach.

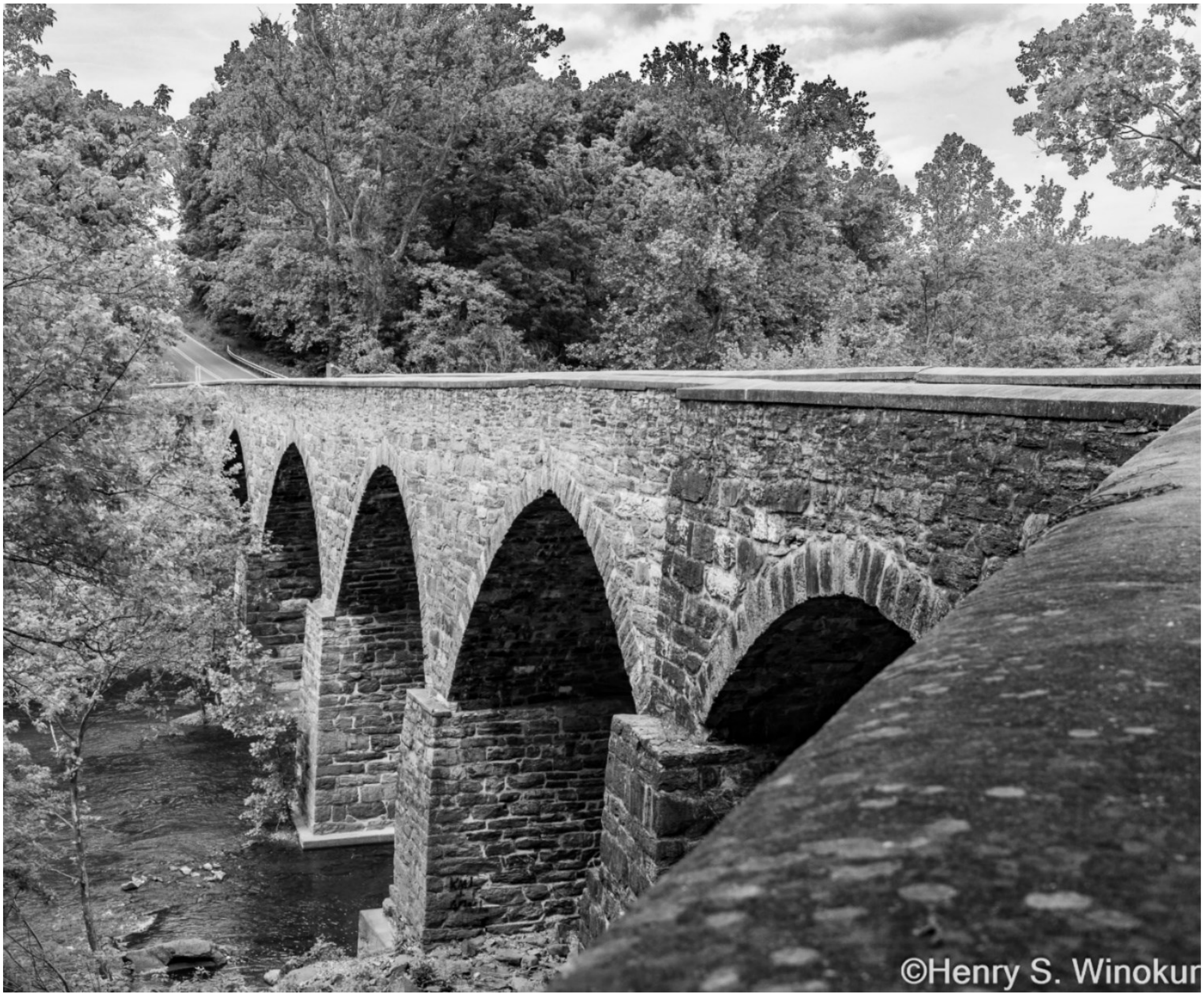
Numerous tech web sites are urging AT&T current and former customers to freeze their credit accounts at the big three credit agencies–TransUnion, Experian and Equifax.

In addition, sign up for two-factor notification on their AT&T accounts and change their AT&T password if it hasn't already been changed. Also, monitor credit reports. This isn't the first time this phone company has had problems.

In a major AT&T outage in March, the company apologized for the disruption and offered a $5 credit to customers.

###

Last issue, someone suggest I ask you to share some of your images with me for the purpose of using up some of the "white space". No one did. So here's one of mine.
This photo is from my trip to Antietam Battlefield in May 2024, but it's at the opposite "end" from where the Battlefield is (central Washington County, MD). **LeGore Bridge**, built in 1898, over the Monocacy River, is on the eastern side of Frederick County, MD.



Camera: Canon R5, 1/160ths, ISO 200, **Lens**: RF 14-35 f/4L IS USM, 35mm, f/ 8.0

President, Registered Agent, Internet Services	Paul Howard, 703-860-9246, president@patacs.org
1st Vice President	Nick Wenri, 703-759-3938, director11@patacs.org
2nd Vice President, Membership Chair	Mel Mikosinski, 860-816-3655, membership@patacs.org
Secretary	Jim Rhodes, 703-931-7854, director7@patacs.org
Treasurer	Roger Fujii, 703-426-5917, treasurer@patacs.org
Meeting Setup, Director	Bill Walsh, 703-241-8141, director14@patacs.org
APCUG Liaison	Gabe Goldberg, apcugrep@patacs.org
Directors: (http://www.patacs.org/boardpat.html)	Mike Emery, Frank Fota, Geof Goodrum, Leti Labell, Kathy Perrin, Melvyn Sacks, Bill Walsh, Henry Winokur
Newsletter Editor	Henry Winokur, editor@patacs.org
Columnists	Volunteers Needed
Vendor Liaison	Volunteer Needed
Publicity	Volunteer Needed

PATACS Information

PATACS, Inc. 201 S. Kensington St. Arlington VA 22204-1141

Club Information call: 703-370-7649 Website: www.patacs.org

Monthly Circulation: 90+

Posts is an official publication of the Potomac Area Technology and Computer Society (PATACS), a Virginia non-stock corporation and a recognized tax-exempt organization under section 501(c)(3) of the Internal Revenue Code. Contributions are gratefully received and tax-deductible.

Posts provides news, commentary, and product information to PATACS members. Products or brand names mentioned may be trademarks or registered trademarks of their respective owners. The contents of the articles herein are the responsibility of the authors and do not necessarily represent PATACS, the Board of Directors, or its members. The authors provide photographs and screen images. Authors retain copyright to their contributions.

Colophon: This issue of *PATACS Posts* was prepared with Microsoft Word 365 (www.microsoft.com). The typeface is mostly Century size 12 through 16. Public domain clip art is from openclipart.org. Artwork from other sources is attributed.

E-mail article submissions and reprint requests to editor@patacs.org.

Membership Policy: Membership dues are (US) $30.00 per year, with a $15 surcharge for international mail. **Printed newsletters cost an additional (US) 5.00 per year**. Members receive extensions of membership for making meeting presentations, and writing articles for the Posts newsletter. Membership in PATACS includes membership in any SIGs and subscription to the Posts newsletter published 8 times per year in print (by US Mail) and PDF (by download). Applications may be obtained at any club meeting, or by downloading from www.patacs.org/membershippat.html. Applications and payments may be completed online. A sample newsletter, membership application, and related information may be obtained by enclosing a check for $2 (US addresses only) and mailing your request to the membership address. Please do not send cash by mail. Payment and applications may also be submitted at any meeting, or mailed to **PATACS Membership, c/o Roger Fujii, 5501 Beaconsfield CT, Burke VA 22015-1914**.

Reprint Policy: Permission to reprint articles from the PATACS Posts is given to schools, personal computer clubs, and nonprofit organization publications, provided that: (a) PATACS Inc. receives a copy of the publication; (b) credit is given to the PATACS Posts as the source; and (c) the original author is given full credit and retains the copyright of their work. Recognition is one means of compensating our valued contributors.

PATACS, Inc.
201 S. Kensington St.
Arlington VA 22204-1141

First Class

AFFIX
FIRST
CLASS
POSTAGE

TEMP-RETURN SERVICE REQUESTED

Meeting schedule (Zoom=Online Only, Hybrid=Online/In-person)

1st Wednesday	7:00 – 9 PM	Arlington General Meeting	Hybrid
3rd Monday	7:00 – 9 PM	Board of Directors Meeting	Zoom
3rd Saturday	12:45 – 3:30 PM	Fairfax General Meeting	Hybrid
4th Wednesday	7:00 – 9 PM	Technology & PC Help Desk (in Arlington)	Hybrid

Arlington Mtg: 5711 S. 4th St., Arl. VA
Fairfax Mtg: 4210 Roberts Rd., Fairfax, VA

Meetings are Hybrid or Zoom (as above)
Fairfax Health/Safety: https://www.patacs.org/fairfaxattreqmts.html
Online Meeting Access Will Be Sent Via Email

PATACS Event Information
Messages may be left at 703-370-7649
Website: **https://www.patacs.org**