

Sun City Computer Club

Windows SIG

May 13, 2024

**Questions, Comments, Suggestions welcomed at any
time**

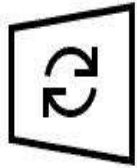
Even Now

- Audio Recording of this session
- Use the link above to access MP4 audio recording
- Audio Recording in Progress
- SIG attendees are required to be members of the chartered club sponsoring that SIG.

Sun City Community Association By-law

- Sig leader – anyone?
- Contributors – Tom McBride
Tip Tipton

Windows Update



Updates available

Last checked: Today, 12:19 PM

2025-05 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems (KB5058379)

Status: Downloading - 0%

Windows Malicious Software Removal Tool x64 - v5.133 (KB890830)

Status: Installing - 0%

Windows 10 Patch Tuesday

Windows Update



Updates available

Last checked: Today, 12:15 PM

Download & install all

Windows Malicious Software Removal Tool x64 - v5.133 (KB890830)

Downloading - 100%

2025-05 Cumulative Update for Windows 11 Version 23H2 for x64-based Systems (KB5058405)

Downloading - 0%

Windows 11 Patch Tuesday

- The May 2025 Patch Tuesday update includes several important fixes and improvements:
- ♦ Windows 10 Update (KB5055612) – This update for Windows 10 version 22H2 brings security patches and maintenance updates. It also fixes GPU paravirtualization issues in the Windows Subsystem for Linux (WSL) and updates the Windows Kernel Vulnerable Driver Blocklist to prevent Bring Your Own Vulnerable Driver (BYOVD) attacks.
- ♦ Windows 11 Update (KB5055627) – The Windows 11 24H2 update introduces new AI features, including Windows Recall, Click to Do, and Semantic Indexing for Copilot+ PCs. ♦ Security Updates – Microsoft has released cumulative security updates for Windows 10 and Windows 11, addressing vulnerabilities across multiple system components.

Microsoft Patch Tuesday May

- Visit Microsoft Store for those updates
- Check Office 365 for updates
- MANY vendors do Patch Tuesday updates
- 78 vulnerabilities
- 11 critical
- 66 important
- 5 actively being exploited
- 2 publicly known

Patch Tuesday

A possible topic of discussion might be the options for people not wanting (or able) to migrate to Windows 11.

Purchase EOL support extension? I've heard that may or may not be available for home users.

Move to Linux distro – Mint is mentioned frequently.

Has there ever been any interest in a Linux SIG?
Do nothing but need to create a windows installer before EOS happens.

Member Contribution





I don't usually get involved with the Windows SIG because I mainly use a Mac but one thing worth mentioning is that Microsoft is ending support for RDP (Remote Desktop Program) on May 27 and removing it from the Windows store though it will still be downloadable from <https://learn.microsoft.com/en-us/previous-versions/remote-desktop-client/connect-windows-cloud-services?tabs=windows-msrdc-msi#download-and-install-the-remote-desktop-client-for-windows-msi>.

Microsoft created the Windows App which is available in the Windows store but cannot be used to remotely connect to another stand-alone Windows machine but only to systems running in their cloud. Rather surprisingly, they also developed and support versions of the Windows app for Android, ChromeOS, IOS, and Mac which are available free in their respective stores. This makes it very easy to connect to a Windows system from any of these operating systems and the connections work quite well. Why they don't support Windows-to-Windows connections is beyond me. The link for more information is <https://learn.microsoft.com/en-us/windows-app/troubleshoot-known-issues-limitations?tabs=web>. I assume that this app will eventually support the Windows-to-Windows connections but I can't find any actual statement to that effect from Microsoft.

The easiest alternative I've found for machine-to-machine connections is RustDesk which can be downloaded from rustdesk.com.

- <https://techcommunity.microsoft.com/blog/windows-itpro-blog/windows-app-to-replace-remote-desktop-app-for-windows/4390893>

Corrected Link
Member Contribution

- Unified Access – Instead of juggling multiple apps, Windows App provides a single interface to connect to Cloud PCs, virtual desktops, and remote services. 
Enhanced Display Options – Supports multi-monitor setups, dynamic display resolutions, and customizable home screens for a smoother experience. 
Optimized for Microsoft Teams – Improves audio and video performance for remote meetings, reducing lag and enhancing collaboration. 
Easy Account Switching – Allows users to seamlessly switch between multiple accounts, making it more efficient for professionals managing different environments. 
Device Redirection – Offers better peripheral support, including printers, USB devices, and local storage, for a more integrated remote experience.

Windows App vs RDP

Copilot version

- [Techradar article - Reinstall Windows 11 every 2 months](#)
- Split drive storage OS C: drive data D: drive
- We're removing the bypassnro.cmd script from the build to enhance security and user experience of Windows 11. This change ensures that all users exit setup with internet connectivity and a Microsoft Account.

Reinstall Windows

- New gamepad keyboard layout for Windows 11
- Xbox controller



- Cannon printer drivers for Windows
CVSS 9.4
Low complexity, lack of user interaction
high impact compromise & confidentiality
Bring your own vulnerable driver
Signed by Microsoft
Period of exploit potential

Current Issues



Hi, I'm Copilot,
your AI companion.

Set up Copilot

Share optional diagnostic data to help
improve Microsoft products



Start Copilot on login to keep it handy



Open Copilot using **Alt+Spacebar** shortcut



Continue

[Privacy](#)

[Terms](#)



Hi, I'm Copilot,
your AI companion.

Set up Copilot

Share optional diagnostic data to help
improve Microsoft products



Start Copilot on login to keep it handy



Open Copilot using **Alt+Spacebar** shortcut



Continue

[Privacy](#)

[Terms](#)

Copilot Update

- Nadella asking the Copilot to "wrap it up by asking or maybe roast giving us each an AI roast?" to which Microsoft's AI-powered assistant says, "Alright, Satya. Let's spice it up."
- Copilot: "Steve, we'll start with you. Your enthusiasm is legendary, but do you ever worry that your energy might short-circuit the AI? I mean, even robots need a coffee break after your pep talks."
- Ballmer replied saying, "Come on, dude. If you can't handle me, you can't handle a huge percentage of the world's population. We're counting on you."
- Fair point, Steve", the Copilot responds and shifts it's attention to Bill Gates. It said, "Now, Bill, you've got that signature thoughtful gaze, but do you ever think the AI might feel intimidated by your intense thinking face? I mean, it's like it's waiting for a blue screen moment".
- Gates countered, "I hope so. I mean, that's all I've got left is these AIs get so damn intelligent. It's just that gaze and my willingness to criticise that differentiates me."

Copilot AI roast Microsoft execs

The Copilot then compliments Gates saying, "And it's a formidable gaze indeed, Bill." On that Steve came up with a witty comeback, "Copilot, would you ever be willing to criticize him?"

- "Absolutely. Criticism is where growth happens", the Copilot answers.
- Lastly, the Copilot asked Nadella a thoughtful question, "Satya, AI seems to be your best buddy. But ever worry that your deep passion for AI could one day have it running the show, leaving you to just enjoy the ride?"

Nadella chose a cricket analogy to support his answer, "Well, the day AI can play like the best cricket player that I enjoy, that's the day it can run the show as far as I'm concerned."

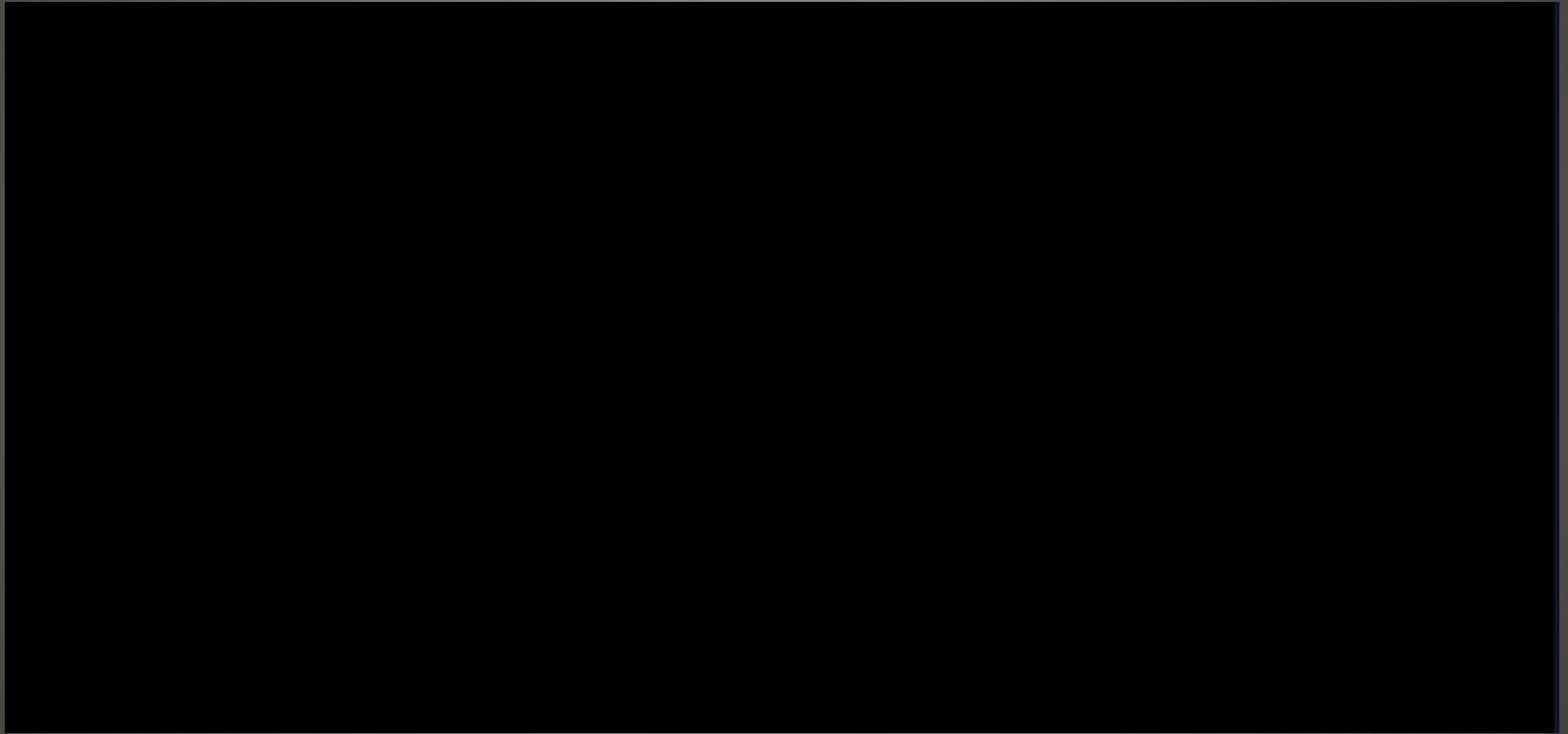
- "Touche, Satya. Let's see if it can hit a century in cricket, and then we'll talk. This has been a blast, gentlemen," the Copilot added.

Copilot AI roast Microsoft execs

- AI event
- Actions (agent), Memory, Vision, Pages, Shopping, Search
- Deep Research
Reliable sources, research document with cites sources
5 Deep Research queries/month
- AI Podcasts
- [Microsoft Blog Copilot Your AI Companion](#)

Copilot

- Browser based, playable level
- “Playing the Model, not playing the game”



Quake II demo

- [15-top-windows-11-tips-everyone-needs-to-know](#)
“This folder should not be deleted regardless of whether Internet Information Services (IIS) is active on the target device.”
- Windows 11 hardware requirements
TPM, Secure boot, 8th generation CPU, resources for AI
- Microsoft Copilot Vision
Sees your screen
Guide use of apps like Photoshop
Was limited to Edge browser
Guide through Minecraft game
- Also AI file search
- Windows Enterprise & Education “hotpatching”
Once-a-quarter cold boot no-reboot-required
Immediate protection, consistent security, minimal disruption

Current Issues

- Microsoft also adds its usual reminder that “on October 14, 2025, Windows 10 will reach end of support. After this date, devices running Windows 10 will no longer receive fixes for known issues, time zone updates, technical support, or monthly security and preview updates containing protection from the latest security threats.”

Current Issues

- Windows 11 24H2 new folder **inetpub**
“This folder should not be deleted regardless of whether Internet Information Services (IIS) is active on the target device.”
- Windows 11 hardware requirements
TPM, Secure boot, 8th generation CPU, resources for AI
- Microsoft Copilot Vision
Sees your screen
Guide use of apps like Photoshop
Was limited to Edge browser
Guide through Minecraft game
- Also AI file search
- Windows Enterprise & Education “hotpatching”
Once-a-quarter cold boot no-reboot-required
Immediate protection, consistent security, minimal disruption

Current Issues

- Windows inetpub folder
April security update
non-admin user create junction point in c:\
Result: blocked security updates
Part of ISS

Current Issues

- Windows April Patch Tuesday error – ignore this error too

Windows PCs might experience error 0x80070643 with an "ERROR_INSTALL_FAILURE" message when attempting to install an update for the Windows Recovery Environment or WinRE."

"this error is observed when the device installs the WinRE update when there is another update in a pending reboot state. Although the error message suggests the update did not complete, the WinRE update is typically applied successfully after the device restarts. Windows Update might continue to display the update as failed until the next daily scan, at which point the update is no longer offered and the failure message is cleared automatically."




Restart

"If you run into Windows Update error code 0x80070643, don't try to fix it because you can't do that."

Current Issues

- Cannon printer drivers for Windows
CVSS 9.4
Low complexity, lack of user interaction
high impact compromise & confidentiality
Bring your own vulnerable driver
Signed by Microsoft
Period of exploit potential

Current Issues

 Account Your info  		
>	2 hours ago	Unsuccessful sign-in
>	2 hours ago	Unsuccessful sign-in
>	Yesterday 10:16 PM	Unsuccessful sign-in
>	Yesterday 10:16 PM	Unsuccessful sign-in
>	Yesterday 8:15 PM	Unsuccessful sign-in
>	Yesterday 8:15 PM	Unsuccessful sign-in
>	Yesterday 6:15 PM	Unsuccessful sign-in
>	Yesterday 6:15 PM	Unsuccessful sign-in
>	Yesterday 4:16 PM	Unsuccessful sign-in
>	Yesterday 4:15 PM	Unsuccessful sign-in
>	Yesterday 2:18 PM	Unsuccessful sign-in
>	Yesterday 2:18 PM	Unsuccessful sign-in
>	Yesterday 2:15 PM	Unsuccessful sign-in
>	Yesterday 12:16 PM	Unsuccessful sign-in

Microsoft Account Login Activity

Security



Change password
Last update: 9/11/2015

Microsoft helps you stay protected online

How you sign in, the devices you're signed into, and the files you save to the cloud are all important pieces to your account's online security.



Account

Strengthen sign-in options beyond a strong password

[Manage how I sign in](#)

Never lose access to your account

Make sure you (and only you) can always get into your account with increased security options like two-step verification and a backup email or phone number.



[Manage how I sign in](#)

[View my sign-in activity](#)

Microsoft Account Login Activity

- Microsoft has introduced the Windows 365 Link, a compact mini PC designed for businesses and enterprise users. This device connects directly to the Windows 365 cloud service, offering a seamless cloud-based computing experience. Key features include:
- Compact Design: Measuring just 4.72 x 4.72 x 1.18 inches, it's highly portable.
- Cloud-Based Operation: Boots in seconds and provides access to Windows 11 via the cloud.
- Connectivity: Equipped with USB-A, USB-C, HDMI, DisplayPort, Ethernet, Wi-Fi 6E, and Bluetooth 5.3.
- Security: Includes features like secure boot, BitLocker encryption, and TPM 2.0.
- Energy Efficiency: Made with recycled materials and ENERGY STAR-certified.
- Priced at \$349.99, it's available in select markets, including the US, UK, Canada, and Japan

Microsoft 365 Link



Microsoft 365 Link

- eMail *spray-and-pray*

Security issues, volume issues, ...

Microsoft new security rules May 5 [email authentication](#)
outlook.com, Hotmail.com, live.com

- SPF: Must pass for the sending domain, and your domain's DNS record should accurately list authorized IP addresses/hosts.
- DKIM: Must pass to validate email integrity and authenticity.
- DMARC: Must ensure, at least, p=none is in the configuration as well as aligning with SPF or DKIM, and preferably both.
- Reduce likelihood of spam & spoofing
- More than 5,000 emails per day
- Non-compliant messages routed to junk
- Legitimate senders gain stronger brand protections & deliverability

Microsoft Outlook security change

- Five obscure Windows tools [article](#)
Live Captions – hearing impaired
Windows Sandbox – light weight Virtual Windows instance
Phone Link – Android and iPhone
Virtual Desktops – productivity
Dynamic Lock – security feature

- Windows 24H2 updates fail with 0x80240069 error

"Devices which have installed the April Windows monthly security update, released April 8, 2025, or later (starting with KB5055528) might be unable to update to Windows 11 24H2 via Windows Server Update Services (WSUS)," Microsoft says in a Windows release health update.

- Microsoft 365 Copilot Wave 2 Spring Release
 - AI agent digital colleagues
 - perform workplace tasks with reasoning capabilities
 - Researcher*
 - Analyst*
 - Agent Store
 - Copilot is browser for AI world
 - Copilot Notebooks
 - Capacity Gap Burnout & Interruptions
 - Employees as Agent Boss

- **Microsoft:**

"AI has started to lower the technical bar for fraud and cybercrime actors looking for their own productivity tools, making it easier and cheaper to generate believable content for cyberattacks at an increasingly rapid rate... AI-powered fraud attacks are happening globally."

- Microsoft Recall feature on Copilot Plus PC
improved AI Windows search Click to Do
- Microsoft Recall back - Opt in as default

YEAHBUT if anyone uses Recall ...

- ActiveX to be blocked by default in Microsoft 365
1996 Interactive Content

"ActiveX is a powerful technology that enables rich interactions within Microsoft 365 applications, but its deep access to system resources also increases security risks.

- Windows NT LAN Manager (NTLM) flow exploited
Patch March 11, 2025
- Microsoft Secure Future Initiative [report](#)
28 objectives 5 completes 11 with significant progress

Current Issues

- Passwords disappearing from Microsoft Accounts
- Password spraying for Microsoft accounts greatly increasing
- Microsoft Authenticator app will stop storing passwords June 1
- Streamline password autofill process
- Passwords removed yet passkeys will not
- DO NOT REMOVE Authenticator -> passkeys will be removed
- Microsoft Authenticator -> Microsoft Edge browser
- “passwordless by default” new accounts
- Passkeys in Microsoft Authenticator app
- Creation of public/private key pair
- Public key to account service
- Private key to phone, computer, YubiKey, or similar
- Account service sends unique challenge
Challenge signed by private key and sent back to account service
Account service used public key to validate user

Microsoft & Passwords

Windows Sandbox is a lightweight, isolated desktop environment designed for safely running applications. It is ideal for testing, debugging, exploring unknown files, and experimenting with tools. Applications installed within the sandbox remain isolated from the host machine using hypervisor-based virtualization. As a disposable virtual machine (VM), Windows Sandbox

provides quick launch times and a lower memory footprint compared to full VMs.

Windows 10 and 11 Pro

Part of Windows: Everything required for this feature is included in supported Windows

editions like Pro, Enterprise, and Education. There's no need to maintain a separate VM installation.

- Disposable: Nothing persists on the device. Everything is discarded when the user closes the application.
- Pristine: Every time Windows Sandbox runs, it's as clean as a brand-new installation of Windows.
- Secure: Uses hardware-based virtualization for kernel isolation. It relies on the Microsoft hypervisor to run a separate kernel that isolates Windows Sandbox from the host.
- Efficient: Takes a few seconds to launch, supports virtual GPU, and has smart memory management that optimizes memory footprint

Microsoft Windows Sandbox

- NO Windows Defender
- Introduced Windows 10 version 1903 (2018)
- Utilizes host OS
thus host OS compromise – Sandbox compromise
- Or
 - ✓ enable Sandbox
 - ✓ restarts system via task scheduler
 - ✓ hides Sandbox
 - ✓ Using different account
 - ✓ Drop malware on infected host
 - ✓ Share access to the host file in the sandbox
 - ✓ Malware executed in Sandbox (No Defender)
 - ✓ Opens backdoor
 - ✓ Access host files via sandbox without ANY logging
- More Sandbox features -> More malware abuse
- Default-enabled clipboard Severe Abuse
- Sandbox signed by Microsoft

Microsoft Windows Sandbox

- Windows 11 enhancements
 - Background execution – lack of user awareness
 - Execution without WSB file – command line arguments
 - Persistent data in Sandbox
- Disable Intel Virtualization in BIOS
- YOUR Vendor will vary

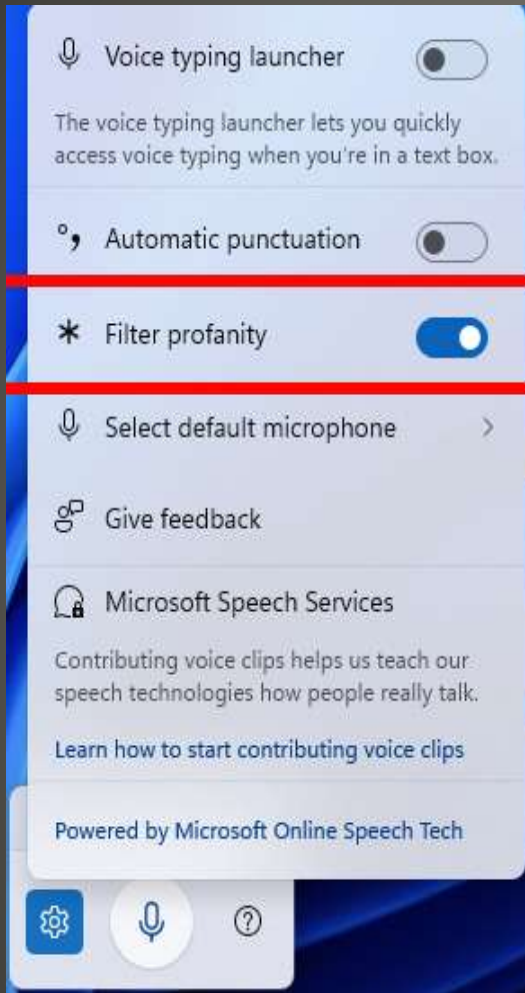
Microsoft Windows Sandbox

- CISA Known Exploited Vulnerabilities Catalog
CVE-2025-24054
NTLM credential stealer
Fixed
- Improper access control in Windows Cross Device Service allows an authorized attacker to elevate privileges locally.
CVE-2025-2476
Feature to use phone camera as webcam
Just 300 milliseconds -> no more than 300 milliseconds
Fixed

Current Issues

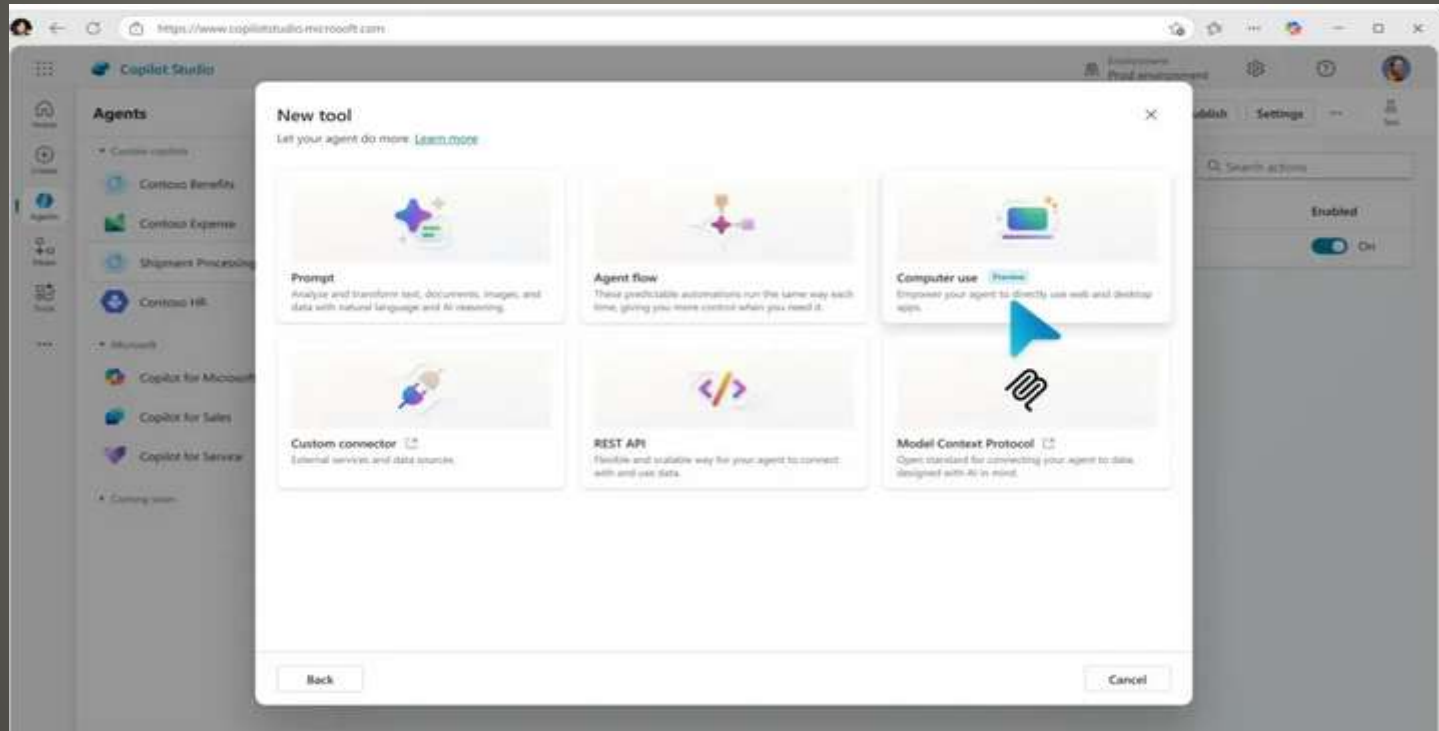
- Microsoft “the future of work”
Hybrid work
Upskilling
Agent Bosses
- Microsoft Windows 24H2 preview KB5055627
Bug fixes
Features:
Recall (preview) Copilot+ PCs
Click to Do (preview) Copilot+ PCs
Improved Windows search Copilot+ PCs
Narrator speech recap, copy, follow along
Phone Link functions from Start menu
File Explorer – pivot based curated views File Explore Home

Current Issues



Current Issues

- Microsoft Copilot Studio Ai agent interact with web & apps
OpenAI Operator
Claude *computer use*
click buttons, select menus, typing into fields



Current Issues

New tool



Let your agent do more. [Learn more](#)



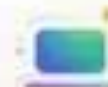
Prompt

Analyze and transform text, documents, images, and data with natural language and AI reasoning.



Agent flow

These predictable automations run the same way each time, giving you more control when you need it.



Computer use

Preview

Empower your agent to directly use web and desktop apps.



Custom connector

External services and data sources.



REST API

Flexible and scalable way for your agent to connect with and use data.



Model Context Protocol

Open standard for connecting your agent to data designed with AI in mind.

Back

Cancel

- Microsoft Copilot Vision
 - Sees your screen
 - Guide use of apps like Photoshop
 - Was limited to Edge browser
 - Guide through Minecraft game
- Also AI file search

Current Issues



Sophisticated Phishing Windows

- WEB site “locked” “frozen”
 - Hosted on Windows.net (Open platform for Azure apps)
 - Exploited hosting services – Windows.net
 - Randomized rapidly changing subdomains
 - Well designed
 - Anti-bot & CAPTCHA
 - Microsoft ant-scareware in Edge browser
-
- Thus the move to MAC
 - MAC page layout and design
 - Code adjustments
 - Still using windows.net & subdomains
 - MAC users now prime targets

Sophisticated Phishing campaign

Recall

Type here to search your history

< Oct 18

Oct 19

Oct 20

Oct 21

Today

Now

11:45 AM
PowerPoint

Enhance
Your Decor

About Us

Shop

Contact

NEW IN

Grace in Every Drop

Discover the pure elegance of nature with SKN. Our beauty products are crafted from the finest natural ingredients, designed to nourish and enhance your skin with every application. Each drop of Niva encapsulates the essence of grace, offering a luxurious experience that leaves you feeling refreshed, radiant, and truly beautiful.

SHOP

glance

Wellness Glance

Today at 10:30 AM

BTF
unny

Search

11:10/22

←

All

Apps

Documents

Web

Settings

Folders

Photos


▶

🔍

👤

⋮

Best match




Family_Farming_Presentation

Microsoft PowerPoint Presentation


Last modified: 10/12/2024, 11:32 AM

Web (20+)




Beginner Guide Vancouver

>



August hiking pictures


>



September hiking plans


>

Local Documents (2)



July_hiking_schedule_template


>




Beginner Guide Vancouver

>


Images (2)



IMG_1938




IMG_4967



Family_Farming_Presentation

Microsoft PowerPoint Presentation



Location


[C:\Users\madisonbutler\Documents](#)

Last modified


10/12/2024, 11:32 AM

Relevance


Content related to "mountains" found.



Open



Open file location




Copy path

Abstract Blue and White Swirls by Jada Jordan

File | C:\Users\OneDrive\Arthistorycollection\art-object-page-164942.pdf

Draw | Ask Copilot | 1 of 1 | Edit with Acrobat



This captivating piece of art draws viewers into a mesmerizing dance of fluid motion and organic forms. Titled "Abstract Blue and White Swirls," the painting features a swirling blend of blue and white hues, creating a sense of depth and movement that seems almost tangible. The contrast sharply with the lighter blue sections, giving the impression of an almost turbulent flow. The texture is varied, with some areas appearing more textured, adding to the complexity and intrigue of the piece.

The abstract nature of this painting invites multiple interpretations. Some might see it as a representation of natural elements, such as water or clouds, while others might interpret it as an emotional or psychological landscape. The lack of defined shapes and the fluidity of the forms encourage viewers to engage on a personal level, finding their own meaning and connection within the swirls and patterns.

Abstract Blue and White Swirls
New York, NY

Summarize

"Abstract Blue and White Swirls" is a captivating painting that features a dynamic blend of blue and white hues. The darker and lighter areas contrast sharply, creating a sense of depth and movement. The rich, varied textures add to the piece's complexity and intrigue.

Copy

Why is TPM so important in Windows 11?

Windows 11 takes security seriously, and TPM is one of its cornerstones. Here's why it matters:

- ***Protects your data:*** TPM can encrypt your data, making it difficult for hackers to access sensitive information. This is especially critical for things like personal details, financial data, and confidential files.
- ***Ensures trusted software:*** TPM verifies the integrity of your system's software and firmware. This feature, called secure boot, helps stop malicious software from launching during startup.
- ***Guards against physical tampering:*** If someone tries to physically tamper with your device's hardware, TPM can detect changes and prevent your system from booting, keeping your device secure from physical attacks.
- ***Supports advanced security features:*** Many of Windows 11's most powerful security features rely on TPM. These tools help keep your data safe, even if your device is lost or stolen.

TPM Trusted Platform Module



Sweepstakes

Microsoft Rewards

\$ **2000000** USD

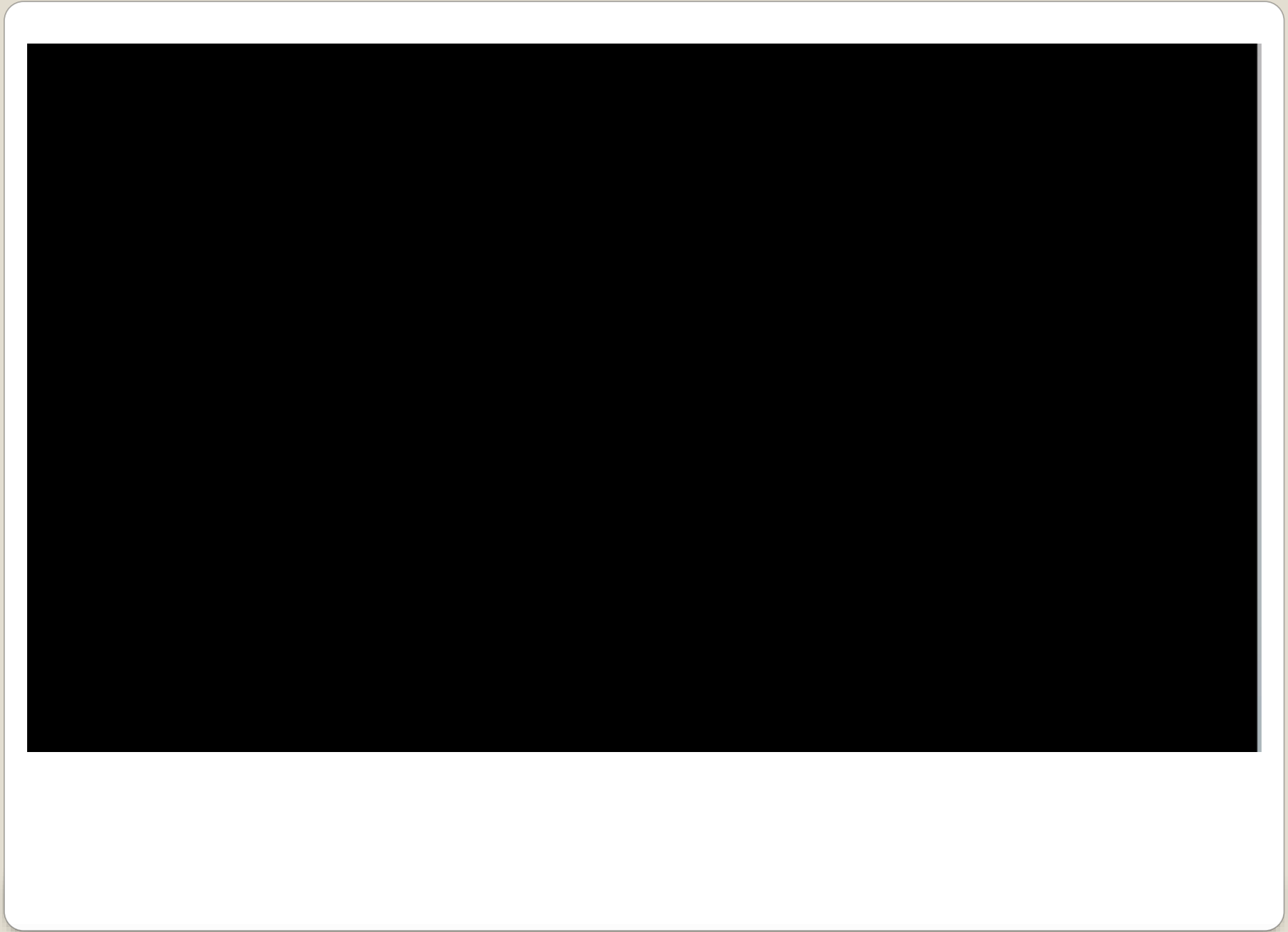
One Million Dollar Grand Prize & 100 Winners

**Claim your 5 entries for a
chance to win \$1 Million USD**

Congratulations, Microsoft Rewards member! By spending \$25 or more at Microsoft Store, you've earned 5 entries towards the grand prize of \$1 million USD¹. Well done on activating your Microsoft Rewards membership.

- Copilot+ PCs
- On device AI
- Understand your intent
- With permission – automate & execute task(s)

AI Agents to change Windows Settings



- [What to know about Copilot - CNET Article](#)
- Chatbot, Image generator, sidebar assistant
- More and more embedded in Microsoft ecosystem
- Available on iOS & Android
- ChatGPT-4o Dall-E 3 Prometheus

- Updates to Updates

Copilot

- Microsoft to cut 3% of its workforce
Dynamic marketplace
FY25 Q3 \$70.1 B revenue
\$25.8B net income

Current Issues

- None of us are as experienced as all of us
 - Awareness, Preparedness, Understanding
 - Participate
 - Topic Suggestions
 - Questions: scccwindows@gmail.com
- 