

The Digital

(membership includes  
monthly subscription)

# Viking



**Twin Cities**

PC USER GROUP

NEWSLETTER

Minneapolis & St. Paul, Minnesota USA • Vol. 45 No.2 • September 2024

*TC/PC Exists to  
Facilitate and Encourage  
the Cooperative Exchange of  
PC Knowledge and  
Information Across  
All Levels of Experience*

**September 2024**

Membership Info .....2

Do You Use Two-Factor

Authentication? ..... 3

Another Look at

Artificial Intelligence . 5

Burned by Another

Security Breach?..... 8

Microsoft Windows 11

Copilot: How Not to

Remove It.....10

TC/PC Calendar.....14

Membership Application 15

Maps to Events..... 16

<sup>4</sup>  
**General Meeting**  
**Tuesday, September 10, 2024**

**7:00 PM**

**FAST: Free Ad Supported Television**

**Presenter: Jack Ungerleider**

**Via Zoom Only**

FAST networks are a growing group of streaming networks that as the name implies are free of charge and support the programming with ads. The main networks have connections to production studios: Pluto.TV (Paramount/CBS), Tubi (Fox), FreeVee (Amazon). We will spend some time looking at these three services and what they offer. 🖥️

**Note:** All TC/PC Meetings and SIG Groups will be virtual until further notice. Visit [tcpc.com](http://tcpc.com) for info.

**Tech Topics with Jack Ungerleider via Zoom at 6pm before the General Meeting.**

TC/PC is a  
Member of



**24-Hour Information • [www.tcpc.com](http://www.tcpc.com)**  
Application form inside back cover

# The Digital Viking

The Digital Viking is the official monthly publication of the Twin Cities PC User Group, a 501(c)(3) organization and an all-volunteer organization dedicated to users of IBM-compatible computers. Subscriptions are included in membership. We welcome articles and reviews from members. The Digital Viking is a copyrighted publication and reproduction of any material is expressly prohibited without permission. Exception: other User Groups may use material if unaltered and credited.

**Disclaimer:** All opinions are those of the authors and do not necessarily represent the opinions of the TC/PC, its Board of Directors, Officers, or newsletter staff. TC/PC does not endorse, rate, or otherwise officially comment on products available; therefore, readers are cautioned to rely on the opinions presented herein exclusively at their own risk. The Digital Viking, its contributors, and staff assume no liability for damages arising out of the publication or non-publication of any advertisement, article, or other item. All refunds in full or in partial, for advertising, membership or any other item shall be at the sole discretion of the Twin Cities PC User Group Board of Directors.

## Advertising

Full page (7½ x 9½)	\$100.00
Two-thirds page (7½ x 6)	80.00
Half page (7½ x 4¾)	65.00
One-third page (7½ x 3)	50.00
Quarter page (3½ x 4¾)	40.00
Member Bus. Card (2 x 3½)	10.00

Multiple insertion discounts available.

Contact Sharon Walbran at: SQWalbran@yahoo.com

Deadline for ad placement is the 1<sup>st</sup> of the month prior to publication. All rates are per issue and for digital or camera-ready ads. Typesetting and other services are extra and must be requested in advance of submission deadlines.

Payment must accompany order unless other arrangements are made in advance. Place make checks payable to: **Twin Cities PC User Group**

## TC/PC 2024-2025 Board of Directors

Meets once or twice per year. All members welcome to attend.

Visit [www.tcpc.com](http://www.tcpc.com) for meeting details.

<b>President</b> —Lee Kaphingst	leekap@comcast.net
<b>Vice President</b> —Curtiss Trout	ctrout@troutreach.com
<b>Secretary</b> - Sharon Walbran	sharon.walbran@gmail.com
<b>Treasurer</b> - Sharon Trout	strout@troutreach.com
<b>Newsletter Publisher</b> Sharon Walbran	952-925-2726 sharon.walbran@gmail.com
<b>Web Master</b> Curt Trout	ctrout@troutreach.com
Board Members:	
Steve Kuhlmeier	skuhlmeier@hotmail.com
Lon Ortnier	612-824-4946 lon@csacomp.com
Lee Kaphingst	leekap@comcast.net
Jeannine Sloan	Ambassador for Friendship Village
Curtiss Trout	ctrout@troutreach.com
Sharon Trout	strout@troutreach.com
Jack Ungerleider	jack@jacku.com
Sharon Walbran	sharon.walbran@gmail.com

## TC/PC Member Benefits

Product previews  
and demonstrations

Special Interest Groups  
Monthly Newsletter

Discounts on products  
and services

Contests and prizes

## Business Member Benefits

All of the above PLUS:

FREE ½ page ad on  
payment of each renewal

20% discount on all ads  
Placed in the *Digital  
Viking* Newsletter

Up to 5 newsletters mailed to  
your site  
(only a nominal cost for each  
additional 5 mailed)

## Newsletter Staff Editor Sharon Walbran

# Do You Use Two-Factor Authentication?

By Phil Sorrentino, Secretary & Newsletter Contributor

Sun City Center Computer Club

<https://sccccomputerclub.org/>

philsorr (at) yahoo.com

If not, you might want to consider it for specific accounts if it is offered. Two-factor authentication is a way of adding an additional level of privacy to a computer account. When you set up an account, typically on a computer server, you assign a "User Name," which is not private, and a Password, which you are advised to keep private. This provides a certain level of privacy because to access your account, you must provide the User Name, which is not private, and the password, which is, hopefully, known only to you. This is probably all you need to do for most of your accounts. However, adding another level of privacy would be prudent to guarantee that you can access the account only for specific accounts. These accounts would be those that you would be very unhappy if someone else, or some other computer, could access and download or manipulate its contents. An account that contains very personal information or an account at a financial institution might be just this type of account.



## Client-Server Architecture

Keep in mind the internet employs a Client-Server Architecture. Using this architecture, your account is on a server computer, not your home computer, tablet, or phone. These (client) devices only provide the ability to connect to the server and manipulate the account contents. So if someone else knew your User Name, which is not protected, and knew or stole or guessed your Password, which is hopefully protected, they could access the account and manipulate the contents. If it's a financial account, they could probably manipulate its value. Unfortunately, no matter how diligent you are in protecting your password, sometimes passwords become known to the bad guys, such as "hackers." If hackers get into your financial account, they can possibly use it for fraudulent financial transfers or payments, or worse, a password alone may not be enough. Even many services that don't offer two-factor authentication have instituted various checks on the computer attempting to use a particular server account, like sending an email to the email of record indicating a new computer is trying to access the account and asking, "Is this you?". If you are concerned about this, google "What happens if someone accesses my account" and see the possibilities. Nowadays, many services employ two-factor authentication to help guarantee that only the account owner can access a particular account.

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

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



What you know + What you have = Positive Authentication

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

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

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



[Go to Page 1](#)

# Another Look at Artificial Intelligence

By Joel Ewing, President, Bella Vista Computer Club  
Bits & Bytes, February 2024

<https://bvcomputerclub.org>

[president@bvcomputerclub.org](mailto:president@bvcomputerclub.org)

(For a general description of artificial intelligence, also see the article "What Is Artificial Intelligence" in the April 2019 edition of the BVCC *Bits & Bytes* at <https://bvcomputerclub.org/PDF/B&B/2019-04.pdf>)

## *Background*

Although having a background in Computer Science, I do not consider myself an expert on AI; but like many, I have seen over the last decade the improved (but not perfect) ability of smartphones to translate the spoken word into written text, chatbots on the Internet and telephone call centers that can briefly make you think you have reached a human, and the fairly sophisticated behavior of "self-driving" cars, including some experiments with autonomous self-driving vehicles in restricted environments.

When in full "self-driving" mode, a Tesla car can recognize enough of the environment around it to sense and follow lane markings, sense other vehicle types and their relative speeds on all sides, interpret speed limit signs, stop signs, stop lights, a variety of warning signs, speed limit signs, adjust speed for sharp curves and slower vehicles, to make decisions on passing slower vehicles. When navigation mode to a destination is engaged, an extensive road map database allows it to know when to turn and what lane it needs to be in for the next turn, to suggest the optimal super-charger stations for long trips, and to automatically pre-condition the battery temperature for optimal charging speed before arriving at a charging station to minimize charging time. Yet with all that sophistication, Tesla's most important safety features are (1) monitoring the human driver for alertness and (2) alerting the human driver to take over if the road conditions go outside the bounds the automation can reliably handle. This is great for removing much of the monotony of long-distance driving on consistently marked interstate highways but not so valuable for city driving, where road repairs, obstructions, and local driving customs tend to demand more human interaction.

The topic of AI was recently raised in a professional computer-related online discussion list I follow. I have also been involved in a church-related Religion & Science group meeting on Zoom over several years that have discussed, among other topics, whether humans are the only life forms on Earth that are conscious or aware, AI, and whether machines could ever cross the thresholds of self-awareness and become aware and direct competitors of humans, possibly even a threat. Some of the following thoughts come from those discussions.

## *AI Current Capabilities*

AI may easily surpass humans in the ability to analyze and deduce conclusions from a large amount of data and propose actions – it already has done that in some areas that are sufficiently limited in scope.

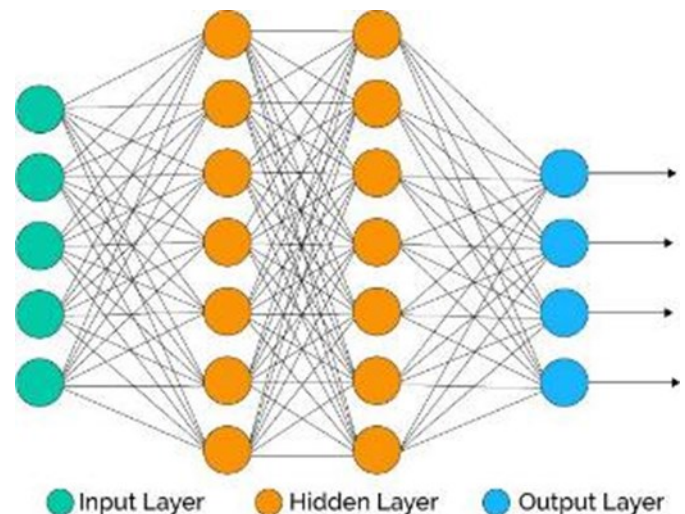
AI is already being utilized to assist in medical diagnosis, such as interpreting medical scans, where large scans may need to be analyzed tediously to look for minor anomalies.

Many Internet search engines utilize some AI techniques to improve the quality of the results.

Some of the more interesting recent free Internet search additions are ChatGPT, BardAI, and BingAI, which can accept queries in natural language and return paragraph responses that appear appropriate, almost human-like. It is possible to request responses in the form of specific types of poetry (ChatGPT) or to request the creation of an image featuring certain objects (BingAI).

Without getting too much into details, at least two main techniques are involved under the covers for the deep learning of advanced AI: trained digital neural networks and large databases created by analyzing many natural language sources of information.

Digital neural networks attempt to emulate the brain's design on a small scale. The idea is that you have a large number of nodes (neurons) that are interconnected to nearby layers of the network, but that each of the interconnections can be adjusted by giving a "weight" to each of the connection paths to determine what strength of incoming signals is sufficient to activate the neuron. To "teach" a neural network, you must supply many different combinations of input signals (on the left), for which the desired output (on the right) is known, and modify the weights so that the correct outputs are obtained for as many as possible, hopefully, all, input value combinations. This is a computationally expensive and, thus, energy-intensive process, but once the best weights are obtained, it is easy to replicate the neural network. The illustration on the right only has 23 nodes. A useful neural network may have thousands of nodes.



Neural networks are particularly useful for cases without clear written rules for arriving at the outputs, like pattern recognition of images and sounds, interpreting the ambiguous parts of natural language speech and text, and predicting large social system behavior like the stock market. While it can be hoped that a new combination of inputs not used in the training process will also produce reasonable outputs, this is not guaranteed and heavily depends on how the training data was chosen. Another drawback of neural networks is that there is no way to explain how they arrived at any specific output from some specific input.

It is clear from ChatGPT's behavior that it has access to an extensive database of contemporary and historical literature. Whether that does or should include those materials still under copyright protection is debated as to whether that violates fair-use restrictions. To be of greatest use, the natural language must be parsed to determine what is being discussed (nouns) and related descriptions (adjectives) and actions (verbs) and deduce further relationships. From that, it is possible to produce indexes and statistical probabilities of relationships. Applying a similar parsing to information requests, it is possible to either find sentences or paragraphs relevant to the query or (more complex) possibly construct "original" relevant sentences based on known associations with the query topic.

### *AI Limitations*

One problem that needs to be addressed is that a considerable amount of data is loose in the real world, which is misinformation, and too much garbage in still produces garbage.

Many humans have problems telling the difference between fact and fiction and between reality and conspiracy theories. Humans have biases in their data choices, yet they will choose the data sources to program future AI. This will inevitably cause some problems.

Every year, you find people, sometimes prominent people, that stumble across a parody or satire written in the style of a news article, mistake it for real news, and make a fool of themselves by calling others to take action against the alarming "news" they have just uncovered. Such humor is usually so over-the-top that it is easily recognized by ordinary people aware of current events. However, some still take it as factual, even if it is on a website like "The Onion," which is well-known for only publishing imaginary news releases.

One needs to understand that while AI can provide helpful guidance within the realm for which it has been trained, it is not infallible. If you ask a neural network to categorize an unexpected combination of inputs, it may make an incorrect identification. Suppose you ask an AI system trained from analyzed text about a topic that lacks accurate information. In that case, it may make incorrect inferences from data that it thinks are similar because they appear statistically related. Even if it has processed relevant information, it may not be able to accurately interpret context, implicit relationships, and time ordering of relationships. If you ask an ambiguous question ("Show me something like X"), the AI may not understand the distinction between creating something fictional that looks like "X" versus finding a fact like "X."

There have already been at least two instances reported in the news of a judge berating attorneys for submitting supporting briefs referencing legal precedents that didn't exist because some AI system created a plausible fictional reference to support their legal argument.

The general public is already indifferent to AI's limitations and abusing AI: asking questions of AI apps in areas where the AI is poorly trained and trusting without verification of fallible responses as being authoritative because a machine produces them. Some newsworthy cases of this abuse have been reported when fatalities result after owners of cars with AI autopilots requiring supervision find ways to entrust the AI with unsupervised autonomous driving, and a crash occurs when the AI encounters situations it is not designed to handle.

### *Could AI be Dangerous*

Some theorize that if we could build a neural network of enough complexity – many orders of magnitude larger than possible today – at some point, a threshold might be passed. That creation might become self-aware and possibly worthy of being called sentient. What discoveries such a tool could make and create! The problems are multi-fold: If it has more knowledge than any human and can exercise creative thought faster than any human, its analysis of human history may lead it to the conclusion it should be the master, not the enslaved person, of humans. This has long been a persistent cautionary theme of science fiction writers. In the fictional Dune prequel "The Battle of Corrin," where sentient machines and humans have long been at war, there is a fictional quote from the sentient robot Erasmus: "Humans were foolish to build their competitor – but they couldn't help themselves."

Suppose we were to succeed in creating machines that could truly approach the complexity and creativity of the human mind. Might they not also be subject to some of the same dangerous mental instabilities as human minds when confronted by conflicting "facts" or subtle design deficiencies? Fatal problems like those afflicted the fictional HAL 9000 in "2001: A Space Odyssey" and the M-5 Multitronic computer in "The Ultimate Computer" Star Trek episode.



I don't think we are at any risk within my lifetime of finding a way to cross that threshold, but that doesn't mean that we shouldn't be concerned that AI in its present state has the capability of causing harm.

AI-based tools used by financial institutions to evaluate whether to approve or deny credit requests have been found to exhibit bias against granting loans to those in minority groups. The AI tools were programmed using data about loans that had been approved subject to historical biases against minorities. Without great care in programming, AI can be used to justify that there is no bias when the reality is that the bias was included in the AI programming and is just more hidden.

Another way we are already seeing AI being abused is by its use to create and spread misinformation on the Internet. While not perfect, it is already good enough to produce deep-fake video and audio and false news reports and control bots on social media networks that spread messages to promote and amplify division and hate. There is some hope that it may be possible to employ AI on the other side to detect and suppress such abuse, but that does require corporations to accept that responsibility.

Another area that should be a serious concern is the possibility that AI could be given the power to make and implement life-and-death decisions without adequate human oversight or just to propose actions that humans might blindly follow in a life-or-death situation. The science fiction genre is full of plots suggesting how badly this can go – possibly human enslavement or extinction.

When you grant AI the power to make decisions and take actions in the real world, most of us want "intelligence" involved, wisdom, and morality. Most of us want decisions made by others that impact our lives to be constrained by a moral compass of what is right and fair. We have no idea how to build that awareness into AI, and since there is no universal agreement on whose standard of morality to use, that may be an impossible task. Even if there was agreement on how to define morality and how to embed that concept into AI, do we trust fallible humans to consistently implement that design without error?

A legitimate concern is that if future AI regulation or its enforcement is inadequate, some individual or corporation with more power and money than wisdom may go rogue, ignore whatever AI restrictions are in place or commonly accepted, and create a dangerous AI device because of a belief it will enhance their short-term profit.

We must be very cautious about what kinds of decisions and actions we entrust to AI in the short and long term. We also need to research how best to enforce that caution. Perhaps future AI, appropriately applied, might even become part of the solution.



**[Go to Page 1](#)**



# Burned By Another Security Breach?

By Kurt Jefferson, Editor, Central Kentucky Computer Society

<https://newsite.ckcs.org/>

lextown77 (@) mymetronet.net

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

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

This security breach is especially troubling because, as Bleeping Computer notes, "AT&T says a massive trove of data impacting 71 million people did not originate from its systems after a hacker leaked it on a cybercrime forum and claimed it was stolen in a 2021 breach of the company." The stolen personal data is from an alleged 2021 AT&T breach that hackers calling themselves ShinyHunters attempted to sell on the dark web.

Search tools like Google, Yahoo!, or DuckDuckGo cannot reach the dark web. It's comprised of websites where everything from drugs to guns to personal information is sold for the right price. Whether or not the stolen data came from AT&T, the wireless giant says it has started notifying millions of customers about the data thefts.

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

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

Numerous tech websites are urging AT&T's current and former customers to freeze their credit accounts at the big three credit agencies—TransUnion, Experian, and Equifax. In addition, sign up for two-factor notification on their AT&T accounts and change your AT&T password if it hasn't already been changed. Also, monitor your credit reports.

This isn't the first time the phone company has had problems. In a major AT&T outage in March, the company apologized for the disruption and offered a \$5 credit to customers.



[Go to Page 1](#)

# Microsoft Windows 11 Copilot: how not to remove it

*The horse's mouth, Copilot AI, did not answer my how-to-remove question accurately or completely.*

by John Krout, Newsletter Contributor and Presenter

Potomac Area Technology And Computer Society

<https://patacs.org/>

## Introduction

Automatic installation of un-requested software is a behavior that I do not favor.

Microsoft forced a double whammy on my Windows 11 desktop computer on February 17.

The February 17 PATACS+OPCUG joint monthly meeting was Zoom-only due to adverse weather. At about 3 PM during that meeting, Zoom froze on my computer, and a minute later, it was apparent the entire computer was frozen. I pulled the power plug and then re-inserted it. When starting up, the computer installed a Windows 11 operating system update, displaying an increasing completion percentage. The download of that update probably caused the initial freeze.

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

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

One day after the meeting, I found an unfamiliar icon in the right corner of my Windows 11 gray taskbar. You can see it in **illustration 1**. The icon is on the right and includes the letters PRE.



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

I also found a scalable Copilot logo graphic in the C:\Windows folder tree. You can see that in **illustration 2**.



Obviously, Microsoft wants to beat its generative AI competitors to desktops. The competitors include mega-firms like Google, Adobe, and Autodesk and startups like OpenAI.

## Where does AI do its work?

In a nutshell, today and for the indefinite but no doubt long future, AI will be executed on servers, not your computer. Personal computers just don't have the hardware for storage and execution of generative AI.

Consider the following consequences of that situation.

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

I am against such monetization.

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

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

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

### **My first interactive generative AI experience**

You can see my dialog with Copilot below. My input is identified as You. I added italics to clarify the two major sub-headings in the generative AI answer.

As you will see below in the dialog, the answer was incomplete. Perhaps I should have asked how to remove the Copilot preview *from my computer*. Maybe I should be glad that the AI could not read my mind.

**You:**

how to remove the Copilot preview

**Copilot:**

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

*Remove Copilot from Taskbar (Temporary):*

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

Follow these steps:

Open the Settings app (you can search for it in the Start menu).

Click on Personalization.

Scroll down and select Taskbar.

Toggle off the Copilot option.

*Disable Copilot Completely (Permanent):*

If you want to permanently disable Copilot, follow these steps:

Click on Start and search for gpedit to open the Group Policy Editor.

In the left-hand panel, navigate to User Configuration > Administrative Templates > Windows Components > Windows Copilot.

Double-click on Turn off Windows Copilot in the right-hand panel.

Click Enabled, then click Apply and OK.

Remember that if you ever want to enable Copilot again, you can follow the same steps and choose "Not configured" or "Disabled" instead of "Enabled" in the last step.

That's it! If you need further assistance with Windows, feel free to ask. 😊

<end of dialog>

I did try the permanent removal option. I encountered a problem: **gpedit** was not found on my Windows 11 computer. I searched on the Windows Store and did not find it there. It appears to be part of Windows 11 Pro only. I am disappointed that Copilot did not say so.

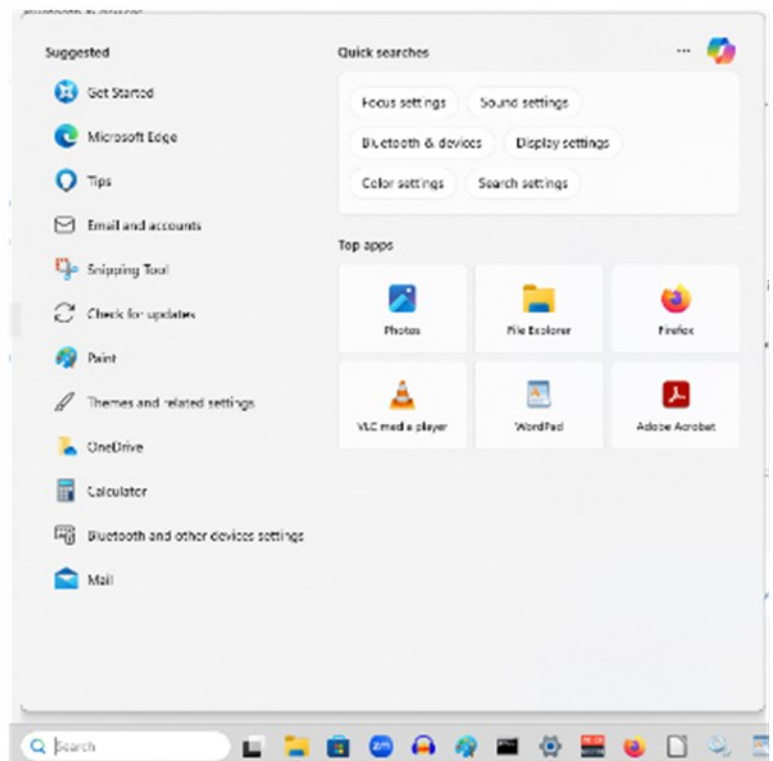
I searched the Web and found a page of scripts for installing gpedit, one for Windows 10 and one for Windows 11. When the script is finished, I can start Gpedit by typing Gpedit.msc in the Windows 11 search field.

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

### Copilot is also found elsewhere on the computer.

A day later, I found the Copilot icon in another place, the popup that appears when the Search field in the taskbar is clicked. You can see that second icon in the upper right corner of **illustration 3**. The second icon does **not** contain the letters PRE.

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



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

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

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

### **Is removal from a computer not possible?**

My Web research also turned up a Microsoft forum page on removing Copilot. A Microsoft rep posted an answer repeating the gpedit technique and reiterated a familiar refrain: **Copilot is now a part of the Windows 11 OS and cannot be removed.**

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

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

Microsoft has demonstrated that it is willing to install what the company considers the latest Microsoft killer app **without giving its Windows customers a choice before or after the installation.** Giving customers a choice might limit Microsoft's profit potential.

That lack of a choice shows that Microsoft does not treat customers respectfully.

ABOUT THE AUTHOR: John Krout is a retired software engineer who has worked on contracts for many Federal agencies in the Washington DC metro region. He began writing and speaking about creative uses of personal computers in the early 1980s. More recently, he has also covered interesting uses of smartphones, tablets, and electric vehicles. He lives in Arlington, VA. John is also an avid photographer and recently enjoyed a trip to Texas to photograph the eclipse.



**[Go to Page 1](#)**

Meetings start at 7:00 PM (9:00 AM on Saturday) unless otherwise noted. \*Virtual Meetings during Covid pandemic.

## September

## October

SUN	MON	TUES	WED	THU	FRI	SAT
1	2	3	4	5	6	7
8	9	10 7 pm General Mtg FAST: Free Ad Supported Television  6pm Tech Topics	11	12	13	14 Linux on Sat- urday SIG 9am—Noon
15	16	17	18	19	20	21 MS Office SIG (includes Access) 9am—Noon
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8 7 pm General Mtg TBD  6pm Tech Topics	9	10	11	12 Linux on Sat- urday SIG 9am—Noon
13	14	15	16	17	18	19 MS Office SIG (includes Access) 9am—Noon
20	21	22	23	24	25	26
27	28	29	30	31		



## You have just read an issue of The Digital Viking.

*Would you like to receive this delivered directly to your email or business each month?*

As a member of TC/PC, the Twin Cities Personal Computer Group, one of the benefits is reading this monthly publication at [www.tcpc.com](http://www.tcpc.com).

As a member of TC/PC, you may attend any or all of the monthly Special Interest Group (SIG) meetings and be eligible for software drawings. The small membership fee also includes access to real-live people with answers via our helplines, discounts, and various other perks.

Does membership in this group sound like a good way to increase your computer knowledge?

It's easy to do! Simply fill in the form below and mail it to the address shown.  
(If you use the form in this issue, you will receive an extra month for joining now.)



9/24

### Here's the info for my TC/PC Membership:

Full name \_\_\_\_\_

Company name \_\_\_\_\_

Address \_\_\_\_\_

City \_\_\_\_\_ State \_\_\_\_\_ Zip \_\_\_\_\_

☐ Home ☐ Business ☐ Change address: ☐ Perm. ☐ Temp. 'til \_\_\_\_\_

Home phone \_\_\_\_\_ Work phone \_\_\_\_\_

Online address(es) \_\_\_\_\_

Where did you hear about TC/PC? \_\_\_\_\_

☐ I DO NOT want any of my information disclosed.

☐ I DO NOT want to receive any mailings

### I'm signing up for:

☐ Individual/Family Membership (\$18)

☐ Business Membership (\$100)

If an existing member your # \_\_\_\_\_

### Make checks payable to:

**Twin Cities PC User Group  
341 County Rd C2 W  
Roseville, MN 55113**

### Or sign up on our website:

<http://www.tcpc.com>

☐ Check # \_\_\_\_\_ ☐ Bill me

☐ New member ☐ Renewal ☐ Prior member

### I'm interested in:

☐ Training classes ☐ Volunteering

☐ Special Interest Groups: New User, Access, etc.

List here:

**Administrative Use Only** Rec'd \_\_\_\_\_ Chk# \_\_\_\_\_



**September 10, 2024**  
**7:00 pm**  
**General Meeting**

**FAST: Free Ad Supported Television**

**Presenter: Jack Ungerleider**

**Via Zoom Only**



341 County Rd C2 W  
Roseville, MN 55113

***FIRST CLASS MAIL***