Bits of Bytes

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

Volume XLIII | March 2023 | Issue 3

Meeting Minutes

by Greg Lenihan, P*PCompAS Secretary

Next P*PCompAS meeting: Saturday, 4 March 2023
Cary Quinn explains what is new in the public domain and neat new freebies for 2023.

President Cary Quinn called the 4 February 2023 membership meeting to order at 9:05 am. David George made the coffee, and Greg Lenihan brought doughnuts. There were no guests, although it was good to see Ilene in person. A $1 donation is requested from members for doughnuts and coffee. A motion was made to approve the January minutes published in the newsletter and the motion passed.

OFFICER REPORTS

President Cary Quinn recognized 13 members in attendance and 4 on Zoom.

VP Paul Godfrey said Joe Nuvolini would give a presentation today on CES and he is working on next month's topic.

Secretary/Newsletter Editor Greg Lenihan announced the next newsletter deadline is 18 February.

Treasurer Toni Logan stated the checking account still stands at $51.74, savings at $2783.47 (after 12 cents interest) for a combined total of $2835.21.

Membership Chair Ann Titus had nothing to report.

Librarian Paul Godfrey had nothing to report.

APCUG Rep/Webmaster Joe Nuvolini was passing along APCUG e-mail from Judy Taylour about events and some said they appreciated it.

BOD Chair Ann Titus had nothing to report.

OLD BUSINESS:

Paul Godfrey has still been unable to get a response from Natalie at the church about projector screens. We aren't sure the church wants them.

A date has not been set for the Volunteer's Luncheon. It was normally held the weekend before Super Bowl

NEW BUSINESS

We are going back to having our monthly breakfasts at the Golden Corral starting in February. Nuvo has booked our reservations.

The club made a motion to give the church $250 cash as our yearly gift and the motion passed. A check was written and given to Greg Lenihan to give to the church.

ANNOUNCEMENTS

John Pearce and Ann Titus have birthdays coming up in the next couple of days.

The next social breakfast meeting will be Saturday, 18 February, at the Golden Corral, starting at 8:00 am.

Our next membership meeting is Saturday, 4 March 2023.

AROUND THE ROOM

John Pearce is gradually getting more accustomed to Windows 11. Right now, he hasn't had the time to do the things he wants to do.

Ilene Steinkruger has a lot of old electronics sitting around and wants to get rid of it. For example, she has a couple of Amazon Kindles whose batteries no longer work and wondered if they have personal information on them.

Joe Nuvolini's brother-in-law has an XP and Win7 machine and he went paperless for his DFAS account. He wasn't able to download forms from the site, so had to use Joe's computer to go back to a paper account.

AJ Whelan asked whether those that had Comcast for cable TV noticed that DVR storage seems to be shrinking. No one seemed to notice a problem or knew what were the storage limits.

Toni Logan finds it interesting that Netflix is dropping family accounts and may require everyone to log in once a month.

PRESENTATION

Joe Nuvolini went through a series of videos of new and best products on display at CES. He provided a link to many CES videos at https://**tinyurl.com/s8dbrw2z.** ☺

In This Issue

Articles

P*PCompAS

Officers

President: Cary Quinn
cary.quinn@gmail.com

Vice President: Paul Godfrey
godfreyp2724@comcast.net

Secretary: Greg Lenihan
glenihan@comcast.net

Treasurer: Antoinette Logan
antoinettelogan@gmail.com

Staff

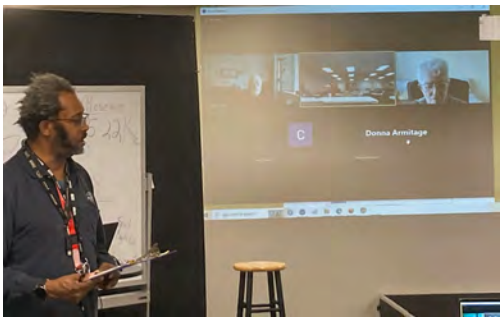
APCUG Rep/Webmaster: Joe Nuvolini
Barista: David George
Drawings: Cary Quinn
Editor: Greg Lenihan
Librarian: Paul Godfrey
Membership: Ann Titus

Committees

Audio: A.J. Whelen
Hospitality: Vacant
Programs: Paul Godfrey
Publicity: Vacant
Nominating: Vacant

Board of Directors

Harvey McMinn
A.J. Whelan
John Pearce
Bob Logan
Barbara McMinn



President Cary Quinn leading the February meeting with remote attendees on screen

Members in attendance at the February meeting.

Digerati back at the Golden Corral for the February monthly breakfast.

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.

What is Wi-Fi, and How Does It Work?

by Gaurav Shukla, reprinted with permission from HowToGeek.com
Original article at: https://www.howtogeek.com/865706/what-is-wi-fi/

Key Takeway

Wi-Fi is a networking technology primarily used to connect to the internet. It uses radio waves to transmit data wirelessly and is supported by various modern electronic devices, including computers and smartphones.

Wi-Fi has become one of the most popular technologies. Most of us use it to access the internet. But what does connecting to Wi-Fi mean, what does Wi-Fi stand for, and how does it work? Here's everything you need to know.

Defining Wi_Fi

Wi-Fi is a wireless networking technology used by computers, smartphones, and other devices to connect to the internet or other devices. It's based on a set of wireless communication standards developed by the Institute of Electrical and Electronics Engineers (IEEE). These standards are also known as IEEE 802.11.

Originally introduced in the late-1990s, Wi-Fi has come a long way. Like any other technology, it has evolved and gotten better. While the first Wi-Fi generation—802.11-1997—offered a maximum link rate of 1-2Mbps, the newest generation—Wi-Fi 6—has a maximum link rate of 574-9608Mbps. The link rate is the top data transfer speed across a wireless link between a router and a device. Wi-Fi 7 or 802.11be, which is expected to be adopted as the next Wi-Fi generation in 2024, is even faster at 1376-46120Mbps.

RELATED: ***Wi-Fi 5 vs. Wi-Fi 6: What's the Difference?***

What Are the Different Wi-Fi Generations?

Wi-Fi generation	IEEE standard	Adopted	Maximum link rate
*Wi-Fi 0**	802.11 or 802.11-1997	1997	1-2Mbps
*Wi-Fi 1**	802.11b	1999	1-11Mbps
*Wi-Fi 2**	802.11a	1999	6-54Mbps
*Wi-Fi 3**	802.11g	2003	6-54Mbps
Wi-Fi 4	802.11n	2008	72-600Mbps
Wi-Fi 5	802.11ac	2014	433-6933Mbps
Wi-Fi 6/ Wi-Fi 6E	802.11ax	2019/ 2020	574-9608Mbps
Wi-Fi 7	802.11be	(2024)	1376-46120Mbps

** Unofficial name*

As we mentioned earlier, Wi-Fi has grown a lot since the debut of its first generation in 1997. As of January 2023, seven Wi-Fi generations have been formally unveiled, including IEEE 802.11-1997. Each Wi-Fi generation has brought new capabilities and has typically been faster than its predecessor.

Although the first three generations of Wi-Fi—802.11, 802.11b, 802.11a—saw some uptake among corporations and early adopters, the introduction of 802.11g in 2003 truly pushed Wi-Fi into the mainstream. It was superseded by 802.11n or Wi-Fi 4 in 2008, which significantly improved the Wi-Fi link rate by introducing MIMO and a channel bandwidth of 40MHz.

However, as of 2023, Wi-Fi 4 and older generations have mostly become a thing of the past. So instead, you'll primarily find Wi-Fi 5 or a newer version, like Wi-Fi 6 or 6E, in modern devices.

How Does Wi-Fi Work?

Wi-Fi uses radio waves to send information to and from devices. A wireless router or access point converts data received from a wired connection to radio waves and transmits it. These radio waves are intercepted by a receiver, such as your smartphone, and converted back to data you can read, listen to, or watch. It's a continuous process in which both the access point and the receiver constantly exchange data as required. So essentially, this is how you receive the webpage you're looking at now, the music you're streaming, or the YouTube videos you watch on your phone.

Wi-Fi has traditionally used the 2.4GHz and 5GHz bands of the radio wave frequencies, but the Wi-Fi 6E version has also introduced the use of the 6GHz band. The 6GHz

Continued on page 4

Wi-Fi (Continued from page 3)

band has more bandwidth than the 2.4GHz and 5GHz bands, so there is less congestion, resulting in faster connection speeds and better Wi-Fi performance.

How Is Wi-Fi Different From Ethernet?

Wi-Fi and Ethernet are two mediums for getting Internet access to your device or forming a local area network. Unlike Wi-Fi, which is wireless and uses radio waves to transmit information, Ethernet is wired and uses physical cables for data transmission. There are advantages and disadvantages to both mediums.

While Wi-Fi is convenient and great for mobility, Ethernet is more reliable, consistent, and secure. Ethernet is also better at reducing latency. The speed of the connection in both mediums depends on the hardware you are using, such as your wireless router, Wi-Fi adapter in your device, Ethernet cable, network switch, etc.

What Does Wi-Fi Stand For?

Wi-Fi doesn't stand for anything. It's not an abbreviation but a marketing name. Interbrand, a leading brand consultancy, invented it for the Wireless Ethernet Compatibility Alliance (now called Wi-Fi Alliance), an industry group that handles the advocacy and branding for Wi-Fi. It's sometimes erroneously spelled out as "wireless fidelity," but that's inaccurate.

According to Phil Belanger, a founding member of the Wi-Fi Alliance, some of his colleagues weren't too sure about having a marketing name that didn't mean anything. So the group added a tagline to Wi-Fi: The Standard for Wireless Fidelity, which led to the confusion around wireless fidelity being the full form of Wi-Fi. But the tagline didn't take off and only diluted the brand. So once Wi-Fi became popular, Wi-Fi Alliance dropped it.

What Do You Need to Access Wi-Fi?

If you want to use Wi-Fi at home, you'll primarily need a wireless router and a Wi-Fi-capable device. There is an excellent chance that the router provided by your internet service price (ISP) already has Wi-Fi support, and you just need to enable it. If not, you can always pick one from our recommendations for the best Wi-Fi routers and connect it to your ISP's router with an Ethernet cable. Even the most budget-friendly routers will do the job.

Depending on the size of your home, your ISP's wireless router may or may not be able to send Wi-Fi to every corner. So if you face dead spots or low signal strength, the best mesh routers or Wi-Fi range extenders can help.

In terms of devices, unless you are still rocking a feature phone, your phone will have Wi-Fi support, and you can simply connect to your newly set up Wi-Fi network. Similarly, laptops and tablets also come with Wi-Fi support. But if you own an older desktop, you'll have to confirm whether it can work with Wi-Fi. If it lacks Wi-Fi, you can get a Wi-Fi adapter.

But if you want to connect to a public Wi-Fi hotspot to access the internet, such as Starbucks Wi-Fi, all you need is a Wi-Fi-capable mobile device, which includes almost every laptop, tablet, and smartphone.

RELATED: *How to Check Your Wi-Fi Signal Strength*

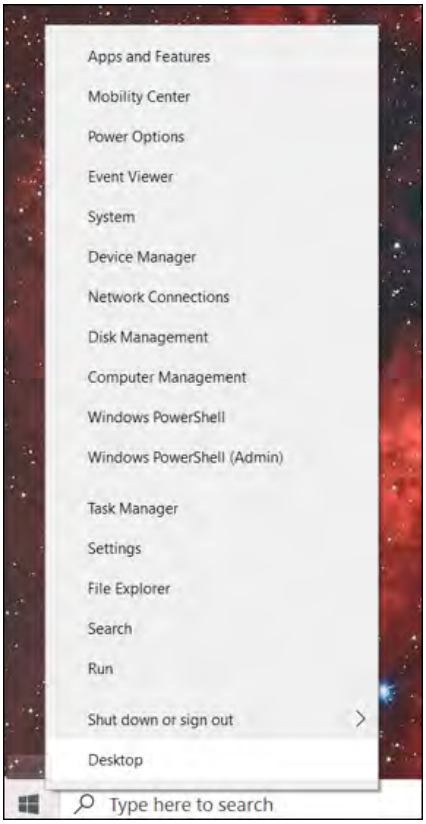
A Convenient Networking Technology

Wi-Fi has arguably changed the way we access the internet on our devices. This has been possible because of its convenience, mobility, simplicity, and expandability. You don't need to worry about the number of available Ethernet ports or deal with different cables. It's also relatively easy to set up and takes seconds to connect.

If you are curious to know even more about it, we have excellent guides on improving your Wi-Fi signal, finding your Wi-Fi password, connecting to Wi-Fi on Windows 11, and more. ☺

Tip: The Power User Menu

The hidden power user menu, which you can launch by pressing Windows+X on your keyboard or by right-clicking the Start button, gives you quick access to some of Windows' most important tools and settings, such as Task Manager, Device Manager, Event Manager, Disk Management, Network Connections, and more. It even includes sleep and shut down options, and you can quickly open File Explorer with a couple of clicks.



Here's How to (Maybe) Trace an Email

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

Thud... an unwanted, spammy email with an obviously fake "From" name just landed in your inbox, and you wish you could find out where it actually came from. Or maybe you got an email several days after it was sent? Read on to learn about some free tools that can help with both situations...

Who Really Sent That Email?

There are times when it's useful to trace the path that an email traveled to get to your inbox. The most common situation is suspected spam, when you want to discover the true source of an email. Delays in receiving emails can also be diagnosed by tracing the path that emails take to you. But tracing emails on your own can be pretty frustrating.

Every email contains hidden information about the path it took to reach you, called "header information." To most people, it looks like 100 or so lines of gibberish, which is why it's hidden by your email program. Here is just a small part of a typical example:

Received: by 110.46.73.35 with SMTP id z62csp234112ita;
Mon, 18 Aug 2022 05:10:19 -0700 (PDT)
X-Received: by 10.67.3.3 with SMTP idbs3pad.121.144187;
18 Aug 2022 05:10:17 -0700 (PDT)
Return-Path: EDDCOQNWXFNNFKD.BNLk9QJHMF3M
HBFK.BNL@example.com
From: "Some User" <someuser@example.com>
To: "My Name" <myaddress@mydomain.com>
Message-ID: 60762392-7dbc-50e41ecd8bee@xt2mta1217.
xt.local

With the possible exception of the "From" and "To" lines, ordinary mortals struggle to make sense out of email headers like this snippet. Geeks who run email servers or those who hunt down spammers for fun may get eyestrain looking at raw headers, too. But there are many online tools that parse email headers to make them more legible by humans.

The Email Header Analyzer is a free online tool provided by MX Tools, Inc., a Texas-based firm that primarily serves network administrators and ISPs. Anyone can use the Analyzer, however; just paste a block of header information into the tool's form and click the "Analyze Header" button.

The results include a bar graph, indicating any delays in the hops that the message took to reach you. It will also show you if any of the mail servers that relayed the message are on a spam blacklist. If the sender's server is on a blacklist, that's a big red flag that the message may be suspicious, malicious, fictitious, or pernicious.

Wrapping Your Head Around Headers

But where do you find those hidden headers? Google provides brief, clear instructions on how to find message headers in Webmail messages, including Gmail, AOL, Yahoo! Mail, Excite Webmail, and Hotmail (now Outlook.com). Instructions for finding headers in desktop clients such as Microsoft Outlook, Apple Mail, Mozilla Thunderbird, and Opera are also given.

The Google Apps Toolbox also includes a message header analyzer. Its main purpose is to highlight delays in message relays and pinpoint their possible sources. (Typically, email messages are received within seconds, even if they must travel half-way around the globe.)

IPTracker is an email header tool that's more suited for non-techie users. In addition to showing the IP address of the sender, it also shows the name of the sender's Internet Service Provider, and the city and country of origin on a map.

Interpreting Email Headers is another Google tutorial, for those who want to read raw email header info. It walks you through each line of a sample header, explaining in plain English what it means.

Identifying a Spammer

If a sender forges the "From" line, you may not be able to find the email address of the actual sender. But analyzing the email headers will show you at least that it WAS forged, and give you an indication where it originated. According

Continued on page 6

What is Common Sense?

It's not so common

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

When it comes to internet safety, the most oft-cited advice is: **Use common sense.**

The most common response is: *Great. Just what exactly does that mean?*

When it comes to technology and safety, "common sense" is important, poorly defined, and quite *un*common.

Let's see if we can define it with some already-familiar rules.

In Short

What is common sense?

Common sense can be summed up in several familiar adages:

- If it sounds too good to be true, it's probably not true.
- If it ain't broke, don't fix it.
- Free is never free.
- Read what's in front of you.
- Don't believe everything you read.
- Be skeptical: question everything.
- Do your research.

If it sounds too good to be true…

Many malicious incursions mask themselves in promises of the seemingly irresistible.

Practical examples of offers that really are too good to be true include:

- Many "free download" advertisements
- Software promising to speed up your computer
- Ads including the phrase "one stupid trick…" or variants
- Click-bait headlines including the phrase "you won't believe" or similar

Common to most, beyond the fact that the promises seem extreme, is that *you weren't looking for them when you found them.*

Look at any website, and you'll see advertisements. Many are legit and well-positioned, but others are little more than over-the-top attempts to get you to click or download whatever they have to offer.

Particularly when you're not looking specifically for something, don't fall for extreme or outlandish claims. The same can be said of most shared or forwarded hoaxes and urban legends as well as many news stories.

Continued on page 7

Trace Email (Cont from page 5)

to Statista, Russia is the top spam-producing country, where 24.77% of all spam originates.

It's also important to keep in mind that a lot of spammy emails are sent from ordinary home computers that are compromised by malware. The spamming masterminds can use networks of infected personal computers that number in the millions, to send their detestable dispatches anonymously. So don't assume that the person in the From: line of an email has any knowledge of having sent it.

For extra credit, you can paste the IP address found on the first "Received" line into the MaxMind GeoIP tool, to learn the approximate geographic location of the sender. (Note that first "Received" line is the one closest to the bottom of the headers. As messages travel over the Internet, the header lines stack up, so you need to read them in reverse order.)

For example, I got a classic 419 Scam email from a spammer recently, showing this: "Received: from User (UnknownHost [105.112.26.217]) by vdt.com …" Sure enough, the MaxMind tool confirmed my suspicion that the sender was in Lagos, Nigeria.

If you think a message is from a spammer or a scammer, don't reply to it. You'll only be confirming to the bad guys that your address is valid, and possibly embroiling yourself in a heap of trouble.

If you can determine that the outgoing mail server is an Internet Service Provider, you can forward the suspect message, with full headers exposed, to abuse@[isp-name].com and often they will disable the sender's account. Don't bother forwarding unwanted emails to the FTC at spam@uce.gov – that address was phased out in 2004. You can, however report a spam message to the FTC, just don't expect a reply. They will share your report with local, state, federal and foreign law enforcement partners. The FTC does not resolve individual complaints, but your report might be used to investigate cases.

Personally, I find it more satisfying to just hit the DELETE button and move on with my life. ☺

Common Sense (Cont. from page 6)

Common sense tells us that **if it promises too much, if it seems too extreme, if it seems too astonishing… *then it's probably completely false*.**

If it ain't broke, don't fix it

Whether following over-inflated promises such as those I just mentioned or out of desperation, I often see people trying to do things to their computers that have nothing to do with a problem they're experiencing.

- They try to solve speed problems they don't have.
- They try to remove malware that is not present.
- They try to update software they don't run.
- They try to fix problems that have nothing to do with their computer.

The list goes on.

I understand that each of those assumes a certain amount of knowledge. How do you know you *don't* have a specific problem? How do you know malware *isn't* present? How do you know that the problem you're experiencing is with the website you visit and has nothing to do with your computer?

That's a fair concern. But if you don't know that you have a problem, then why are you trying to fix it?

Turn the thinking around.

Common sense means not doing something because you *might* have a problem, but taking action because you *know* you have a problem and not before.

Research the problem first. **Confirm you actually have a problem that needs fixing before you try to fix it.**

(I'll talk about research shortly.)

Free is never free

The economist's old acronym is TANSTAAFL: "There ain't no such thing as a free lunch." That's exceptionally true online.

Every "free" service has a cost. It may be the advertising you see, the mailing list you need to sign up for, the personal information you're sharing, or something else entirely, but ***there is no such thing as "free"* on the internet**.

Most commonly, people fall into the "free" trap through advertisements of this variety: "FREE Scan! Scan your computer for malware for FREE!"

Some of these ads are 100% accurate. The *scan* is completely free. The not-so-free part? If you want to do anything about what the scan finds, you'll need to pay. It's a common sales tactic.

Less reputable programs lie to you. They warn you of malware and other scary things you don't have or that aren't issues — all making it appear that giving them your money is the only way to avoid certain doom.

This brings us to another important point.

Read what's in front of you

This is a point that frustrates me. It works like this:

- A program fails or something goes wrong.
- The user gets frustrated or confused.
- The user completely misses the fact that *the solution was included in the error message* or descriptive text.

Another similar scenario:

- Someone gets an email and reads the first line, which is so outrageous that their reactions kick in right there and they stop reading.
- As a result, they miss the text after that, which puts the statement in a clearer context or provides additional information and removes all the outrageousness.

When something goes wrong with your computer, take the time to **read what's on the screen in front of you**. I get so many questions that could be avoided or quickly dealt with had the questioner just slowed down and read the instructions in front of them.

I understand that those instructions are not always comprehensible. Honestly, I do. But *sometimes they are* so clear and obvious that just taking the time to slow down and carefully read what's on your screen will get you a long, long way.

Which brings us to the flip side of the coin.

Don't believe everything you read

I'm a firm believer that people are basically good. But that doesn't mean that everyone is good or that everyone has your best interests in mind, particularly when it comes to the internet. It's too easy, particularly in today's connected and information-rich world, to spread misinformation as fact. We see it *all the time*.

Misleading ads are only one blatant example. Misleading ads pre-date the internet by decades, if not hundreds of years. It's just

Continued on page 8

Common Sense (Cont. from page 7)

that today's technology often makes it difficult to distinguish snake oil from valuable and effective medication unless we're careful.

The internet can also supply us with a wealth of information to help us separate over-inflated claims from reality.

It can also provide us with even more misinformation. "It's on the internet, so it must be true" is one of those statements everyone laughs at because it's so blatantly wrong, it's laughable. Common sense tells us that because something is on the internet has absolutely no bearing on its accuracy. Yet we see people act as if it is, believing random and misleading statements from vague sources with less-than-altruistic agendas.

With information coming at you from so many random directions from sources both reliable and unreliable, **it's critical that we not believe everything we read just because it's been formatted attractively on a site that *looks* authoritative**.

And that brings us to the most important point of all.

Above all, be skeptical

Want something that's very common sensical? **Question everything. Even me.**

Never accept information at face value, particularly on the internet, and particularly from sites or individuals you've never heard of before.

Be skeptical. Ask questions. Consider the source and what that source's agenda might be in spreading its message.

Over time, develop a set of resources that you trust. Naturally, I hope *Ask Leo!* will be one of them, but honestly, what matters more is that you reach out and find your own trustworthy sites, sources, services, and individuals.

Then use those resources to help you evaluate the constant stream of information and misinformation heading your way.

Yes, that's a little bit of work. But it's critical.

Do This

Search for yourself

Learn the basics of how to not only use a good search engine (Google, Bing, or others), but also how to interpret the results. **Understand the difference between the advertisements presented on the search results page and the actual results**.

Look for well-known reputable sites in those results, not just sites that happen to rank highly. As much as search engines work to make it not so, ranking highly in a search result is not an indication that the site is legitimate or trustworthy.

If you choose to look at information presented by a site you've never heard of before, remember, *you've never heard of it before!* Without more research, there's no way to know whether the information is valid, biased, or completely bogus.

Get help

If you're uncertain how to go about researching a particular topic, **there's nothing wrong in asking for help**. You may have more experienced friends or family members who can help you find what you're looking for. Librarians are also valuable resources when trying to determine the validity of information you run across online.

Regardless of who's helping you, it's still important to be skeptical. When they suggest a site as a trustworthy resource, don't be afraid to ask them why they trust it.

Look carefully for confirmation

There are two types of confirmation:

- Source B repeating what source A has said.
- Source B independently presenting similar information or coming to the same conclusion source A did.

The first isn't confirmation at all, it's *repetition*. The problem is, when enough sites and so-called sources all repeat what *only one* of them has said, it may feel like many sources have all come to the same conclusion. In reality, it's nothing more than a single opinion repeated over and over. This is known as the *echo chamber*.

Remember: **repetition isn't confirmation**. You want to find multiple sources that are confirming (or denying) the issue, and are doing so having arrived at their conclusions *independently*, using their own research.

Use debunking sites

I'm a huge believer in using sites like snopes.com, factcheck.org, mediabiasfactcheck.com, politifact.com, truthorfiction.com, or any of several others before reacting to the latest over-the-top, can't-possibly-be-true news story, tech tip, or emailed rumor.

Many are very timely and do the kind of research you want to see before getting all excited

Continued on page 9

Common Sense (Cont. from page 8)

or worked up about what just landed in your inbox.

Use resource sites

There are resource sites for just about any topic. Develop a set of sites that you trust. For example, when it comes to technology, I would hope Ask Leo! is on your list. Visit the sites for which you already have a level of trust and see what they say about the issue at hand. As always, I'm not saying that you need to trust them completely, but use them *as part of your research* to develop your own well-thought-out opinions.

The bottom line is this: if something you run across is worth the effort of taking any action at all — even if it's just to forward an email — then it's also worth your time to research it first. At worst, it may save you some embarrassment. At best, it could protect your computer, your identity, and even your possessions. ☺

Do This Before Installing Any Program on Your Computer

by Albert Khoury at Komando.com (tip from 1/6/23)

Copyright 2023. 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

Your PC is running things in the background without you knowing it, and Windows is the main culprit. While some quiet tasks are necessary to keep things going, others can be switched off. The result is a faster, smoother experience. **Tap or click here for five processes you can end right now**.

When you buy a new computer, it comes packed with features and programs you might never use. You may also find third-party apps included in a deal with the manufacturer.

The same applies to software. Whether you're installing an operating system, a productivity app or a game, there's always a chance they'll try to sneak in some things you don't need. You can catch them in the act and prevent it before it happens.

Here's the backstory

When installing software, you'll sometimes find different installation options such as express install (sometimes called recommended) and custom install (also called advanced install and often labeled for advanced users).

This is how they get you. Since many people don't consider themselves "advanced" users, they'll go with the simple or recommended option. Makes sense. Just let the program do all the work.

The truth is that express installations often include unwanted software and sometimes malware. At the very least, they'll take up more storage space.

Some programs even change your default settings, browser, homepage or search engine, so you'll want to have the option to opt out of this. You won't have these options in the express or default installation.

Finally, express installations can opt you into data collection, sync your contacts, or include some other invasion of privacy. While you may be able to change these settings later, it's better to nip them in the bud during the installation phase.

Here's what to do

Always go with the custom or advanced option. Aside from choosing a destination folder or drive, you may have the option to uncheck boxes for optional software and settings you don't want or need.

Read everything carefully and tick off the boxes as needed. Don't worry about messing anything up — the installer will include the necessary files to run the program no matter what you choose. It just won't include the extras you left out.

RELATED: PC speed boost: You can disable these services without breaking anything

NOTE: For smaller, simpler apps, you may have the option to download a portable version. A portable app doesn't use an installer. All the files required to run the app reside in a single folder, which you can put anywhere on your system.

Rather than installing a portable app, you typically download it as a ZIP file, extract it to a folder, and run the executable file for the app. ☺

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

Coming Events:
Next Membership Meeting: 4 March beginning at 9 am (see directions below)
Next Breakfast Meeting: 18 March @ 8:00 am, Golden Corral, 1970 Waynoka Road
Newsletter Deadline: 18 March
Check out our Web page at: http://ppcompas.apcug.org