

East SIG Report – September 2024

After welcoming members to the September meeting of East SIG, host Frank Maher outlined the nights agenda below:

Presentation 1: **Q&A** by George Skarbek

Presentation 2: **WinToys for Windows 10 and 11** by Frank Maher

Presentation 3: **Gemini and Copilot compared** by Frank Maher

Presentation 4: **Why you should consider stop using Google Search** by Trevor Hudson

Presentation 5: **Why Am I Using So Much Bandwidth** by Dave Botherway

Presentation 6: **Finding and Using the EAST Website** by Frank Maher

Presentation 7: **Fake Windows Updates** by Dave Botherway

Q&A

by George Skarbek

Q1: I've been told my 4-year-old Nokia phone is being discontinued because it's not running 4G. But when I look at the network settings it says I'm on 4G. Has anyone else come across this?

A1: 4G will be around for a long time. It's 3G that is being switched off.

[Stuart Gruneklee] Your phone may be on 4G, but your phones VOIP may be on 3G. Telstra and Optus network users can text the number "3" to "3498" to check if their device will function after the 3G shutdown. You will get a response that your phone is okay or not

[Dave Botherway] I was getting messages from Optus that my ZTE phone would not work on 4G. The specs however show the phone would work on 4G. I visited the tech support at an Optus store and was told there are some frequencies Optus is not supporting in the 4G domain. For that reason, while my phone will work in 4G, that particular frequency if needed, is not available.

[Richard Bradford] When 4G was first introduced, there were multiple versions because the specifications had not yet been finalized. You might have an early version of a phone with 4G that doesn't have the current specifications. Different countries also have differing 4G specifications.

[Alan Wiseman] My understanding is your phone must support VoLTE (Voice over LTE) emergency calling to make an emergency call to 000, after the 3G network closes. If your phone doesn't support VoLTE emergency calling, you will not be able to make emergency calls to 000.



Figure 1 – 3G Shutdown

[George] If you can manage without a phone for a few days, I recommend buying a reconditioned Android or iOS phone, that's 2 or 3 generations old. For example, while the latest Samsung model is the S24, going back to the S23 or S22 can still get you an excellent phone. These models were top of the line when released but have since been superseded, making them much more affordable. By searching for reconditioned versions of these devices, you could pay a fraction of their original price, sometimes just a quarter of what they cost 2 or 3 years ago.

The last phone I bought was a reconditioned Android phone. The condition rating of the phones searched were shown as “fair”, “good”, or “excellent”. The price difference between “fair” and “excellent” was around \$100. I chose the “good” condition, and when it arrived, it looked immaculate, like a brand-new phone straight from the shop. That was a few years ago, and it's still working perfectly. Instead of paying around \$1,100 for a new phone, you might pay closer to \$400 for a reconditioned one, saving a significant amount of money while still getting a high-quality device.

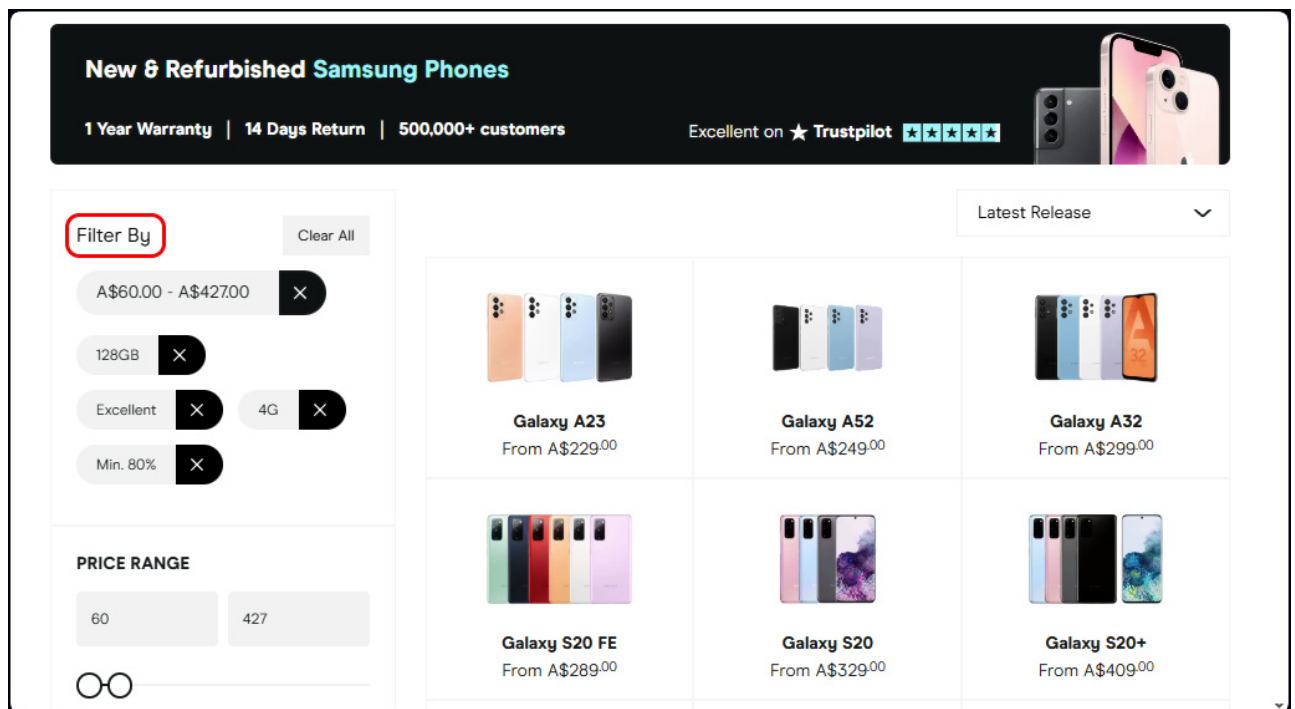


Figure 2 – Search results for Refurbished Samsung phones

Q2: The reason many people buy new phones is because the batteries deteriorate over the years. Do the reconditioned phones have new batteries?

A2. No, they don't have new batteries. My batteries in my previous reconditioned phone lasted 5 years before it suddenly started overheating. You may need to charge a reconditioned phone daily, rather than every 3 to 4 days, but it still should give you 5 years use.

Q3. In Firefox I get messages to make chrome the default browser. Is there a way to turn off that message?

A3. [Richard Bradford] Buried in the Firefox Settings you will find a setting to make Firefox your default browser. Turn that on and you won't get that message anymore.

Q4. What precautions do you take in periods of thunder and lightning?

A4. None, because for the last 15 plus years, I've had a UPS (Uninterruptible Power Supply) connected to my computer. I have updated models over that time. A UPS will keep the computer going for 20 minutes, enough time to save any work and shut down the computer properly. If lightning strikes, it can cause severe electrical surges that may damage the fuse box and other electrical components. While a UPS (Uninterruptible Power Supply) should absorb the power surge, the computer will most likely not be harmed.

If the power goes out, or someone pulls out the plug while saving or updating a file on a desktop computer, a number of things can happen:

1. **File Corruption:** If the file is being actively written or updated when the power is cut, it may become corrupted. Parts of the file could be incomplete or damaged, making it unreadable or unusable when you try to open it later.
2. **Loss of Unsaved Data:** Any unsaved work will be lost. If the power is interrupted before the changes are fully written to the hard drive, your work may not be recoverable.
3. **Operating System Instability:** If the system was updating critical files or the operating system itself at the time of the power cut, it could cause larger issues. In some cases, this may lead to system crashes, boot failures, or needing a repair or reinstall of the operating system.
4. **Hard Drive Damage:** Repeated sudden power loss can increase the wear and tear on your hard drive, particularly if it's a traditional spinning hard drive (HDD). For solid-state drives (SSD), the risk is lower but still possible over time.

UPS's are not expensive at \$120 to \$130. Using an uninterruptible power supply can help protect your data from sudden power cuts, giving you enough time to properly save your files and shut down the system safely.

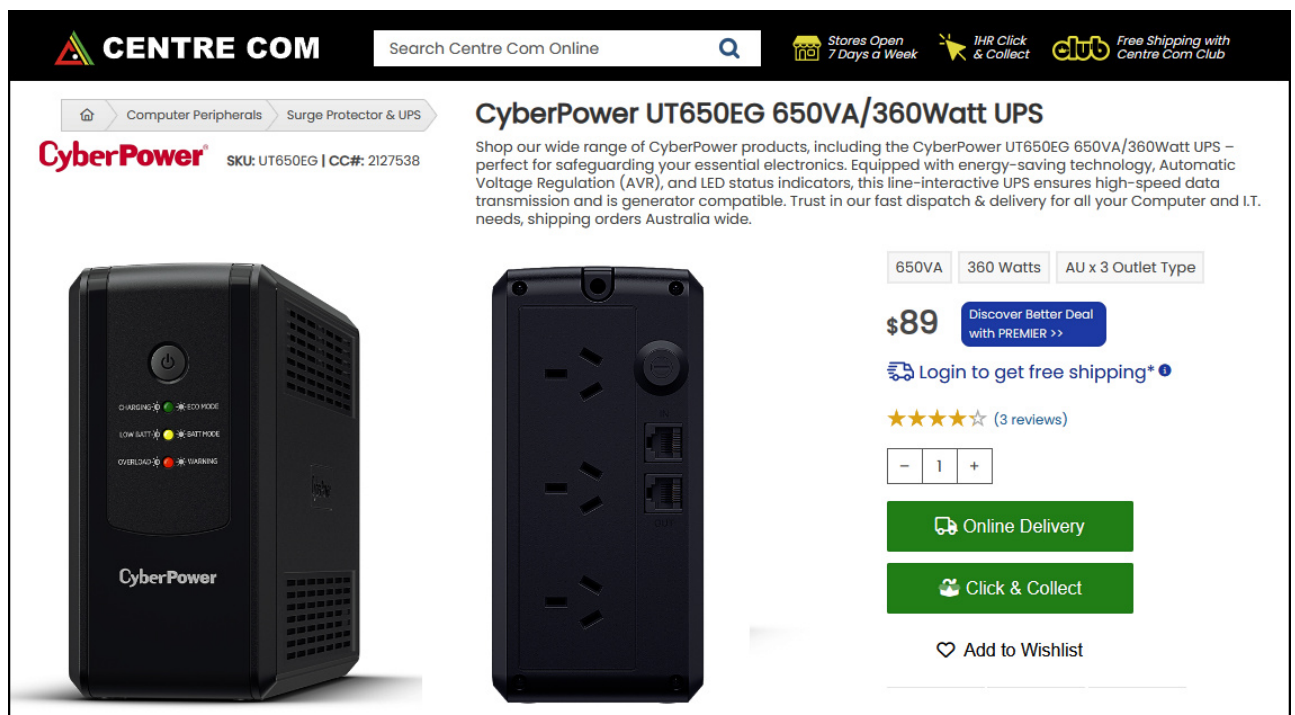


Figure 3 – Budget CyberPower UPS

WinToys for Windows 10 and 11

by Frank Maher

WinToys is a free utility application available only from the Microsoft Store, offering a range of options to customize and optimize Windows. It's packed with features that give users greater control over how Windows looks and functions.

Frank Maher found the tool to be well-organised, with its clean user-friendly interface, displaying much of the information needed on the home screen (see Figure 4). After using WinToys, Frank noted that it made tweaking Windows much easier than navigating through Settings or the Windows Control Panel, where you need to know exactly what you're doing and where to go.

The app is divided into various categories such as Apps, Services, Boost, Health, and Tweaks, accessible from an icon panel on the left side of the WinToys screen. Frank found it to be a handy little tool for adjusting Windows settings in a much more straightforward way compared to using the traditional Windows Settings.

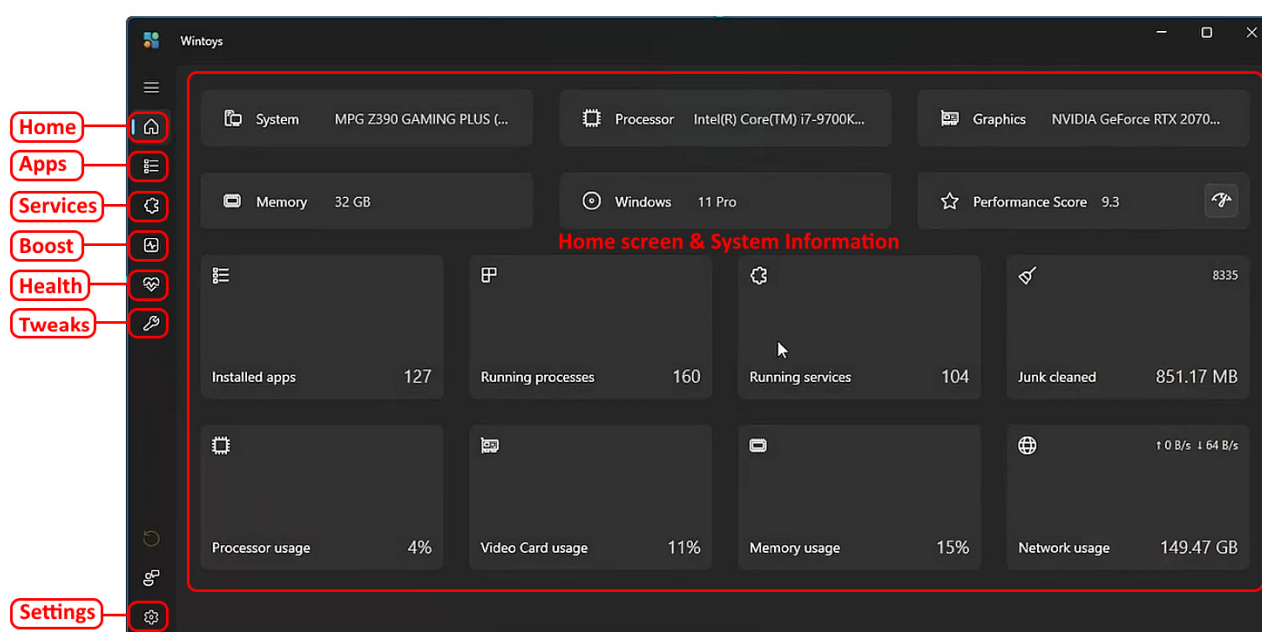


Figure 4 – WinToys Home screen & System Information

To fully explain the features of WinToys, Frank shared the excellent YouTube video by presenter KB titled “WinToys: The Safest Windows PC Optimizer.” The video can be viewed on YouTube at <https://www.youtube.com/watch?v=4JexxBYrMIs>

The **Home** screen in WinToys provides a handy overview of your system information, including the make of your processor, graphics card, RAM and other hardware details. It displays your PC's current memory and network usage, performance scores, the number of installed programs and running processes.

The **Apps** section displays a full list of installed software, which you can sort by name, date or size. This allows users to manage their installed applications, including system apps, that can't usually be removed, such as Microsoft Edge. The tool makes it easy to uninstall unwanted system applications, even those restricted by default.

The **Services** section is a simplified version of Windows Task Manager, which displays running services. It categorises them to help users disable unnecessary ones to optimize performance. You can find out what the services are, by clicking their Description button. In KB's example, 67 unnecessary services were identified.

Next, KB demonstrates the **Boost** feature, which provides various options for improving performance, including enabling the "Ultimate Performance Power Plan." The app recommends specific Windows settings that users can enable or disable, making performance tuning easier for non-experts.

In the **Health** section, WinToys offers tools for optimising Windows, such as managing startup settings and performing Windows repairs if the system crashes or shows blue screens. The Declutter feature helps clean storage as shown in Figure 5.

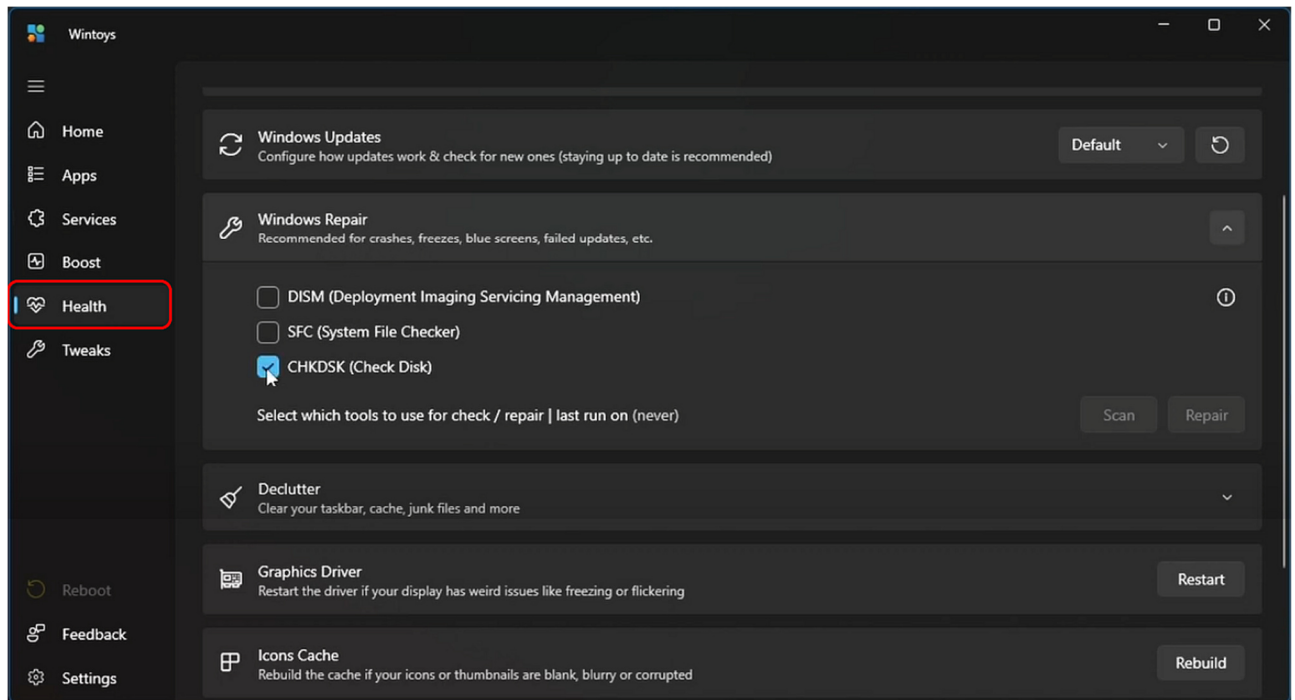


Figure 5 – WinToys Health section

The **Tweaks** section provides privacy and desktop-related settings. Users can disable Bing search in the start menu, extract Spotlight images from the lock screen to save as wallpapers, customize your desktop, Start menu and File Explorer. Windows privacy settings can be adjusted to stop Microsoft spying on you and show personalized ads.

Overall, KB praises WinToys as a safe and effective tool to optimise Windows by recommending changes to system settings. It's easy to use, even for users unfamiliar with manually configuring system settings, and the app's interface is visually appealing.

Gemini and Copilot Compared

by Frank Maher

In this presentation, Frank Maher compared the results of two questions posed to Google's Artificial Intelligence bot, Gemini, and Microsoft's Copilot.

Question 1

Frank recently investigated the upcoming Windows 11 feature update 24H2 by asking two AI tools, Gemini and Microsoft Copilot, about the 10 best new features in the update. To his surprise, the responses were significantly different, with only two features in common: Copilot integration and the Enhanced Taskbar.

Frank found the discrepancies between the two AI-generated lists quite astonishing, leaving him to question the overall significance of the update. He reviewed each of Gemini’s suggested features but found the update “pretty underwhelming” for everyday users like himself. Similarly, after examining Copilot’s top 10 responses, Frank’s initial impression remained unchanged; the update did not seem to offer anything particularly compelling.

The differing answers from Gemini and Copilot suggest that many of the new features in the 24H2 update may be minor tweaks that most users are unlikely to notice or find useful in their day-to-day tasks. Frank’s overall assessment is that, for most users, the update will likely pass by without making any meaningful impact on their Windows experience.

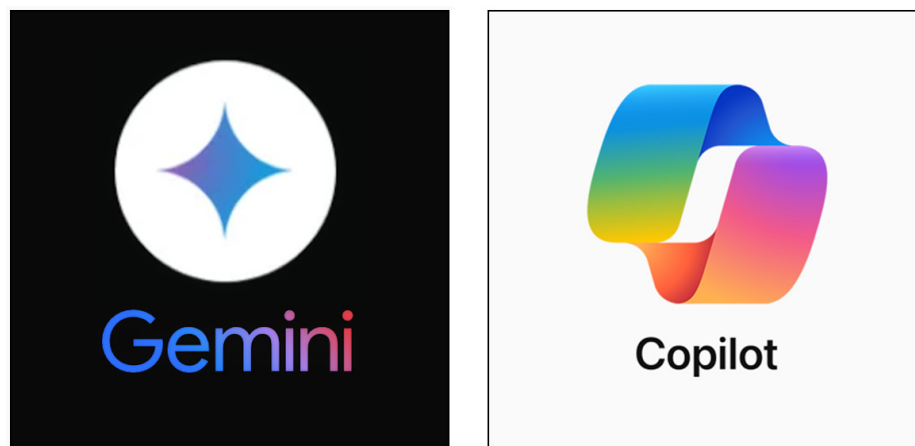


Figure 6 – Google Gemini & Microsoft Copilot compared

Question 2

Following the initial inquiry concerning the new features in the Windows 11 24H2 update, Frank posed a second question to both Gemini and Copilot: “What are the top 10 must-have free programs for Windows 10 and 11?”

This time, the results were slightly closer aligned, with five of the ten recommended programs being common between the two lists. Both Gemini and Copilot recommended VLC Media Player, 7-Zip, Audacity, CCleaner, and LibreOffice, which Frank recognised as good choices for any Windows setup.

Copilot’s additional recommendations included ShareX for screen capture, OBS Studio for video recording and streaming, Kaspersky Security Cloud Free Anti-Virus, Ultimate Windows Tweaker, and Privado VPN Free, the ten selections offering a mix of utility, media, and security options.

Gemini, on the other hand, suggested a different set of programs beyond the shared recommendations, including GIMP for image editing, NotePad++ for coding and advanced text editing, Chrome (or Firefox) for web browsing, Malwarebytes Anti-Malware for additional security, and FileZilla for FTP transfers.

Frank found Gemini’s selection more appealing, as it provided a broader range of functionality and better catered to the needs of everyday users. In his view, Gemini’s list offered a more well-rounded mix of essential free software that would genuinely enhance the Windows experience.

Why you should consider stop using Google Search

YouTube video recommended by Trevor Hudson

In a recent YouTube video, Leo Notenboom shared his decision to stop using Google Search, outlining his reasons and exploring alternatives. Google, once known for delivering the best search results, has undergone a process referred to as "enshitification." This four-stage process involves prioritising user experience at first but eventually sacrificing user satisfaction in favour of profits and advertisers. Leo suggests that Google has entered stages two and three, where users are being exploited by the dominance of paid advertisements over organic search results.

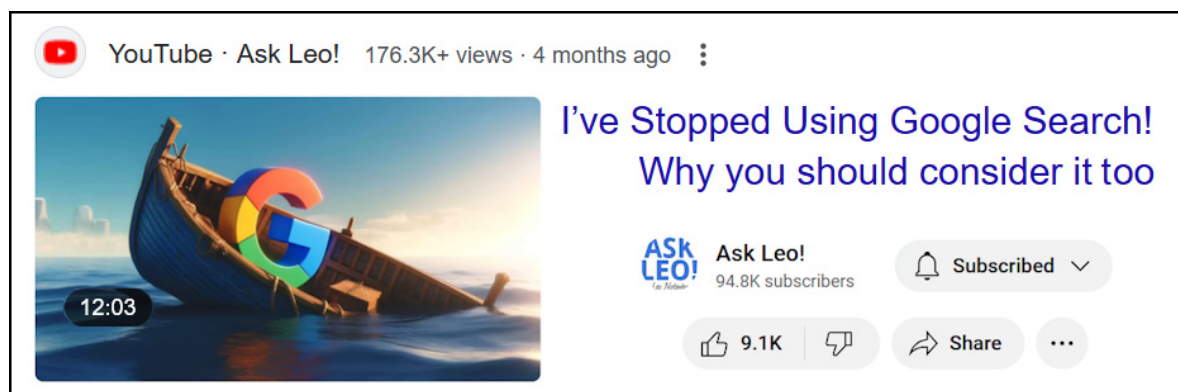


Figure 07 – Ask Leo's YouTube banner

To illustrate this, Leo demonstrates a search for "coffee makers" on Google. The top results are filled with ads, and it takes several scrolls to reach any actual search results. Google has been described as an ad delivery company that occasionally shows search results, misleading users who may not realise they're clicking on paid promotions.

Leo explores alternatives to Google Search, starting with Bing. Though Bing also features ads at the top, it offers fewer of them, and they're more clearly marked. However, Leo resists using Bing because Microsoft aggressively pushes it, often disregarding user preferences for other search engines.

DuckDuckGo is one of Leo's preferred alternatives. While it also includes ads, these are clearly labelled and not based on users' prior behaviour, making it a more privacy-focused option. Leo has made DuckDuckGo his default search engine due to its commitment to privacy.

For those seeking an entirely ad-free experience, Leo recommends Kagi. Kagi operates as a paid service with no ads, offering clear search results without any distractions. Despite sourcing some results from Bing, Kagi delivers them without the clutter of ads, which Leo finds worth the subscription cost.

Leo also briefly mentions other search engines such as Brave, Perplexity AI, Yahoo, and even AOL, highlighting that some may offer unique features or privacy enhancements.

In conclusion, Leo advises users to consider DuckDuckGo for privacy-conscious searching or Kagi for an ad-free experience. Both offer viable alternatives to Google and Bing, which are increasingly dominated by paid ads.

Why Am I Using So Much Bandwidth

by Dave Botherway

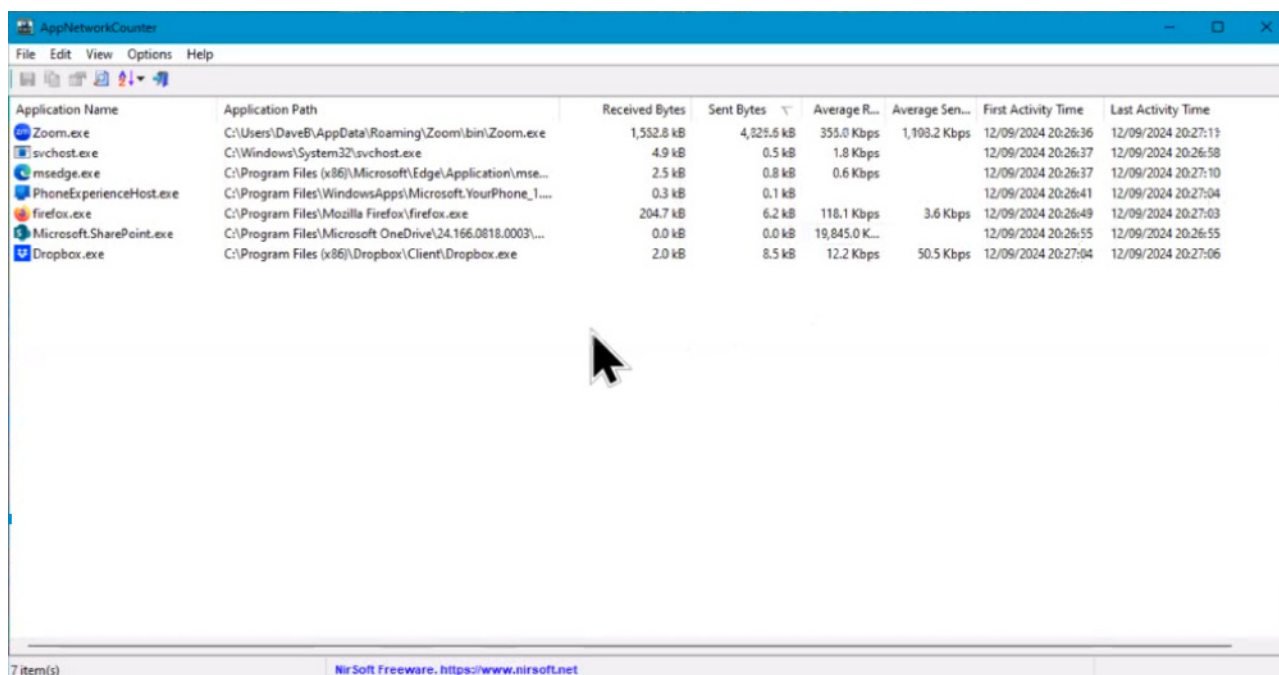
This presentation outlines how Dave Botherway used **AppNetworkCounter** to determine which applications on a fellow resident's computer was causing high bandwidth usage. Dave then provided steps to diagnose and rectify data consumption.

Background

The issue of high bandwidth usage was raised in the retirement village when a resident, limited to a 70GB monthly data plan, received a warning that he had used 50% of his data allowance just one-third into the month. Despite not using his devices excessively, the resident's data usage continued to rise, reaching 75% just two days later. In response, and without a clear answer, the resident upgraded his Telstra broadband plan to 400GB per month to avoid the cost of excess data charges.

Investigation and Demonstration

Dave Botherway, a fellow resident, investigated the issue using a free tool called AppNetworkCounter by NirSoft (<http://www.nirsoft.net>). Dave demonstrated the app live to the audience, showing how it works in real-time with applications such as Zoom and Firefox usage highlighted. The app provides detailed statistics, including Received Bytes, Sent Bytes, First Activity Time and Last Activity Time, which help identify how much data each application is consuming.



Application Name	Application Path	Received Bytes	Sent Bytes	Average R...	Average Sen...	First Activity Time	Last Activity Time
Zoom.exe	C:\Users\DaveB\AppData\Roaming\Zoom\bin\Zoom.exe	1,552.8 kB	4,825.6 kB	355.0 Kbps	1,109.2 Kbps	12/09/2024 20:26:36	12/09/2024 20:27:11
svchost.exe	C:\Windows\System32\svchost.exe	4.9 kB	0.5 kB	1.8 Kbps		12/09/2024 20:26:37	12/09/2024 20:26:58
msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\mse...	2.5 kB	0.8 kB	0.6 Kbps		12/09/2024 20:26:37	12/09/2024 20:27:10
PhoneExperienceHost.exe	C:\Program Files\WindowsApps\Microsoft.YourPhone_1...	0.3 kB	0.1 kB			12/09/2024 20:26:41	12/09/2024 20:27:04
firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe	204.7 kB	6.2 kB	118.1 Kbps	3.6 Kbps	12/09/2024 20:26:49	12/09/2024 20:27:03
Microsoft.SharePoint.exe	C:\Program Files\Microsoft OneDrive\24.166.0818.0003\...	0.0 kB	0.0 kB	19,845.0 K...		12/09/2024 20:26:55	12/09/2024 20:26:55
Dropbox.exe	C:\Program Files (x86)\Dropbox\Client\Dropbox.exe	2.0 kB	8.5 kB	12.2 Kbps	50.5 Kbps	12/09/2024 20:27:04	12/09/2024 20:27:06

Figure 8 - NirSoft AppNetworkCounter

Key Findings

Using AppNetworkCounter on the resident's computer, Dave immediately detected unusual activity, with the main culprit being a process called **svchost**, which was consuming a significant amount of bandwidth. Dave explained that svchost is a Windows service that hosts various essential system processes. Further investigation was needed to determine which specific service was causing the data drain and whether it should be stopped. AppNetworkCounter also highlighted applications that the resident had forgotten he installed, that were contributing to additional data usage.

Solution and Recommendation

Dave identified the problematic applications and adjusted settings to reduce their data consumption. As a result, the resident could revert to his previous 70GB data plan, saving money on his internet costs.

About AppNetworkCounter

AppNetworkCounter is a free lightweight tool from NirSoft, that runs without installation, providing a detailed overview of data usage by individual applications. It displays extensive network traffic data which can be configured with additional columns to suit the user's needs. By right clicking on an application name from the list and selecting Properties, all its network data is displayed giving more in-depth statistics, including the application name and path as highlighted in Figure 9 below. Knowing the path can help trace where data usage is coming from.

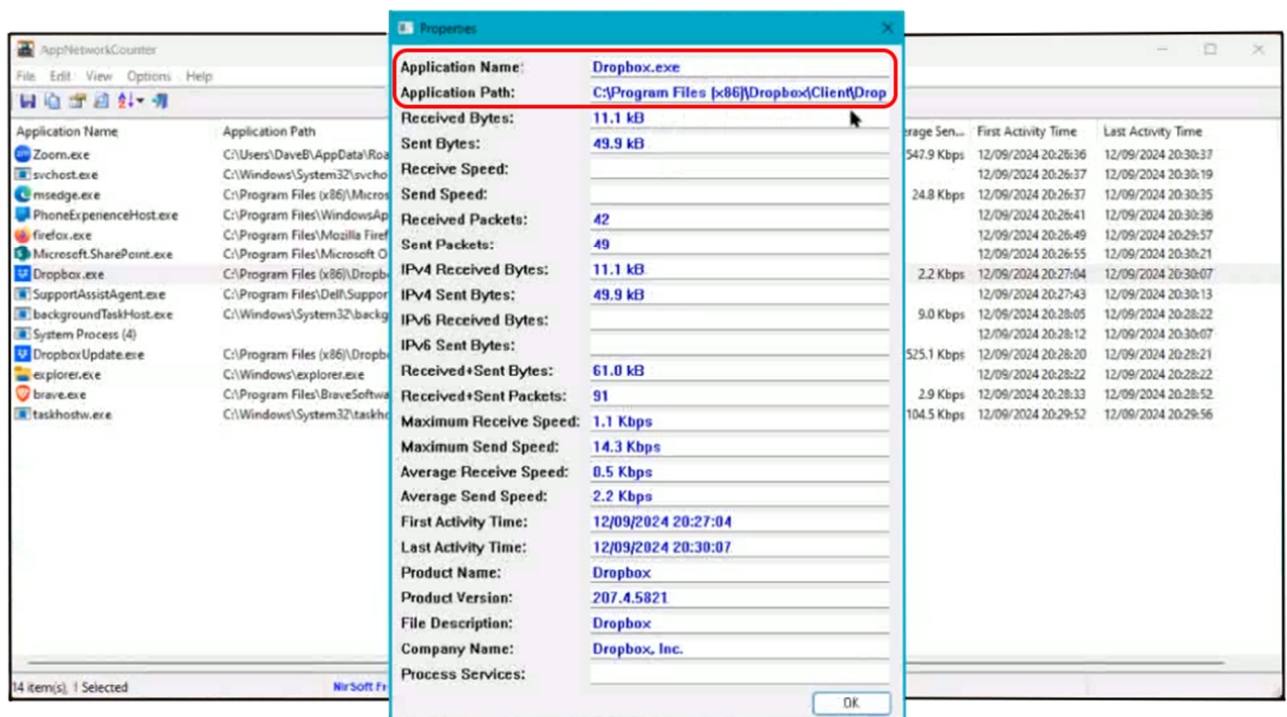


Figure 9 – AppNetworkCounter Properties window

Conclusion

Dave recommended AppNetworkCounter to everyone, highlighting its effectiveness as a network monitoring tool. NirSoft is well known for its reliable freeware support software, and AppNetworkCounter proved to be an invaluable tool in diagnosing and rectifying data usage issues in the case presented, potentially saving the resident money on his broadband plan.

Finding and Using the EAST Website

by Frank Maher

The East SIG website is currently undergoing an upgrade, and in this presentation, Frank Maher guides members through the steps needed to access the East SIG website and the East Group meeting reports. Frank emphasised that the meeting reports are a valuable resource, now being indexed to make finding past presentations much easier.

To access the East SIG website, members must first log in as MelbPC members. The steps for members to log to the MelbPC website are:

1. Goto the Melbourne PC Users group website at www.melbpc.org.au
2. Select “Member Logon” from the top menu.
3. From the drop-down menu select “Member Login” (Figure 10)

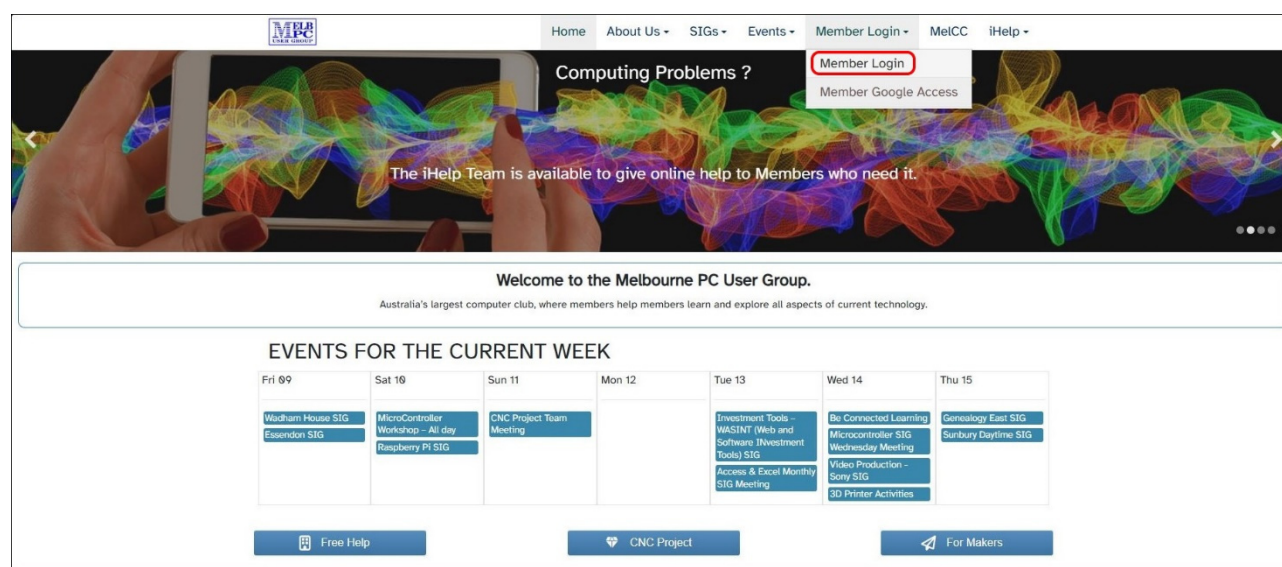


Figure 10 – MelbPC Member Login

4. You will then be directed to a list displaying your various email addresses. Here you select your MelbPC Google Workplace login account. i.e. xxxx@melbpc.org.au
5. Enter your MelbPC password and select “Next”
6. On acceptance of your password, you are returned to the main MelbPC.org.au “Home page”

After logging in as a MelbPC member in step 6 above, the East SIG website is accessed from the MelbPC “Home page” as follows:

1. Select “SIGs” from the main MelbPC menu.
2. From the drop-down menu select “SIG-List – all SIGs Details”
3. From the “SIG – Manage your Subscription” page select “East SIG”
4. From the text box select “Click here for SIG Website” (Figure 11)
5. The East SIG meeting reports can then be accessed from the East SIG menu.

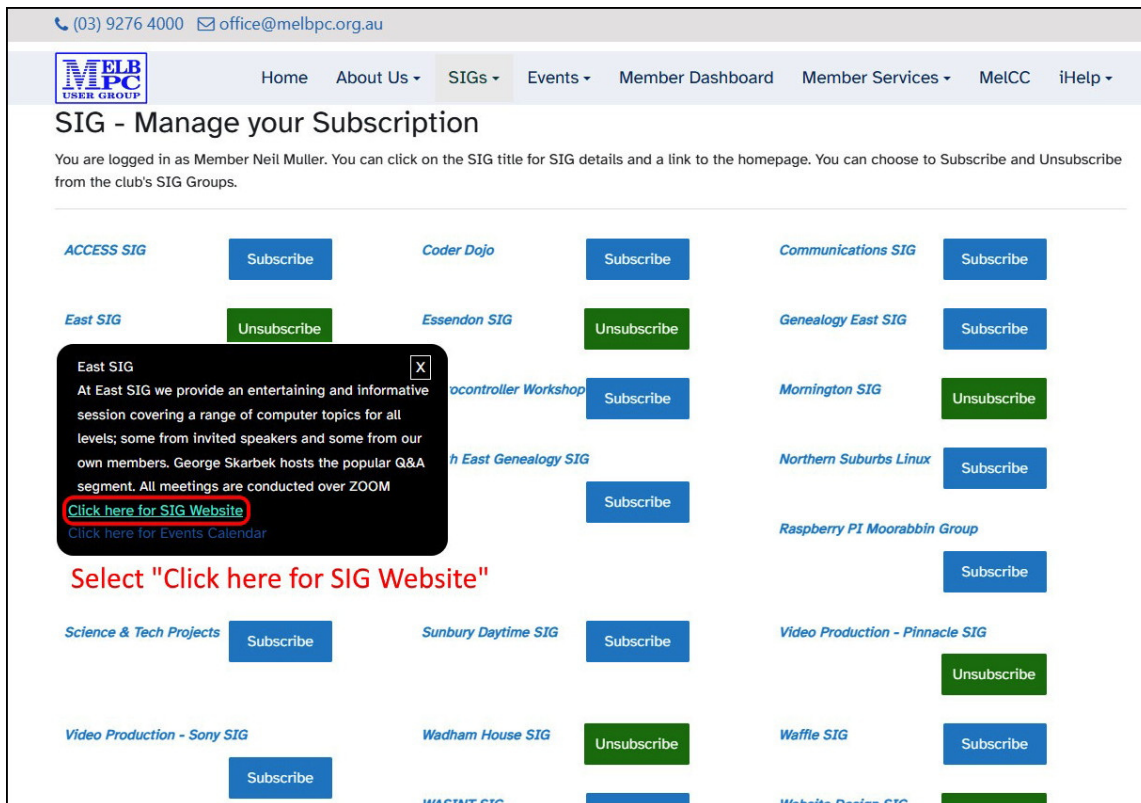


Figure 11– MelbPC Link to East SIG website

After demonstrating how to access the East SIG website, Frank navigated to the "Past Meeting Reports" section from the East SIG home page menu. (Figure 12) He selected "2024" and then clicked on "February" to display the pdf report for the February East SIG meeting. Frank then scrolled through the report, highlighting several of the topics covered.

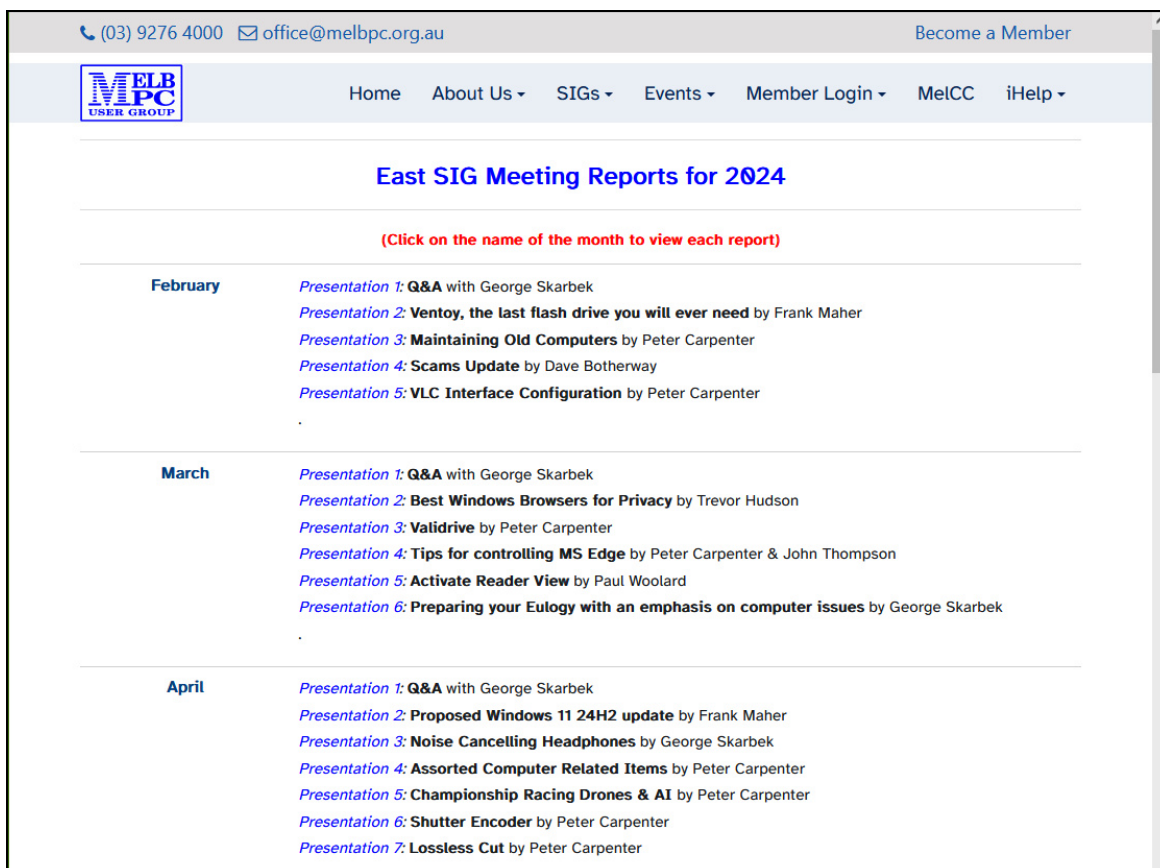


Figure 12 – MelbPC Link to East SIG website

Fake Windows Updates

by Dave Botherway

In this presentation Dave Botherway highlights a growing security threat to Windows users detailed in an article from the MakeUseOf website titled "Scammers are Using Fake Windows Updates to Steal Your Files." Dave summarises how these scams work, how to identify them, and most importantly, how to protect yourself.



Figure 13 – Fake Windows Updates article from the MakeUseOf website

Overview of the Scam

Scammers are increasingly exploiting fake Windows updates to steal personal information and files. The scam typically involves tricking victims into granting remote access to their computers, which allows scammers to display a fake Windows update screen. This process often starts with a simple request to connect via remote access tools, like AnyDesk, TeamViewer or Windows Remote Desktop. Once the scammer gains access, they can execute the fake update, effectively masking their malicious activities while gaining control over the victim's computer.

How the Fake Windows Update Scam Works

- 1. Initial Contact:** Scammers usually initiate contact under a false pretext, such as offering technical support. They may ask to connect using a remote access tool, commonly AnyDesk, TeamViewer, or similar software.
- 2. Establishing Remote Access:** The victim is asked to enter a 10-digit code, specific to their remote access session. This step grants the scammer administrative access to the victim's computer.

- 3. Executing the Scam:** Once connected, the scammer displays a fake Windows update screen. The screen mimics a legitimate update, complete with familiar blue graphics, convincing the victim that their system is undergoing routine maintenance. However, during this time, the scammer is free to access files, install malware, or steal personal information.

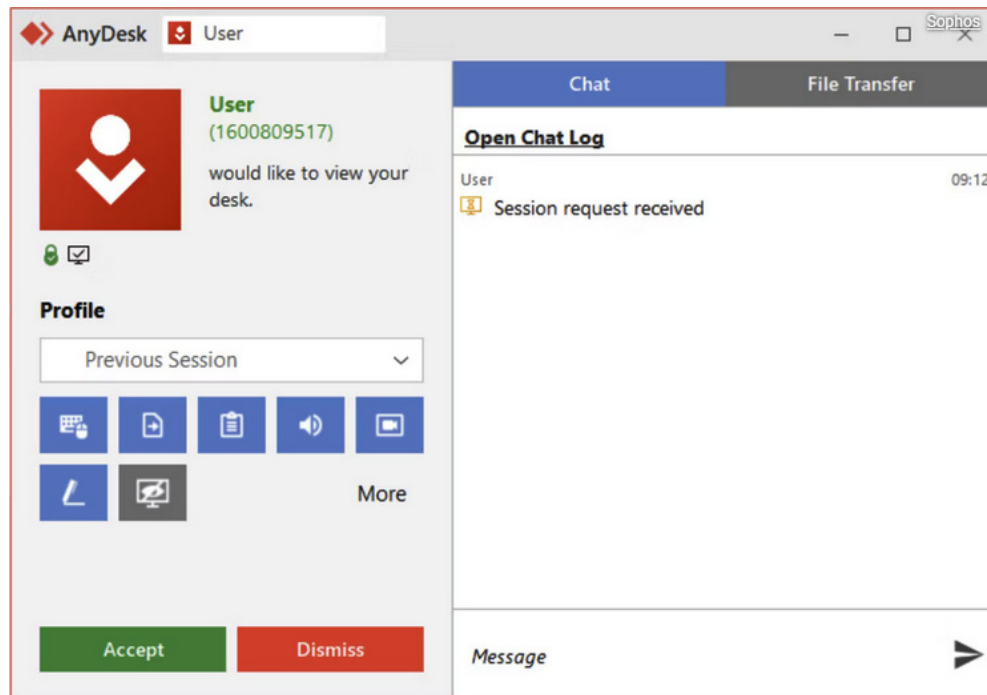


Figure 14 – AnyDesk

Identifying Fake Windows Updates

Dave emphasised the importance of awareness and vigilance. Scammers often choose times when Windows updates are expected or when topical events make users more susceptible, such as during tax season or major holidays. It's crucial to be sceptical of unexpected update screens, especially if someone else has remote access to your computer.

Preventing the Scam

- 1. Do Not Grant Remote Access:** The most effective way to prevent this scam is simply not to allow unknown third parties to access your computer remotely. If someone claims to need access, verify their credentials thoroughly.
- 2. Immediate Action:** If you suspect you've been tricked into granting access, disconnect your internet immediately by unplugging your Ethernet cable or disabling Wi-Fi. This can stop the scammer before they cause further damage.
- 3. Educate Yourself and Others:** Awareness is the best defence. Dave discovered that several village residents had installed remote access software like AnyDesk without realising its potential risks. Regular reminders and educational sessions can help community members stay alert.

Comments from iHelp Team Member Stewart Gruncklee

Stewart, an iHelp team member, explained that although remote access tools are valuable for legitimate support, they pose risks if misused. He emphasised the importance of verifying the identity of anyone offering remote assistance and suggested a cautious approach: wherever possible, talk users through their problems rather than taking control of their computers.

Conclusion and Recommendations

The fake Windows update scam is a reminder of the importance of vigilance in the digital age. Dave Botherway's advice highlights the critical need to avoid giving remote access to strangers, verify the legitimacy of any support claims, and educate ourselves and others about the risks involved. For those needing help, seek trusted sources and always verify the identity of anyone requesting access to your computer. Remember, scammers thrive on gaining your trust and can quickly exploit any opportunity to gain control over your device. Stay alert, and always think twice before granting remote access.

Neil Muller