Bits of Bytes

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

Volume XLVI | March 2026 | Issue 3

The Prez Sez

by John Pearce, President, P*PCompAS

Microsoft Secure Boot certificates issued in 2011 and used into 2023 begin expiring in June 2026. Is an expired certificate a concern? Yes, it is if you rely on Secure Boot to protect your PC against boot-level threats. Microsoft issued new certificates in 2023. Thus, PCs built in 2023 or later should already have the new certificates.

Different manufacturers have different requirements to prepare for the Secure Boot certificate updates. My 2022 HP Envy running Windows 11 had a BIOS update in December 2025. I am hopeful my PC is ready for the new security certificates. I run the HP Support Assistant each month to check for additional HP updates. The certificate update should happen as part of a monthly patch update.

Your mileage may vary depending on the manufacturer of your PC. If the new certificates are news to you, please check the website for your PC's manufacturer for details. If you want more information, please search "secure boot certificate expiration" in your favorite browser. ☺

Next P*PCompAS meeting: Saturday, 7 March 2026
A Zoom link will be sent out.
No presentation topic has been announced.

Meeting Minutes

by Greg Lenihan, P*PCompAS Secretary

The 7 February 2026 membership meeting was started via Zoom by President John Pearce at 9:02 am. The meeting minutes from last month were approved.

OFFICER REPORTS

VP Cary Quinn said the presentation today would be about CES 2026, with one video on security. We may have an APCUG presentation in April.

Newsletter editor Greg Lenihan said the deadline for the March newsletter would be 21 February.

Webmaster Greg Lenihan reported he made some progress on updating the opening page on our website and posting the latest newsletters. References to our former meeting place were removed. We need to add a reference to our Discord server. He shared the changes made on Zoom so members could see them.

Treasurer Toni Logan reported the $50 check for our APCUG dues cleared. The Volunteers Luncheon ran about $135. We have a total of $1463.40. Toni prepared a simple budget for this year. We'll have $50 APCUG dues, the state of Colorado will get $25, another $135 for a Volunteers Lunch, and $25 was added in for software/ hardware updates or purchases. She also will be doing an IRS filing in February.

Membership Chair Ann Titus had nothing to report.

Librarian Paul Godfrey had nothing new to report.

APCUG Rep John Pearce had nothing to report.

BOD Chair Bob Logan had nothing to report.

OLD BUSINESS

An audit of the treasurer's files was performed at the monthly breakfast on 17 January by Toni Logan, Cary Quinn, and Paul Godfrey. The audit passed muster.

NEW BUSINESS: None

ANNOUNCEMENTS

The next social breakfast meeting will be on Saturday, 21 February, at the Golden Corral, starting at 8:00 am.

Continued on page 3

In This Issue

Articles

P*PCompAS

Officers

President: John Pearce
jlpnet@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 February 2026 meeting.

Members and guest attending the January 31st Volunteers Luncheon

Digerati at the February breakfast at the Golden Corral

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.

You Don't Need to Pay for Third-Party Antivirus Software to Protect Your PC Anymore

by Timothy Jacob Hudson, reprinted with permission from HowToGeek.com

Original article at https://www.howtogeek.com/you-dont-need-to-pay-for-third-party-antivirus-software-to-protect-your-pc-anymore/

Summary

- Most consumer devices already come with strong default security measures equivalent to or better than third-party software.
- Common vectors of attack for malware are already blocked by modern systems before they even reach your antivirus program.
- Individual consumer PCs are not a primary target for cybercriminals, and cyberattacks are often conducted by exploiting vulnerabilities against third-party software, not the computer OS itself.

Do you still pay for third-party antivirus software like Norton or McAfee? You may be surprised to learn that there's no real benefit to doing so. Software like this is mostly obsolete today.

Who pays for third-party antivirus software, and why?

It might sound like a bold claim, saying that you don't need third-party antivirus software anymore. After all, recent statistics show that roughly half of American consumers use such programs. Interestingly enough, those same statistics also show that users over 65 are more than twice as likely to subscribe to paid antivirus software than those under 45.

Why is that? Well, there is certainly more than one reason, but a big one is simply misunderstanding and tradition.

In the past, having third-party antivirus software was prudent, almost mandatory to keep your computer safe. Some people who grew up in that era are comfortable with the idea of paying for these subscriptions, not realizing that things have changed: your computer protects itself just fine these days.

Not only do computers come out of the box equipped with incredibly good security these days, but most malware threats aren't even targeting individual consumers. But you don't have to take my word for it right away. Let's dive into this in more detail.

Default security measures are more than enough today

All of your consumer devices come with default protection right off the shelf. With iOS and Android, their official app stores weed out malware and keep you safe. Mac has been using XProtect anti-

Continued on page 4

Meeting Minutes (Cont. from pg 1)

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

AROUND THE ROOM

Cary Quinn is still trying to fix a power adapter on his Dell laptop. He took it apart to see what part he needs. Next month, Cary may discuss freeware he uses and backup solutions for mobile devices.

David George uses a Mac and his wife uses a PC, and he asked if there was a way to sync calendars. Cary recommends Google Calendar on each computer. You can link your accounts.

Toni Logan said her Dell computer shut down. Her oldest son had a Dell that did the same thing and did not know why. Toni backed up her financial files. Toni also is checking with Comcast about a new router because hers is old. They will probably mail it and she will have to install it using the Xfinity app on her phone.

John Pearce put the club computer on his home wireless network and updated it from 23H2 to 24H2. However, 25H2 is the current version, so had to change the setting to download updates as soon as available. John has started to receive his financial statements via the web (paperless) and it has turned into a bigger project than predicted. He is receiving lots of notifications of files to download and decided to change naming conventions. He needs more storage and is looking into a network storage device. And last of all, John is trying to get a Windows 10/Linux Mint dual-boot to work. The latest Windows update wiped out the dual-boot he installed.

Greg Lenihan shared the Central Florida Computer Society Discord server where Cary might find links to suitable topics from their meetings and special interest groups that could be used in our meetings.

PRESENTATION

Cary Quinn showed three videos on the best and worst of CES 2026 and also showed a video on security using Signal. ☺

Anti-Virus (Cont. from page 3)

malware for more than a decade, and it has an excellent record.

Windows has Microsoft Defender Antivirus, which has consistently aced security tests run by third-party organizations. Since around seven years ago, Defender Antivirus has consistently earned perfect or near-perfect scores in protecting your PC.

Needless to say, that's as good as it gets, and the program comes free with your Windows computer. There's no paid antivirus software that can outperform this free, default option from Microsoft. They may offer more features, but not more practical benefits. But even beyond these built-in systems, there are other reasons a third-party option isn't worth the trouble even when it's free.

Most malware vectors are already blocked

In the early 2000s, one of the most common ways to get malware was through an email attachment or a network connection. In fact, these methods were so popular at the time that most people still imagine malware coming through them.

But just like the default antivirus software employed by manufacturers, other aspects of the digital world have come a long way since then as well. Most email clients already block executable file attachments, and network firewalls are way more robust than they used to be.

Of course, there are always new attack vectors for malware, such as MSI packages, script interpreters, and much more. Even so, your default protection options, such as Microsoft Defender Antivirus, are constantly being updated and upgraded to face these threats, too.

Simply put, there's nothing that third-party antivirus software does for you that your free, default antivirus software isn't doing already. Many threats are already blocked by defenses like your firewall or email client, and your default antivirus software gets nearly everything else.

On top of all of that, you can exercise a bit of caution to avoid sketchy things that might pose a threat, such as suspicious links and websites claiming that you're the one-millionth visitor. Combine all of that, and you're more than secure enough with free, default antivirus software.

If you still don't feel better about all of this by now, there's yet another good reason you don't need to shell out for a third-party antivirus program

Individual consumer PCs are not a popular target for malware

We all like to think we're special, right? Well, it's pretty nice to be a nobody when it comes to cybercrime. The fact of the matter is that most cybercriminals aren't interested in targeting individual users and their computers. Most of us aren't worth the time and effort.

The real targets of malware attacks are big-name companies with millions or billions of dollars and valuable data. Sometimes their motives are more obscure, but regardless, the people getting targeted by hackers and malware are usually big organizations.

For example, Game Freak and the Internet Archive were hacked recently. Microsoft was hacked not too long ago due to a vulnerability in SolarWinds management software. A vulnerability in a third-party app called MOVEit resulted in Shell, BBC, British Airways, and other big companies getting hacked as well.

This is also why you should ditch the third-party antivirus software. Hackers are generally not targeting vulnerabilities in a computer's OS these days. They target vulnerabilities in third-party programs like MOVEit or SolarWinds to get in and cause damage.

In this way, your third-party antivirus program might even be more likely to create an exploitable weakness than it is to protect you, and it wouldn't be able to defend your computer against those types of threats anyway. Organizations require dedicated IT departments and real-time intrusion monitoring to do that.

This might all sound very scary: if Microsoft can get hacked, what's stopping a hacker from getting to little old you? If Microsoft can get hacked, why should you trust its Defender Antivirus for your computer?

Continued on page 5

12 Things That Cause Computer Crashes

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

Have you ever experienced the dreaded Blue Screen of Death? Does your PC or Mac computer lock up, freeze, crash, or display cryptic error messages? These sorts of problems can be very difficult to diagnose, because many things can cause a desktop computer or laptop to crash (and even burn!). Before you blame those mischievous gremlins, here are some common causes of computer crashes and some tips on how to deal with them...

Why Do Computers Crash?

Often I'll get a reader question along the lines of "My computer keeps crashing, what should I do?" As much as I'd like to help, that's not enough information to diagnose the problem and suggest a solution. It's like telling your auto mechanic there's a funny noise coming from your car, and asking him for advice on how to fix it.

A computer crash may or may not be in the eyes of the beholder—it can take the form of a complete power down, an unexpected restart, the Blue (or Black) Screen of Death, or a screen freeze. In some cases, just restarting the computer will get you going again. But chances are, you haven't really solved the problem. Here are a dozen things that can cause your computer to crash:

#1 - HEAT: An overheated processor (CPU) or graphics card (GPU) may shut down your computer without warning to avoid damage. Heat can build up because a cooling fan is not working or is clogged with dust. Hard drives are also temperature sensitive, and I suspect that motherboards and RAM memory can become flaky when temperatures inside a desktop or laptop computer rise above normal.

One of my computers used to experience random crashes every few months. I found that periodically opening the case and cleaning all the fans, heat sinks and components with a can of compressed air would solve the problem temporarily. Replacing the system fan (which was making a loud buzzing noise) solved the problem.

There are several free utilities that monitor temperatures within your computer and fan speeds; some will even let you control fan speed. See Do You Know Your Computer's Worst Enemy? for additional tips and download links. A few years ago, my desktop PC would just lock up or shut down at seemingly random times. I used a free temperature monitor program to determine that my graphics adapter was overheating. When I opened the case, I found that its cooling fan had seized, and was partially melted! Fortunately, it was designed to send a "Warning, Danger!" signal to the motherboard, which prevented it from catching fire. Computers (and even smartphones) can catch fire, so don't ignore signs of overheating.

I should mention that laptops are especially prone to overheating, especially thin and light

Continued on page 6

Anti-Virus (Cont. from page 4)

Again, it's a matter of viable targets and vectors of attack. You're not a high-value target worth hacking 99% of the time, and the ways those hackers got into big companies like Microsoft are far removed from the type of vulnerabilities you possess as an individual user.

Even if you don't have full faith in your default antivirus software, don't forget: anything that could get past that default antivirus software could get past some third-party antivirus software too, so there's still no real benefit to paying for it.

Ultimately, the days of third-party antivirus software are long past. Paying for these subscriptions is paying for peace of mind, but only if you don't realize how little it does for you and your computer security.

We live in a tough economy right now. If you're looking to save on your monthly bills, cutting out these extra programs is a great place to start. After that, maybe consider saving some money on your electric bill. ☺

Computer Crashes (Cont. from page 5)

models. Laptops are more prone to heat-related crashes because their compact designs pack electrical components into small spaces. The thin chassis of a laptop relies on narrow heat pipes, heat sinks, and small fans to move heat away from the CPU and GPU, which can become clogged with dust, pet hair, or cooking grease over time. When airflow is restricted, temperatures rise quickly, and the system may respond in two main ways: thermal throttling or full shutdown.

Thermal throttling is when the processor or graphics chip deliberately slows itself down to reduce heat and protect the hardware from damage. This can make the laptop feel sluggish, stutter during video playback, or freeze briefly. A full shutdown happens when temperatures reach a critical threshold and the system powers off abruptly to prevent damage. It's a bad idea to use your laptop on soft surfaces like beds and couches that block vents. You might try using a laptop cooling pad, and periodically cleaning the fan and vents with compressed air. (Make sure the laptop is powered off, and aim the nozzle so you're blowing dust out of the vents, not deeper into the laptop.)

AskBob reader Dan shared this related story: The cashier at a hair salon was swearing at her computer because it kept shutting down every few minutes. Her "expert" friend recommended an new PC, but Dan suspected a heat problem, and offered to check it out. He found that the heat sink was COMPLETELY packed with hair, grease and chemicals that had been pulled in by the fan. Dan removed the heat sink, cleaned it thoroughly, and it ran like a champ. Other environmental factors such as smoking, pets, carpeting and cooking fumes can exacerbate the overheating issue.

And as strange as it sounds, fire ants have been identified as culprits in some overheating incidents by infesting computer components and damaging thermal paste and pads. These ants are attracted to the electrical fields and warmth of PCs, where they can eat or nest within GPUs and power supplies. Yikes, if you have fire ants in your computer, overheating may not be your worst problem!

#2 - SOFTWARE ERRORS: If crashes occur only when you're using a specific software application, that's the first place to look for problems. Sometimes a software bug causes a crash when a certain operation is attempted. Check the software maker's website for any updates that may fix your problem. It's also a good idea to scan your computer to ensure that all your software is up to date with the latest security patches. See Here's Why You Must Keep Your Software Updated (and how to do it for free) for some tips on getting that task done.

Don't forget that Chrome/Edge/Firefox browser extensions and Windows Store apps can cause problems. Keep them in mind when attempting to isolate a software problem. Occasionally, software may become corrupted or "scrambled" and cause crashes too. If a software update (or removal) and a disk check (see below) don't fix your problem, you may have to remove and then re-install the corrupted software.

The Windows Reliability Monitor is a built-in diagnostic tool that gives you a timeline view of how stable your PC has been, and will show you if there have been crashes, unexpected shutdowns, or system errors. It's a handy tool when you're trying to figure out whether crashes are tied to a specific app, driver, or Windows update. On Windows 10 and 11, type "reliability" in the Start search box and press Enter.

#3 - HARD DRIVE ERRORS are yet another potential cause of computer crashes. A problem with your hard drive doesn't necessarily mean that it needs to be replaced. There are a variety of factors that can cause files, folders, or partitions to become damaged or lost. Human error, malware, and poorly designed software are all possibilities.

A drive error may be a logical error in the Master File Table, or a defective sector on the disk itself. Windows has a built-in utility that will detect and fix logical errors, and mark bad sectors so they are not used to store data. See Windows Hard Drive Errors for more information about the CHKDSK utility, and other programs that can help. (That article was written for Windows 7, but the information still applies to Windows 10 or 11.)

SSDs (Solid State Drives) can also develop issues such as bad blocks, firmware bugs, and optimization errors. And despite what you may have heard, CHKDSK does work on SSDs, and can help to clear up some problems.

If you can't restart your computer after a crash, see Harbinger of Hard Drive Hardship? before going off in search of a new hard drive.

#4 - MALWARE: Viruses and other forms of malware often causes computer crashes; in fact, some malware is written to do just that. Running a full scan with one or more good anti-malware tools is a good thing to do when crashes occur at random. My current favorite is PC Matic, which uses a "whitelist" approach, in addition to traditional "signature based" virus detection methods.

#5 - DEVICE DRIVERS: Outdated device drivers can cause crashes. I've heard reports where simply plugging a device into a USB port caused a system crash. Drivers

Continued on page 7

Computer Crashes (Cont. from page 6)

usually work fine until you install a new operating system or a major update to an existing operating system, such as a Service Pack or one of those twice-yearly Windows Updates. If you start suffering crashes after an operating system change, updating the drivers for your printer, scanner, CD/DVD drive, external hard drive and other peripheral devices may solve the problem. The best place to look for new device drivers is the vendor's website. Stay away from "driver update" websites and downloadable programs that offer to scan your system and supply new drivers. To learn more about device drivers, see [TIP] Time to Update Your Drivers?

#6 - FLAKY MEMORY: It's rare for RAM memory to go bad, but that can be a cause of computer crashes. Sometimes a RAM chip with a "bad spot" will work fine, until a software program attempts to use that portion of memory. Windows Memory Diagnostic is a built-in tool that will test your RAM memory for errors. On Windows 10 and 11, type "mdsched" in the Start search box and press Enter. Memtest86 is another utility that can diagnose problems with RAM and other hardware that may be causing computer crashes. My related article How to Test and Fix Your Computer Hardware contains links to that and several other handy diagnostic programs. Both of those memory testers require a system restart.

#7 - FAILING POWER SUPPLY: Unexpected restarts can also be a sign of a failing power supply. When someone has tried everything else, and their computer is still glitching at seemingly random times, I sometimes recommend a new power supply. Fortunately, power supplies are cheap and easy to replace yourself. See Is It Time to Replace Your Power Supply? for some helpful tips.

#8 - ELECTRICAL PROBLEMS: A sudden surge or loss of electrical power can damage your computer or cause it to crash. In addition to losing anything you were working on at the time, power glitches can also cause head crashes in hard drives, which can damage a disk and the data on it. A power surge can damage your power supply or other components. To guard against power surges and power failures, I do recommend that you get an uninterruptible power supply (UPS) to provide a backup power source and surge protection for your computer. For complete protection, look for one that comes with software and a cable that can send a signal to safely shutdown your computer in the event of a power failure. See Battery Backup Power - Here's What You Need to Know.

#9 - OVERCLOCKING: Over-clocking involves fiddling with the BIOS settings to run a computer's CPU, GPU, or RAM at a higher clock rate than it was originally designed for. In some cases, this can result in better performance, but it can also lead to system instability and crashes. Overclocking accelerates the wear and tear on computer components, and can cause overheating and memory errors. See How Fast Is Your CPU? Benchmark it! for some related info.

#10 - COSMIC RAYS: Really? Yes, really! A friend of mine who is an expert in electronics trouble shooting said this: "A Single Event Upset (SEU) can cause electronic circuitry to malfunction. **An SEU can be caused by a power glitch, or a cosmic ray passing through a integrated circuit, and can actually flip the logic state (from 1 to 0 or vice versa) of a circuit.** A cascading effect may trigger a hardware lockup, an error in calculation, or an infinite loop in software." See Silver Bullets, Cosmic Rays and Tired Computers to learn more about that.

#11 – Firmware and BIOS/UEFI Bugs These are less often the culprit of system crashes, but motherboard firmware can cause crashes after updates or even at seemingly random times. Consider checking your computer vendor's website for BIOS/UEFI updates. If there was a recent firmware update, reverting to an older version may fix instability issues.

#12 – Resource Exhaustion (Gremlins again)
Resource exhaustion happens when a computer runs out of a critical resource such as RAM, CPU time, or disk space, and the system can no longer handle new tasks smoothly. When memory is exhausted, the operating system starts swapping data in and out of the page file on the hard disk, which is much slower than using physical RAM. This "thrashing" makes the machine feel sluggish, unresponsive, or prone to freezing and crashes. Similarly, if the CPU is maxed out for long periods or the disk is completely full, programs may fail to start, save files, or stop responding, even though there is no obvious hardware fault.

From the user's point of view, resource exhaustion looks like those pesky gremlins causing mysterious slowdowns, apps hanging, or the system crashing under heavy load. (This can happen when a buggy program has a memory leak or an infinite loop.) Running Task Manager or Resource Monitor can reveal which process is consuming excessive CPU, RAM,

Continued on page 8

PSA: You Can Watch a Ton of Genuinely Great Movies For Free on YouTube

by Sydney Butler, reprinted with permission from HowToGeek.com

Original article at https://www.howtogeek.com/psa-you-can-watch-a-ton-of-genuinely-great-movies-for-free-on-youtube/

Most of us think of YouTube as a place where the content is made by regular people, rather than professional outfits. For the most part, this is still true, but fundamentally, YouTube is technically no different from any streaming service. Which is why you'll also find honest-to-goodness movies on YouTube that are both legal and free to watch.

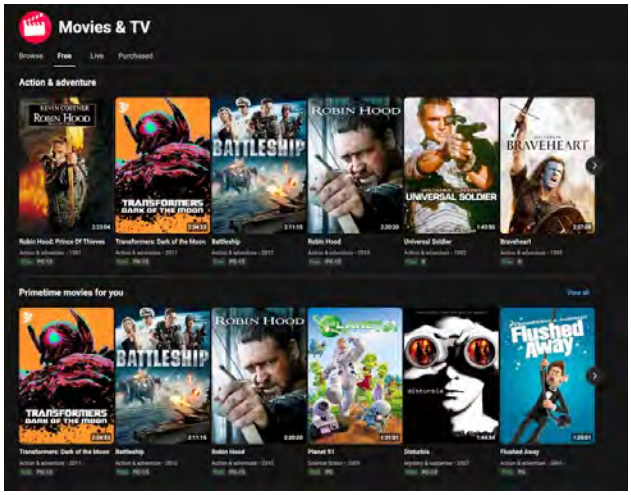
What counts as a "classic movie" and why YouTube has them

While you're not likely to find free new movies on YouTube (at least not legally), there are plenty of films that are now in the public domain or have had their rights cleared. In some cases, it's the actual rights holder of a film that's chosen to upload it to YouTube and make it widely available. After all, this is one way to keep making advertising money or get a slice of that YouTube Premium pie.

The only thing to watch out for is illegal uploads. YouTube's pretty good at removing infringing content these days, but some uploads are still done by people without permission. Sometimes they're well-meaning, like uploading an old VHS recording or a DVD rip for something that's streaming nowhere. In some cases the rights holders are unclear or no longer exist, so there's no one who can make a legal takedown claim.

Either way, it's best to make sure the upload you're watching has the right permissions to be on YouTube, and this is usually disclosed in the description of the video, the channel, or simply by virtue of the channel having official standing.

If you're looking for newer fare, well, you can head over to the official YouTube "Movies & TV" section and check under the "Free" tab. You'll see plenty of great titles there too, which have been licensed by YouTube.



This isn't available in every region, but if you have a VPN, you might find it possible to access this library of free films if you set your service to the right region.

Prime examples you can watch right now

On the classic movie front, you can watch something like *It Happened One Night*, a 1934 romantic comedy starring Clark Gable. This is part of a massive classic movie collection hosted by a channel called Stream City, which also has many more contemporary films like *1941* starring John Belushi, Dan Aykroyd, and Ned Beatty. If you want to find cult movie gems, then Cult Cinema Classics is another advantageous resource.

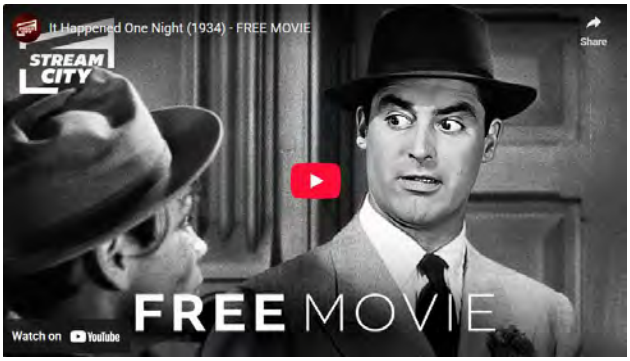
Continued on page 9

Computer Crashes (Cont. from page 7)

or disk. Closing or updating that app usually restores stability.

BONUS TIP: If your problem is software-related, there's a free program called WhoCrashed that you can run after experiencing a system crash, unexpected shutdown/reset, or "blue screen of death" event. WhoCrashed will analyze your Windows system log files, report on the most likely cause, and offer suggestions on how to fix the problem. WhoCrashed runs on Windows XP, Vista, 7, 8, 10 and 11. ☺

Free Movies (Cont. from page 8)



If we head over to YouTube's official free movie selection, you can watch classics like *Good Will Hunting*, *Spaceballs*, and *Braveheart*. To be honest, I think the actual streaming quality on YouTube leaves much to be desired, but given that you can watch these for free, I'm willing to take on a more lenient attitude.

How to find them, and how to watch

The easiest way to find classic movies to watch on YouTube for free is to use search terms like "full movie free" or "classic full movies." As I mentioned above, you're likely to get quite a few hits for movies that have been uploaded illegally, and I advise you to avoid those since we can't condone piracy. Instead, look for channels that specialize in legal uploads of full classic films, and become a subscriber so you can easily access those libraries in the future.

If you really want to play it safe, simply stick to the official YouTube Movies & TV channel. The selection is quite large, so there should be more than enough to keep budget-conscious streamers happy.

Why this is more than just nostalgia

I don't know about you, but I'm constantly disappointed by the selection of movies on streaming services these days. When I first subscribed to Netflix (and only Netflix), it had pretty much any movie I could want in its database. It's why I started feeling more comfortable with the idea that physical media wasn't necessary.

Oh, what a fool I was. As more streaming companies entered the market, that backlog of old movies became fragmented, and large swathes of them left streaming completely, which is a major reason I own literally hundreds of DVD and Blu-ray discs today, ensuring that the movies I care about the most will always be available to me.

Not everyone wants to own a room full of discs, though, and YouTube is doing a phenomenal job of filling that specific gap of movies that still have a strong niche following, but that big streaming companies can't justify hosting unless it's literally part of their own IP. Between dedicated licensed channels and YouTube's own official solution, there's a good chance you'll find old films you're looking for on the same service known for react channels and overblown video thumbnails. ☺

Tips to Try

Windows 11 drag tricks: Dragging a file does way more than you think. Hold Ctrl while dragging to make a copy. Hold Shift to move it without duplicating. Hold Alt to create a shortcut. Use the right mouse button while dragging for a quick options menu on drop. And drag any window to the edges or corners of your screen to snap it into place.

Windows can fix itself: There's a safety feature you can turn on now in case your computer fails to start later. Go to Settings > System > Recovery > and enable Quick machine recovery. If it can't boot one day, your PC will connect to the internet, look for a fix from Microsoft and try to repair itself.

Your screenshots are tattletales: Every photo your phone takes stores hidden data called EXIF. That includes the exact GPS location, date, time and even what device you used. Share a photo from your home and someone can pinpoint your address. On iPhone, open a photo, tap the info (i) button, then tap Adjust under the map and select No Location. On Android, open the photo in Google Photos, tap the three dots > Edit > Location > Remove location. Note: Depending on your make and model, the steps may be a tad different.

P*PCompAS Newsletter
Greg Lenihan, Editor
e-mail: glenihan@comcast.net

Coming Events:

Next Membership Meeting: **7 March 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 March @ 8:00 am, Golden Corral, 1970 Waynoka Road**

Newsletter Deadline: **21 March**

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