

Bits of Bytes

Newsletter of the Pikes Peak Computer Application Society, Colorado Springs, CO

Volume XLVI

February 2026

Issue 2



The Prez Sez

by John Pearce,
President,
P*PCompAS

My thanks to Greg Lenihan for helping move our equipment storage box, a.k.a. the wood box, out of the church and thanks to Toni Logan for allowing the box to be stored in her basement.

One of the benefits of the in-person meetings was the conversations that preceded the meetings and those that happened during the breaks. I would like to make sure the Zoom meeting is open by 8:45 a.m. and available for conversations and those need not be computer or tech related.

Stay safe and take good care of yourself!!

Meeting Minutes

by Greg Lenihan,
P*PCompAS Secretary

The 3 January 2026 membership meeting was started via Zoom by President John Pearce at 9 am. There were no guests. The meeting minutes from last month were approved.

OFFICER REPORTS

VP Cary Quinn called in from a hospital room to report that he had some videos to show and would start work on a presentation in February.

Treasurer Toni Logan reported she transferred \$50 from savings to checking to pay for our APCUG dues. She also deposited \$175 from the coffee fund, which should cover

Next P*PCompAS meeting: Saturday, 7 February 2026

A Zoom link will be sent out.

No presentation topic has been announced.

our Volunteers Luncheon. We have a total of \$1338.35.

Membership Chair Ann Titus has not heard from anyone lately, but our last count was 20 members.

Newsletter editor Greg Lenihan said the deadline for the February newsletter was 24 January.

Librarian Paul Godfrey had nothing new to report.

APCUG Rep John Pearce had nothing to report. He sent an e-mail to our APCUG contact about his duty requirements, but has not heard back.

Webmaster Greg Lenihan said that after Christmas he started looking at sites that had website templates. There are quite a few that allow you to create free websites, but want you to pay to host your site. Greg plans to give Francis Chao (APCUG) a call to see if he has recommendations. Joe Nuvolini says he can supply Greg with current files from our website.

BOD Chair Bob Logan had nothing to report.

OLD BUSINESS: None

NEW BUSINESS:

Toni Logan asked if we were going to make a gift to the church this year. John Pearce said we would be donating club equipment as a gift.

John Pearce said a financial review for 2025 needs to be made, and it could be done after our next breakfast. Cary Quinn and Paul Godfrey volunteered to help Toni Logan.

John Pearce and Greg Lenihan inventoried the contents of our storage box at the church. John proposes that the projector and wireless microphone be donated to the church. Once they are gone, we are destined to Zoom meetings. A motion was made to hold on to these items for at least six months, just in case, and the motion passed. Toni Logan said she has space in her home for the storage box. John Pearce said we would look into the storage box location.

Ann Titus said she had a box of receipts from past purchases and asked if we needed to keep them. The answer was it was not necessary but they should be shredded.

ANNOUNCEMENTS

The next social breakfast meeting will be on Saturday, 17

Continued on page 3

In This Issue

Articles

How to Attend a Zoom Meeting	3
Stop Wi-Fi Sharing	8
Windows Recycle Bin.....	5
Windows Troubleshooting Tool	4
Your TV is Spying on You	7

P*PCompAS

Meeting Minutes	1
Prez Sez.....	1



Officers

President: John Pearce
jljnet@comcast.net

Vice President: Cary Quinn
cary.quinn@gmail.com

Secretary: Greg Lenihan
glenihan@comcast.net

Treasurer: Antoinette Logan
antoinettelogan@gmail.com

Staff

APCUG Rep: John Pearce
Discord Admin: John Pearce
Drawings: Cary Quinn
Editor: Greg Lenihan
Librarian: Paul Godfrey
Membership: Ann Titus
Webmaster: Greg Lenihan

Committees

Hospitality: Antoinette Logan
Programs: Cary Quinn
Publicity: Vacant
Nominating: Vacant

Board of Directors

Bob Logan
David George
Greg Lenihan
Joe Nuvolini
Paul Godfrey



Zoom participants at the January 2026 meeting.



Digerati at the January breakfast at the Golden Corral

Tip from the Golden Gate Computer Society

Google is allowing AI to scan all your emails and the documents attached to them. Everything you've sent or received in your account can be scanned by AI. If you don't want this to happen, follow the steps below.

- Go to Gmail
- Click on settings (gear icon)
- Click on See all settings
- Scroll down until you see Smart features/turn on Smart features in Gmail
- Uncheck the box next to that
- Box comes up that says: Turn off and reload
- Click that. It reloads your email.
- Go back to Settings (gear icon).
- Click again on See all settings
- Scroll down to Google Workspace Smart Features
- Click on manage workspace smart feature settings
- Turn off both buttons on the right
- Click on Save

The Pikes Peak Computer Application Society newsletter is a monthly electronic publication. Any material contained within may be reproduced by a nonprofit user group, provided proper credit is given to the authors and this publication, and notification of publication is sent to the editor. Any opinions contained in this newsletter are made solely by the individual authors and do not necessarily reflect or represent the opinions of P*PCompAS, its officers, or the membership. P*PCompAS disclaims any liability for damages resulting from articles, opinions, statements, representations or warranties expressed or implied in this publication.

P*PCompas welcomes any comments, letters, or articles from members and non-members alike. Please send any articles to the editor (see last page for address). The editor reserves the right to reject, postpone, or edit for space, style, grammar, and clarity of any material submitted.

How to Attend a Club Zoom Meeting

It was suggested that members be reminded of how to attend a Zoom meeting. You may be a little rusty since we last met this way during the Covid days. The following was obtained from AI and modified slightly.

To join a Zoom meeting, you generally need the meeting's invitation link or Meeting ID/passcode, a device (computer, tablet, phone) with internet, and optionally the Zoom app, though you can often join from a web browser without downloading anything first, just ensuring your microphone and camera devices are set to the correct options. Without a camera or microphone, you can watch the meeting on your screen, but you won't be seen, and can't be heard.

Key Requirements:

- **Invitation Info:** The meeting link or the unique 9-11 digit Meeting ID and passcode.
- **Internet Connection** [Internet Connection](#): A stable connection is crucial for audio and video.
- **Device:** A computer, smartphone, or tablet.
- **Audio/Video:** Speakers & microphone (built-in or external), and a webcam (optional but recommended).

How to Join:

1. Using the Link (Easiest):

Click the meeting link from your email or calendar invitation and follow the prompts, choosing to open the app or join from your browser.

2. Using the App:

Open the Zoom app, click "Join a Meeting," enter the Meeting ID and passcode, then click "Join".

3. From the Web (No Download):

Click the link, then look for and select the "Join from your browser" option if prompted to download the app.

After Joining:

- **Join Audio:** Click "Join with Computer Audio" (or similar) to hear others.
- **Mute/Unmute:** Click the microphone icon in the bottom-left to control your audio.
- **Start/Stop Video:** Click the camera icon to control your video.
- **Waiting Room:** You may need to wait for the host to admit you.

Those familiar with Hewie Poplock on Tech for Senior can watch this video:

<https://www.youtube.com/watch?v=xQs3lakqapQ> ☺

Meeting Minutes (Cont. from pg 1)

January, at the Golden Corral, starting at 8:00 am.

The Volunteers Luncheon will be held on 31 January at the Golden Corral [at 11:30 am].

Our next membership meeting is on Saturday, 7 February 2026.

AROUND THE ROOM

Joe Nuvolini asked if anyone uses Mailwasher, which allows you to delete e-mail from your mail server before they come to your inbox. Joe would like to get rid of Mailwasher, and wonders if

simply uninstalling it would allow his e-mail to go to Thunderbird without problems.

Cary Quinn has one computer that needs a fixed power connector. Also, Cary is also looking for a good camera/microphone for a desktop computer. Several members said they use reasonably priced Logitech devices.

Harvey McMinn has a new laptop and it offered to help transfer files from his old computer, however it could not transfer everything. John Pearce said he is suspicious of programs that attempt to move files because they miss items

and he usually reinstalls his applications.

John Pearce noticed the club computer is running Windows 11 version 23H2, but it tells him it is up to date. John will try to update the computer manually.

PRESENTATION

Cary Quinn had a YouTube playlist made with three videos: "3 Privacy Fixes Most People Never Make," "Nancy Drew is Free. It's Public Domain Day," and "Goodbye to the Tech That Died in 2025." ☺

This is the Most Useful Windows Troubleshooting Tool You Keep Overlooking

by Arol Wright, reprinted with permission from [HowToGeek.com](https://www.howtogeek.com)

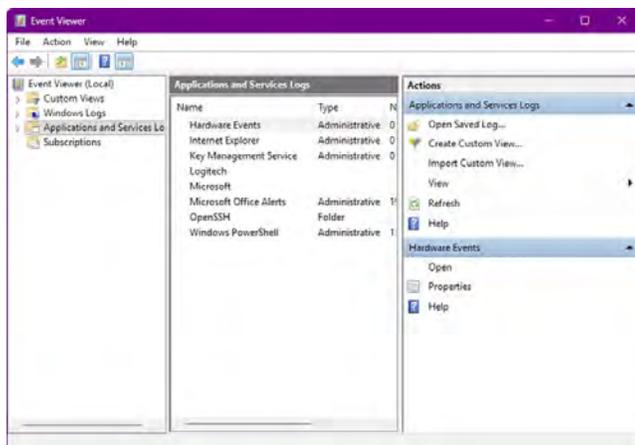
Original article at <https://www.howtogeek.com/this-is-the-most-useful-windows-troubleshooting-tool-you-keep-overlooking/>

Troubleshooting a Windows PC can oftentimes be quite a bore—and depending on your specific issue, it can either be pretty easy or absolute hell. And if you're doing so right now, you might want to learn how to use this specific tool to see everything your PC is doing—and where, exactly, it's messing up.

I'm talking, of course, about the Windows Event Viewer. But what is it, exactly?

What is the Windows Event Viewer?

The Windows Event Viewer is a system tool [within Windows](#) that functions as a sort of centralized log repository for all system, security, and application notifications. Technically, it is a Microsoft Management Console (MMC) snap-in that provides a graphical interface for viewing and managing the vast quantity of event logs that the OS generates in the background. While you interact with the graphical surface of Windows, the kernel and various services are constantly communicating their status through these logs. And while they're hidden most of the time—there's no need for you to constantly look at them anyway—this is where you see all of that. The tool essentially acts as the “flight recorder” or “black box” for a PC, capturing a detailed chronological record of everything from minor background service updates to catastrophic hardware failures.



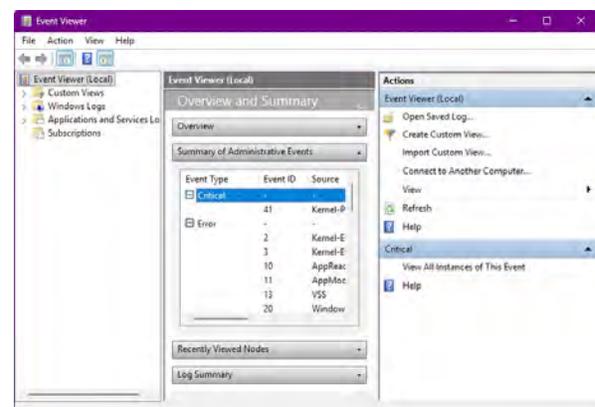
When you open the Event Viewer, which is typically accessible via the eventvwr.msc command or the Administrative Tools menu, you are presented with a structured hierarchy of logs. The most significant of these are the Windows logs, which are further categorized into Application, Security,

Setup, System, and Forwarded Events. The underlying architecture of these logs is based on XML, allowing for structured data storage that includes precise timestamps, unique Event IDs, and source identifiers. And it's probably one of the most important aspects of it, since it ensures that every action taken by the software or hardware leaves a digital footprint. For instance, the System log records events generated by Windows system components, such as a driver failing to load during startup, while the Application log stores data generated by installed programs, such as a database error or a browser crash.

The tool does not actively fix problems on its own; rather, it's in charge of collecting raw data, providing evidence and logs to aid you in your own troubleshooting process.

How useful is it?

Its usefulness lies in its ability to translate vague symptoms into specific, actionable data points. When a computer crashes or an app freezes, Windows often displays a generic error message stating that “something went wrong.” Sometimes it does give you more details than that, but still, rarely enough info to actually know the culprit behind said freeze. Was it another app? Did your [CPU/RAM fail to keep up](#)? The Event Viewer bridges this gap by providing the granular technical details necessary for root cause analysis. Its primary value is derived from the “Event ID” system, where every recorded



incident is assigned a specific numerical code. These codes are universal standards within the

Continued on page 5

Does the Recycle Bin Take Up Space, and Where Is It? Mysterious and hidden.

By Leo A. Notenboom, <https://newsletter.askleo.com>; published under the Creative Commons License

The Recycle Bin is your friend. I'll show you where it lives and how to control the space it uses.

When you delete a file using Windows File Explorer, that file is placed in the Recycle Bin. The Recycle Bin in Windows has saved many a person from grief, I'm sure.

But where exactly is it, and do the deleted files still take up space?

Let's look.

In Short

Recycle Bin space, location, and control

The Windows Recycle Bin stores deleted files, which take up space until the bin is emptied. Hidden on each drive, it can be managed by adjusting its size or deleting the folder entirely. It offers control over file recovery and space management across all drives and is accessible via a single desktop icon.

Continued on page 6

Win Troubleshooting (Cont. from page 4)

Windows ecosystem, meaning that a technician can take an obscure Event ID, cross-reference it with Microsoft's documentation or online technical communities, and immediately identify the specific failure point.

The tool also has pretty cool filtering and sorting capabilities. A system might generate thousands of "Information" level events per hour, which are generally harmless indicators of normal operation. However, the Event Viewer allows users to create Custom Views that filter out this noise, isolating only "Warning," "Error," or "Critical" level events. This capability transforms a massive, unreadable list of data into a concise report of system health.

It's also useful for identifying patterns over time. By analyzing the frequency of specific errors, you can determine if a problem is a one-off glitch or a symptom of a deteriorating component, such as a failing hard drive controller sending repeated timeout warnings. It allows for a proactive approach to system maintenance, letting you spot software conflicts or driver instabilities before they result in

total system failure. You can't stop hardware failure, but you can prevent it from disrupting your workflow if you act quickly.

When should you use it?

You might want to consult the Windows Event Viewer immediately following any unexplained system behavior or performance degradation. It is most frequently the first port of call after a [Blue Screen of Death \(BSOD\)](#) or a sudden, random reboot. In these scenarios, the OS cannot display an error message on the screen because the graphics subsystem has crashed, but the kernel often manages to write a "Critical" event to the System log just before the shutdown. By checking the logs timestamped at the exact moment of the crash, you can often identify if a specific driver, such as a graphics card update or a network adapter, triggered the collapse.

The tool is equally vital when troubleshooting specific app crashes. If a game or productivity suite closes to the desktop without an error window, the Application log will almost always contain a record of the crash, identifying the faulting

module or dynamic link library (DLL) responsible.

Beyond crash diagnostics, the Event Viewer should be used during security audits. The Security log tracks "Success Audit" and "Failure Audit" events, detailing every time a user attempts to log in or access a protected file. If you suspect unauthorized access to your machine, this log will reveal the exact time of the intrusion attempt and the user account involved. Additionally, it is prudent to check the viewer when a computer feels sluggish during boot.

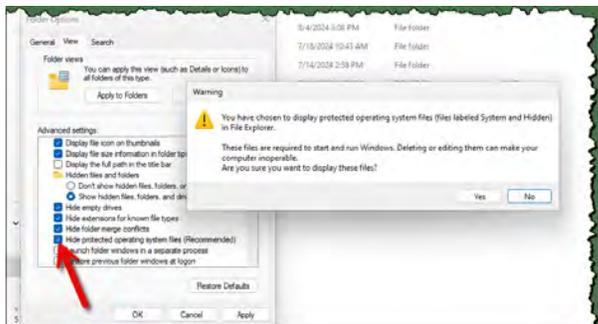
The "Diagnostics-Performance" log specifically tracks how long the system takes to start up and shut down, flagging specific programs or drivers that are causing delays.

Ultimately, it should be used whenever you move from merely observing a computer problem to actively trying to solve it. If you can fix a problem through any other means without relying on it, by all means, go ahead. But if you use the Event Viewer right, it will make your life so much easier. ☺

Recycle Bin (Cont. from page 5)

Where is it?

By default, the Recycle Bin is well hidden. It's not enough, for example, to say "View Hidden Files" in Windows File Explorer settings. You must also UNcheck "Hide protected operating system files (Recommended)".



As you can see, before Windows respects your choice, it gives you a stern caution about the importance of those files.

Once you've clicked **Yes**, you'll be able to see a Recycle Bin on all of your internal drives and most¹ external drives. They have different names based on how the drive was formatted; on NTFS-formatted systems, it is named **\$Recycle.Bin**. On FAT32/exFAT-formatted systems, it is named **Recycle Bin**.

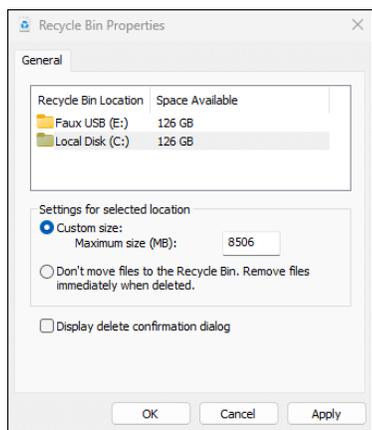
In all cases, Recycle Bins are located in the [root](#)/top of the drive.

Note that the Recycle Bin may not exist until at least one file has been deleted.

How much space does it take up?

The Recycle Bin definitely takes up space. Since the "deleted" files aren't really deleted at all, but instead moved to the Recycle Bin, they continue to take up space until the Recycle Bin is emptied or the file is deleted permanently.

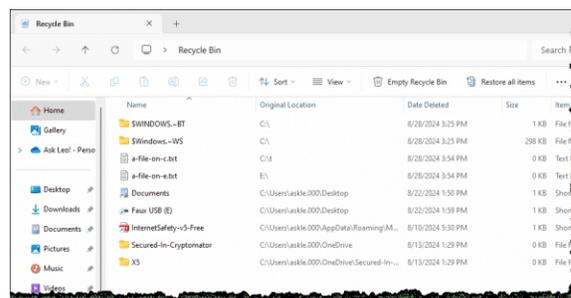
However, you can control the upper limit of how much space the Recycle Bin can take up. Right-click on the desktop Recycle Bin icon and click on **Properties**.



Each drive capable of having a Recycle Bin is listed, along with the size of the drive it's on. Click on one of the drives, and you'll be able to set the "Custom size" for the Recycle Bin on that drive. Once the Recycle Bin exceeds that size, older files will be removed — permanently deleted — to make room for newly recycled files.

Every drive, yet one control

Even though there are multiple Recycle Bin folders across multiple drives, there's only one Recycle Bin icon on your desktop. Double-click it, and it will open in Windows File Explorer, listing all the files currently contained in all Recycle Bins.



Note that the original location listed includes the drive on which the file is located. As per the toolbar items, you can **Empty Recycle Bin** to permanently delete all files in all Recycle Bin folders on all drives, or you can **Restore all items to send all the files back** to where they lived before you deleted them.

You can also right-click on a file and choose to Delete (meaning permanently delete) or Restore the individual file.

Emptying the Recycle Bin on only one drive

You may have multiple drives and multiple Recycle Bin folders (one per drive). What if you're running low on space on only one of the drives and would like to empty the folder *only on that drive*?

There are two approaches.

In Recycle Bin properties, set the space to be used by that drive to 1MB (zero doesn't work), click on **Apply**, and then reset the space to be used back to its original value.

That's too cumbersome for me. I use a slightly different [hack](#): I just delete the Recycle Bin folder *on that specific drive*. Surprisingly, the folder is not protected, and with "Hide protected operating system files" turned OFF, you can just click on it and delete it like any other folder. It and all its contents are permanently deleted. The next time you delete a file on that drive, it'll be recreated. ☺

Yes, Your TV is Spying on You (here's how to stop it)

By Bob Rankin, <http://askbobrankin.com>, published through the APCUG

Almost every television sold these days is advertised as a Smart TV. Behind the screen, these TVs are computers with an operating system, a hard drive, and Internet connectivity. They also have cameras, a microphone, and sophisticated software that allows them to collect and sell your viewing data. And because they are constantly connected, the same risks (malware and hacking) that apply to computers also apply to smart TVs. Read on to learn about the privacy and security risks of smart TVs, and what you can do to minimize them...

How to Stop Smart TV Spying

What makes a smart TV smart? When they were first introduced, it was the ability to connect to the Internet, and bring streaming channels and movies to your living room. Later, built-in microphones and cameras added features such as voice commands, hand gestures, and facial recognition, allowing you to control your viewing without so much as picking up the remote.

But both the internet connectivity and those advanced interaction features can be a liability. If a hacker gains access to your connected TV by exploiting a vulnerability, they could use those built-in cameras and microphones to spy on you and your conversations, while you sit transfixed on your couch during a Netflix binge session.



One article I found on this topic said something to the effect that “a bad actor can take control of your television,” and do nefarious things like change the channel, or show inappropriate content to children. That

made me laugh, and reminded me of the early-1990s [Goodtimes Virus spoof](#). If a hacker gains access to your TV, they won't out themselves by doing something as obvious and stupid as that.

If they hack your smart TV, they could use your Wi-Fi network to gain access to other devices on your home network, such as desktops, laptops, baby monitors, and even your “smart” appliances.

Why do I mention the possibility of your smart TV getting hacked? According to a Wikileaks article from 2017, [the CIA was doing exactly that](#) to some Samsung models. That vulnerability has been patched, but you can be sure there are ongoing efforts in this realm.

The larger threat to your privacy comes from within. Smart TV sets use a surveillance technique called Automatic Content Recognition (ACR) to figure out what you're watching. By “watching what you watch,” whether it's on streaming services like Netflix, cable, satellite or broadcast TV channels, even DVDs or video games, ACR can identify the content by comparing snippets of onscreen data with a database of known recorded works. If you've ever used Shazam on your phone to identify a song, you can see how this would work on your TV.

ACR does have some legitimate uses. It can be used to identify copyright violations, and also to personalize your viewing. If it can determine what kind of shows you watch, it may be used to recommend similar content. But it exists primarily to collect your viewing data and sell it to data brokers. Your viewing profile is bundled with your IP address, from which your approximate location and socioeconomic status can be determined. You can then be targeted with ads on your TV, smartphone, and desktop computer for products that fit your profile.

A study done by Northeastern University found that many smart TVs sent the ACR data to Amazon, Facebook, and Google. ACR viewing data was also sent to Netflix, even if the service was not present or activated on a set. Targeted ads are common on the Internet. You visit a website selling shoes, and you see ads for shoes. The same is happening as you “surf” the content on your TV screen.

Continued on page 8

Stop Wi-Fi Sharing: How to Fix Your Router Right Now

from *The Current Newsletter at Komando.com* (tip from 1/13/26)

Copyright 2026. WestStar TalkRadio Network, reprinted with permission. No further republication or redistribution is permitted without the written permission of WestStar TalkRadio Network. Visit Kim Komando and sign up for her free e-mail newsletters at: www.komando.com

The Current reveals how AI is turning your home router into a neighborhood spy. Kim Komando exposes the secret networks and shows you the 10-minute fix to take back your privacy today.

TL;DR (The Short Version)

- Your Echo and Ring devices share your bandwidth with the whole neighborhood, and yes, you're paying the bill.

- The ISP ghost may be using your house as a free public hotspot for strangers.
- Routers collect digital fingerprints from nearby devices and sell this data.

OK, here's something wild that you might not know. Your Wi-Fi router isn't sitting there twiddling its antennas while connecting your phone to Netflix.

It's actively scanning everything around it,

Continued on page 9

TV Spying (Cont. from page 7)

In 2017, TV maker Vizio was fined \$2 million by the FTC for selling this data without disclosing the surveillance to customers. Such disclosures are now mandatory. The "permissions" are granted (on an opt-out basis) by the user during setup, and the option to disable data collection is available in the TV settings. But each manufacturer calls it something different, and it can be hard to find the privacy settings. Samsung calls it Viewing Information Services, on Vizio sets it's Viewing Data. LG calls it Live Plus, and Sony has Samba Interactive. Do you think that obfuscation is intentional?

Consumer Reports has [instructions for turning off ACR](#) on most major TV brands, including Hisense, Insignia, LG, Philips, Samsung, Sharp, Sony, TCL, Toshiba and Vizio.

Be aware that ACR is not limited to streaming services. It now commonly "watches" everything that appears on your TV screen (that includes inputs from HDMI, DVD and game consoles) and that sampling can be extremely frequent (dozens of times per minute on some sets).

You should also check the privacy settings on any streaming services such as Netflix, Hulu,

Amazon Prime, YouTube, Roku. You'll want to check for things like deleting your watch history, ad tracking/personalization options, Data Monitoring settings, and turning off interest-based ads. Login to your account with a web browser, and poke around for "Permissions", "Privacy and Settings", "Data Privacy" or similar headings.

It's a little geeky, but putting your TV and other "connected" devices on your WiFi router's Guest network can shield you from some of these privacy invasions. See this CNET article on [Setting Up Guest Wi-Fi](#) for help with that. Connect the smart TV and other gadgets (smart speakers, smartwatches, fitness trackers, thermostats, smart locks, and video doorbells) to the guest WiFi, leaving PCs, laptops and phones on your main WiFi network.

What About Those Cameras and Microphones?

Built-in cameras can be used to enable hand gestures to control your TV. LG sets with embedded cameras have supported hand gestures for a decade. Sony's Bravia Cam allows you to use hand signals to pause, adjust volume or turn off the TV. But it will also scold you if you're too close to the screen. Microphones and speech recognition tech allows you to

change the channel or search for a show.

As I mentioned earlier, a determined hacker with knowledge of a remotely exploitable vulnerability could use your TV set as a way to watch you. Even if you're not concerned about hackers, do you really need to control your TV by pointing or grunting?

Check the settings to see if these features can be disabled on your TV. Or if you can find the camera on the face of your smart TV, a piece of black tape can be used to cover it.

In closing, here are a few more tips to boost the privacy and security of your smart TV:

- Find out what kinds of data your specific model is collecting, what is done with that data, and how you can limit that. This information should be in your manual, or on the vendor's website. Search online for your TV's model number and the word "privacy."
- Don't rely on factory settings. Explore the privacy settings on your set, and change any default passwords if you can.
- Check the manufacturer's website to see if there are any updates or security patches that can be applied. ☺

Wi-Fi Sharing (Cont. from page 8)

collecting data on everyone and everything nearby. Even people who aren't on your network.

I know, creepy, right?

Amazon's neighborhood network

Unless you manually turn it off, your Echo and Ring devices share a slice of your internet with other Amazon gadgets up to half a mile away through Amazon Sidewalk.

Yep, your friendly neighbors, and even that guy who lets his dog crap on your lawn, get a piece of the line you pay for. If your neighbor's Ring loses Wi-Fi, it hops onto YOUR Echo to upload footage. You're running free surveillance infrastructure for Amazon, and you never agreed to it.

Here's how to shut it down:

- **For Alexa:** Open your **Alexa app** > **More** (three lines) > **Settings** > **Account Settings** > **Amazon Sidewalk** > toggle "Enabled" **Off**.

- **For Ring:** **Ring app** > **Menu** (three lines) > **Control Center** > **Amazon Sidewalk** > **Off**. Do this today.

Genius on Amazon. They get neighborhood networks for free. But we're smarter than that.

Your router tracks everything

Every phone and laptop broadcasts a MAC (media access control) address, a digital fingerprint. Your router picks up these signals from every device nearby.

Mesh systems like Eero and Google Nest build profiles of who is near your house and when, then send that data back to the mother ship.

Your public hotspot for strangers

Renting a router from Xfinity, Spectrum or Cox? Bad news: You're paying the power bill for a public Wi-Fi hotspot that isn't

for you. Without asking, ISPs broadcast a second, hidden signal (like xfinitywifi) from your equipment, so strangers can hop on.

The ISPs claim the traffic is separate, but you're still subsidizing their national network with your electricity. Plus, it creates signal noise that can slow your own speeds and gives hackers a reason to linger outside your house.

Fix it: Log into your ISP account, find **Manage Internet** or **Advanced Settings**, look for **Public Wi-Fi Hotspot** and toggle it **Off**.

It takes 60 seconds, and it's a massive win for your privacy.

What to do right now

First, stop renting equipment. Buy your own [modem & router combo](#) (17% off, \$250). You'll save money monthly and won't be a free hotspot for the block.

Second, log into your router (usually 192.168.1.1 or 192.168.0.1) and disable anything labeled analytics, telemetry or motion sensing.

Router companies figured out they're sitting on incredibly valuable data about your life. They're selling it. But you can take back control in minutes. ☺



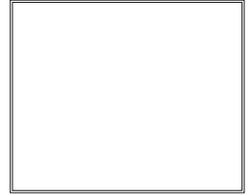
Tip: Fix Windows 11 Right-Click Menus

Microsoft messed with context menus so you only see "important" options, and the rest are hidden under Show more options. Annoying, right? Quick fix: Hold Shift + right-click on any file or folder to see the full menu instantly

Tip: Screenshot and Record on Windows 11

For quick screenshots, press Windows key + Shift + S to open the Snipping Tool, then drag to capture the area you want. For recording, press Windows key + Shift + R, select the area you want again, and hit Start.

P*PCompAS Newsletter
Greg Lenihan, Editor
4905 Ramblewood Drive
Colorado Springs, CO 80920
e-mail: glenihan@comcast.net



Coming Events:

Volunteer's Luncheon: 31 January at the Golden Corral, 1970 Waynoka Road, at 11:30 am

Next Membership Meeting: 7 February 2026 beginning at 9 am with login available by 8:45 am. Zoom links will be e-mailed out to all members on the roster.

Next Breakfast Meeting: 21 February @ 8:00 am, Golden Corral, 1970 Waynoka Road

Newsletter Deadline: 21 February

Check out our Web page at: <http://ppcompas.apcug.org>