

# Sun City Computer Club

Cyber Security SIG  
December 5, 2024

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

**Even Now**

- Audio recording of this session as MP4 file
- Audio recording available at link shown above
- Wake Words
- (re)Mute your selves

## 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 replacement
- Take over
- Inclusion Zoom & Recording
- Training, Counsel
- Summers are Important
- Leader(s)???
- Contributors
  - Wayne Kurtz, David Barnes, Tom McBride, Bob Allen

**New Leader???**

- NRO Anti-Fraud Group presentations  
Activities Center Atrium  
3:15 – 4:15  
December 9, December 16  
January 13, January 20, January 27  
February 3, February 10, February 17
- Scams and Computer Safety SIG
- Sun Rays Anti-Fraud Group

- Chrome Version 131.0.6778.109 (Official Build) (64-bit)
  - Edge Version 131.0.2903.70 (Official build) (64-bit)
  - Firefox Version 133.0
  - Safari version 18.1.1 (20619.2.8.11.12)
  - Brave Version 1.73.97 Chromium: 131.0.6778.108
  - Vivaldi Version 7.0.3495.23
  - DuckDuckGo Version 0.94.3
  - Arc Version 131.0.6778.86
  - Tor 14.0.3
- 
- ChromeOS 131.0.6778.96

## Browser Versions

Passwords, Identity, Credentials, Passphrases, Authenticators, Security Keys, Passkeys

All of the above and more are becoming more and more vital to our cyber environments. Yet, a lot is misunderstood. In an attempt to raise awareness of these topics, the Computer Club's Cyber Security SIG held an in-person seminar covering the topics with:

Attendee input and questions

Closed captions

A PDF file of the material

Closed caption ability

The Handouts are at this link:

<https://www.sctexas.org/Files/Library/31008/IDENTITYCREDENTIALSPASSWORDSPASSPHRASE.PDF>

The recorded video:

<https://vimeo.com/940842154?share=copy>

**Rejected Newsletter Article**  
**Can you spot the mistakes?**

- Wi-Fi nearest neighbor attack – across the planet  
Drone on the roof
- Finastra financial services giant data breach  
8,100 financial institutions 400GB
- JPMorgan Chase pays \$40 billion in fines  
Anti-competitive practices, securities abuses, and others
- Thousands of Palo Alto Networks firewalls hijacked  
Use of recently patched security vulnerabilities  
Installed backdoors, crypto mining and other malware
- T-Mobile unsupported phone brands  
4G Band 71 5G N71  
T-Mobile customers informed  
Mint Mobile, US Mobile, Tello, and others not informed
- [New York Times Chinese Telecommunications Hack](#)
- [FBI CISA Joint Communications Infrastructure Guidance](#)

## Current Issues



- Synapse fintech middleman crisis

NOT FICA backed regulations

Yotta, Juno, and others

- Eken video doorbells

Aiwit, Andoe, Bitepass, CutePanda, Eken, Fishbot, Gemee, Guggre, Luckwolf, Rakeblue and Tuck

- Sad Announcement email - with full name of acquaintance

"When you open them you will see why I actually wanted to share them with you today"

"Never thought I would want to share these images with you, anyways here they are"

- Air Fryer(s) Location, recorded audio permissions

- Water systems "high risk vulnerabilities"

And UK-based Thames water "falling apart"

DEF CON Franklin project

- Undersea cable advisory board

15-2000 cable faults per year 3 repairs per week

## Current Issues



- US based data brokers – data Wiesbaden Germany
- Graykey & smartphones iOS 18.1

Before First unlock

Data encrypted PIN REQUIRED Wi-Fi passwords encrypted  
SIM available if not PIN protected No contacts listed  
No iMessage previews

After First unlock most data available (unencrypted)

Law Enforcement & attackers – powered on but isolated  
iCloud access

iOS 18 reboot after 72 hours of inactivity

Springboard then kernel panic

iOS 18 tells other iPhones on lower iOS versions – Reboot  
Wirelessly ??

- CISO professional liability insurance

## Current Issues

- CISA access via web shell from previous CISA engagement
- Proton roadmap

#### Proton Mail

increased security improved SPAM & phishing detection

Language support for Finnish & Hindi

Desktop Proton Mail as mail default app

#### Proton Calendar

More integrated with Proton Mail

Advanced event scheduling

personalized notes for calendar invitations

#### Proton Drive

macOS app, public docs & folders, enhanced organizational tools

## Current Issues

- QNAP firmware update locks NAS access from customers
- Blue Yonder suffering ransomware attack  
Supply chain management for thousands of companies  
Starbucks, Morrisons  
5 or so per 2011  
20-25 major ones per day
- Matrix threat actor  
Botnet cameras, video recorders, routers  
Multiple vulnerabilities & tools from Internet hacking forums  
35 million world-wide admin:admin root:camera  
di-it-all-yourself cyberattack
- Department of Homeland Security programs  
SMARTLink Intensive Supervision Appearance Program
- 0-click 0-day vulnerabilities  
Firefox, Tor, October 9 Windows November 12

## Current Issues

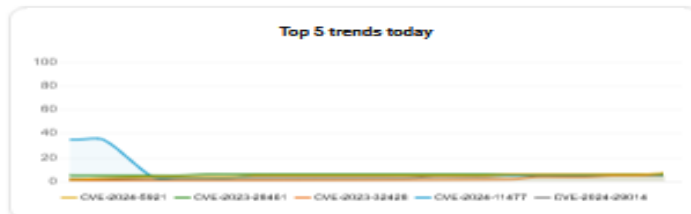
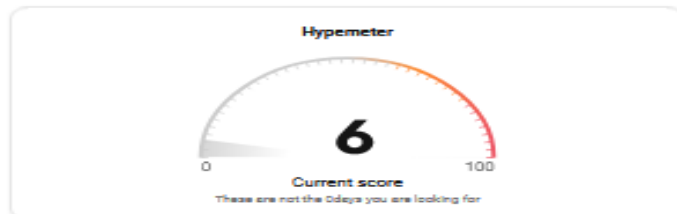
- Intruder - attack surface management
- Intel
- Tracks trending CVEs

**Intel**

# CVE Trends Beta

Updated 38 minutes ago

## At a glance



## Trending

Top 10 CVEs trending on social media within the last 24 hours.

| Trending   | Hyper score (H) | Published    | Description  | Last 24 hours |
|--|-----------------|--------------|--|---------------|
| 1 <a href="#">CVE-2024-5921</a><br>High 7.1                        | 10° 6           | Nov 27, 2024 | An insufficient certification validation issue in the Palo Alto Networks GlobalProtect app enables attackers to connect the GlobalProtect app to arbitrary servers. This can enable a local non-administrative operating system user or an attacker on the same subnet to install malicious root.          |               |
| 2 <a href="#">CVE-2023-28461</a><br>Critical 9.8 · Exploit known   | 10° 5           | Mar 15, 2023 | Armit Networks Armit AG Series and vAG (9.4.0.081 and earlier) allow remote code execution. An attacker can browse the filesystem on the SSL VPN gateway using a flags attribute in an HTTP header without authentication. The product could then be exploited through a vulnerable URL. The               |               |
| 3 <a href="#">CVE-2023-32428</a><br>High 7.8                       | 10° 5           | Sep 6, 2023  | This issue was addressed with improved file handling. This issue is fixed in macOS Ventura 12.4, iOS 16.5, iOS 16.5 and iPadOS 16.5, watchOS 9.5. An app may be able to gain root privileges.  |               |
| 4 <a href="#">CVE-2024-11477</a><br>High 7.8                       | 10° 4           | Nov 22, 2024 | 7-Zip Extended Decompression Integer Underflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of 7-Zip. Interaction with this library is required to exploit this vulnerability but attack vectors may vary.          |               |
| 5 <a href="#">CVE-2024-29014</a><br>High 8.8                       | 10° 4           | Jul 18, 2024 | Vulnerability in SonicWall SNA100 NetExtender Windows (32 and 64-bit) client 10.2.339 and earlier versions allows an attacker to arbitrary code execution when processing an SPC Client update.  |               |
| 6 <a href="#">CVE-2024-10542</a><br>Critical 9.8                   | 10° 3           | Nov 26, 2024 | The Spam protection, Anti-Spam, Firewall by CleanTalk plugin for WordPress is vulnerable to unauthorised Arbitrary Plugin Installation due to an authorization bypass via reverse DNS spoofing on the checkWithoutToken function in all versions up to, and including, 6.62.2. This makes it               |               |
| 7 <a href="#">CVE-2024-10781</a><br>High 8.1                       | 10° 3           | Nov 26, 2024 | The Spam protection, Anti-Spam, Firewall by CleanTalk plugin for WordPress is vulnerable to unauthorised Arbitrary Plugin Installation due to a missing empty value check on the 'getLkey' value in the 'perform' function in all versions up to, and including, 6.66. This makes it possible for          |               |
| 8 <a href="#">CVE-2024-53844</a><br>Medium 5.3                     | 10° 3           | Nov 26, 2024 | E.O.D.I (Enhanced Dialog Driven Interface) is a middleware to connect and manage LLM API bots. A path traversal vulnerability exists in the backup export functionality of EODI, as implemented in 'RestExportService.java'. This vulnerability allows an attacker to access sensitive files on the server |               |
| 9 <a href="#">CVE-2024-53930</a><br>Medium 5.6                     | 10° 2           | Nov 25, 2024 | WildDocs before 1.0.85 allows stored XSS by authenticated users via data that comes after \$\$\$, which is mishandled by a KeTeX parser.   |               |
| 10 <a href="#">CVE-2024-0012</a><br>Critical 9.3 · Exploit known · | 10° 1           | Nov 18, 2024 | An authentication bypass in Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to gain PAN-OS administrator privileges to perform administrative actions, tamper with the configuration, or exploit other                          |               |



## Checkout



**Wireless Headphones**

|              |                 |
|--------------|-----------------|
| Subtotal     | \$94.99         |
| Tax          | \$6.65          |
| <b>Total</b> | <b>\$101.64</b> |



## Checkout



**Wireless Headphones**

|              |                 |
|--------------|-----------------|
| Subtotal     | \$94.99         |
| Tax          | \$6.65          |
| <b>Total</b> | <b>\$101.64</b> |

**paze**

**Paze**

# Your eligible cards

## My Card

\*\*\*\* 1234



Add to cart



**ready to use**

07/27



# Paze



No  
No  
**No**  
No  
No  
No

manual card



**Paze**

No

No

No

No

No

usernames or passwords<sup>+</sup>



Paze

No

No

No

No

No

downloading other apps



Paze

# Added security

**My Card**



\*\*\*\*   



**Paze**



Paze



Modern Chair



**paze**<sup>SM</sup>



**E-mail**



Check out with **paze**

**Paze**

**paze**<sup>SM</sup>



**E-mail**

john@doe.com



Check out with **paze**

**paze**<sup>SM</sup>



**Verifying your identity**



**Paze**



**paze**<sup>SM</sup>



## Payment



**My Card**

\*\*\*\* 1234

**Bank Rewards Credit**

\*\*\*\* 1234



**My Card**

\*\*\*\* 6441

**Any Bank Credit**

\*\*\*\* 6441



**My Card**

**Next Bank Debit**

\*\*\*\* 4835

**Paze YOUR DIGITAL WALLET**

paze<sup>SM</sup>



## My Card

**Bank Rewards Credit**  
Credit Card

\*\*\*\* 1234

### Card details

Card number \*\*\*\* 1234

Billing address  
1234 Maple Lane, San Francisco, CA 94016

paze<sup>SM</sup>



## My Card

**Bank Rewards Credit**  
Credit Card

\*\*\*\* 1234

### Card details

Card number \*\*\*\* 1234

Billing address  
1234 Maple Lane, San Francisco, CA 94016

[Confirm details](#)

**Paze YOUR CARD DETAILS**

- Opt Out
- <https://mywallet.paze.com/footerOptOut>
- Token based
- WEB based



## Sorry to see you go!

You will no longer be able to access your Paze wallet if you proceed with opting out.

By selecting "Opt out of Paze," you consent to receive a one-time verification code via SMS text. Message and data rates may apply.

Opt out of Paze

[Return to Paze](#)

Paze



## To opt you out, we'll need to find your wallet.

We need the email you use with any participating bank or credit union to find your wallet.

Email



## Confirm opt out.

By confirming opt out, you are deactivating the Paze wallet for:



If there is a wallet associated with this email, we will opt it out of Paze. An email will be sent to you for confirmation.

Paze is offered by your banks and credit unions, so if you decide to use Paze in the future, visit their website or app to add a card to the service.

Confirm opt out

Cancel



## You've successfully opted out.

We'd love your feedback, please let us know why you've opted out.

- ☐ I'm not interested in using digital wallets
- ☐ I'm happy with the digital wallet I currently use
- ☐ I don't understand the value of Paze
- ☐ I don't want to use Paze
- ☐ Other

Submit feedback

Exit Paze

# Paze

| Word Count               |  | ?      | × |
|--------------------------|--|--------|---|
| Statistics:              |  |        |   |
| Pages                    |  | 10     |   |
| Words                    |  | 4,003  |   |
| Characters (no spaces)   |  | 21,706 |   |
| Characters (with spaces) |  | 25,640 |   |
| Paragraphs               |  | 72     |   |
| Lines                    |  | 315    |   |

# Paze Service Agreement

- Walmart & other merchants
- No transaction fees
- Customer data collection
- Now Walmart Pay
- Poor security
- Additional App

**CurrentC**

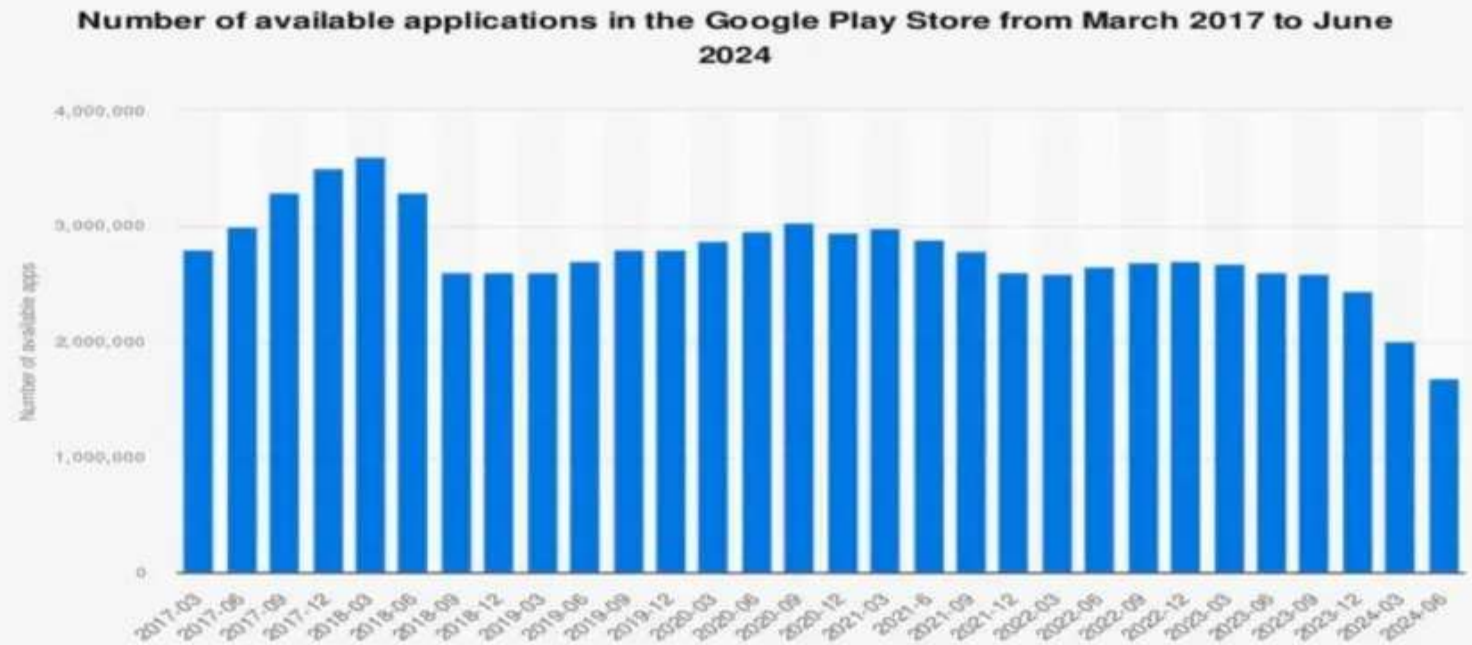
- Cyberwarcon – annual conference report  
North Korea gaining cybercurrency  
VC, recruiters, IT workers  
teleconference issues “load this to fix”  
Remote IT workers: pay, steal secrets, plant spyware, extortion, ...
  - UEFI bootkit for Linux  
Bootkitty
  - AI phishing  
smishing  
vishing
- Thanks for the contribution



# Current Issues



- "Surveillance and Digital Control at Work"
- Google Play Store app purge



**Sources**

Android; Google; Data.ai; AppBrain  
© Statista 2024

**Additional information:**

Worldwide; Google; Android; Data.ai; March 2017 to June 2024; figures have been rounded

# Current Issues

- Salt Typhoon thousands of thousands network gear needs replacing
- 7-Zip malware vulnerability – patch
- Hoboken, New Jersey city hall ransomware  
All services suspended
- Reminder Bing Wallpaper App  
Peruse Chrome cookies “to ensure Bing app is already installed
- FBI warning  
scam websites up 89%  
80% of shopping offers in inboxes are fraudulent  
Search engine results poisoned to send traffic to bad sites

[FBI Shopping Warning](#)

## Current Issues

- Check Point online shopping warning
- Check URLs closely for misspellings or unusual host domains.
- Make sure the URL starts with "https://" and shows a padlock icon.
- When emails come in, reference the sender against emails you know to be real. Don't click anything you're not sure about.
- Don't blindly click through on QR codes.
- Never input unnecessary details like your social security number, and avoid inputting extra info like your birthday where it's not required."

## Current Issues

- Examples:

- Stüssy (Streetwear): *stussycanadablackfriday[.]com*
- Longchamp (Bags): *longchampblackfriday[.]com*
- Wayfair (Online Home Store):  
*wayfareblackfriday[.]com*
- SOREL (Footwear): *soreloutletblackfriday[.]com*
- Crew (Retail): *jcrewblackfriday[.]com*
- IUN (Footwear): *blackfriday-shoe[.]top*

## Current Issues

- Mobile devices with smaller screens
- If in doubt:
  - “Report the scam immediately to authorities like Action Fraud in the UK or the FTC in the US
  - Tell your bank and, if relevant, freeze your cards – requesting new ones
  - Stop contact with the scammer and don’t tell them why
  - Change any passwords that may have been compromised
  - Freeze your credit to prevent scammers opening new credit lines in your name. You'll need to contact each of the three major credit bureaus separately: Experian, TransUnion, and Equifax
  - Gather evidence of the scam in case it is required”

## Current Issues



**Police reported ahead**

From Waze drivers

Are they still there?

Yes

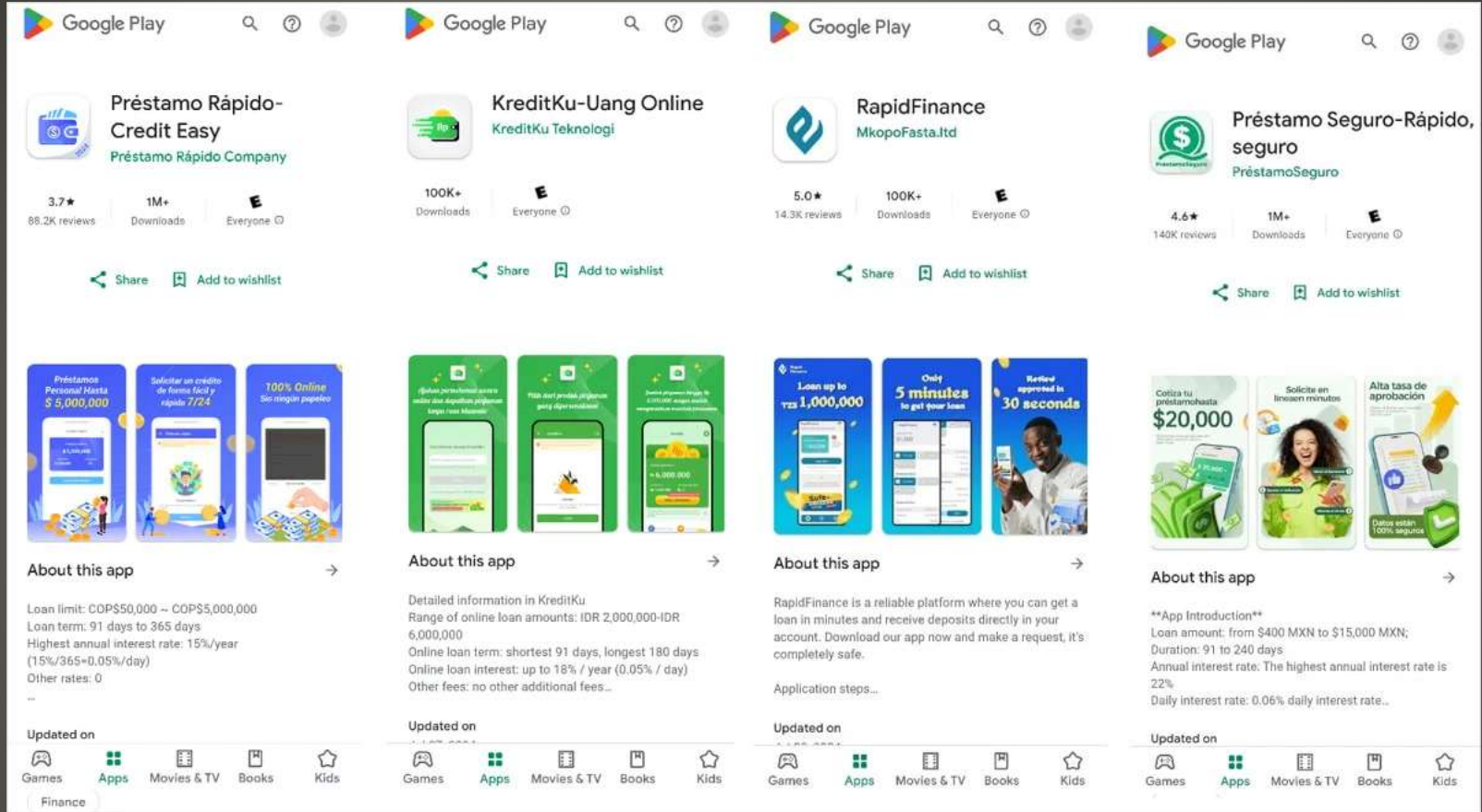
No

**Google Maps reporting from Waze**

- FALSE financial tools
- Loans “fast-tracked” deceptive / false terms
- 15 Apps in Google Play store
- 8 million downloads
- Misuse of permissions

**Spy Loan**





Spy Loan examples

- Member contributed article, Thanks David  
[Wired article Google Photos & AI](#)
- US Coast Guard warning Chinese port cranes
- Pakistan blocks BlueSky
- REPO swatting attacks  
GitHub & GitLab    attacker sneaks malicious files to repo  
reports to GitHub or GitLab  
Account taken down
- Palo Alto Networks vulnerabilities attacked  
Very good reputation – not deserved    PHP
- D-Link VPN routers with un patchable EXTREME vulnerabilities  
DSR-150 150N 250 250N  
DSR-500N 1000N
- VPN usage against Shariah law    *abetting in sin*

## Current Issues

- Chinese lidar sensors complex firmware  
Potential disable via satellite lasers
- ChatGPT freeze for names: David Mayer et al
- Potential Microsoft license hack  
Extended Security Update? Windows 10
- Samsung delay Android 15 – Fake Updates
- <https://theyseeyourphotos.com/>

This web site takes a photo you download to this site, then has Google use its AI to document what Google's AI sees and documents any findings. This information was posted on the Computer Club's AI SIG Message Board.

Consider posting your AI findings to inform other club members!

- AT&T to shutdown DSL and traditional phone service

## Current Issues

- UK cyber report 2024 triple number of threats over 2023
- Amazon super computer with home-grown AI chip  
Apple also uses Amazon AI chips
- National Public Data shuts down  
272 million SSN 600 million phone numbers
- Digital epileptic seizures  
image-based automatic driving systems - epilepticar
- Tor seeking WebTunnel bridge volunteers  
[Tor project WebTunnel paper](#)
- Zello (mobile push-to-talk app) request all users change passwords
- Android scareware – mimic cracked or malfunctioning screens
- Corrupt file sent by attackers  
Bypass security suites and email filters  
Click here to recover corrupt file => Infection

## Current Issues



**World Labs 3D generation**



- Microsoft Windows Recall feature available  
Insider build 26120.2415 Snapdragon Copilot+ PCs  
[Microsoft Windows Insider blog](#)  
Ability to disable/turn off ?  
Requires Windows Hello face or fingerprint enrollment  
Click to Do to be expanded  
Search both text and image  
Search filter: financial, encrypted messaging, ...  
Not available on IT managed machines  
Requirements:
  - BitLocker or device encryption
  - TPM 2.0
  - Windows Hello
  - Hyper-V

## Windows Recall

- iOS and Android spyware checker  
iVerify Basics \$1 Subscribers get regular scans  
App creates file to download to iVerify for analysis  
Provide email address
- Microsoft Windows 11

TPM 2.0 plays a crucial role in enhancing identity and data protection on Windows devices, as well as maintaining the integrity of your system. TPM 2.0 also helps future-proof Windows 11. One way it does so is by helping to protect sensitive information as more AI capabilities come to physical, cloud, and server architecture.

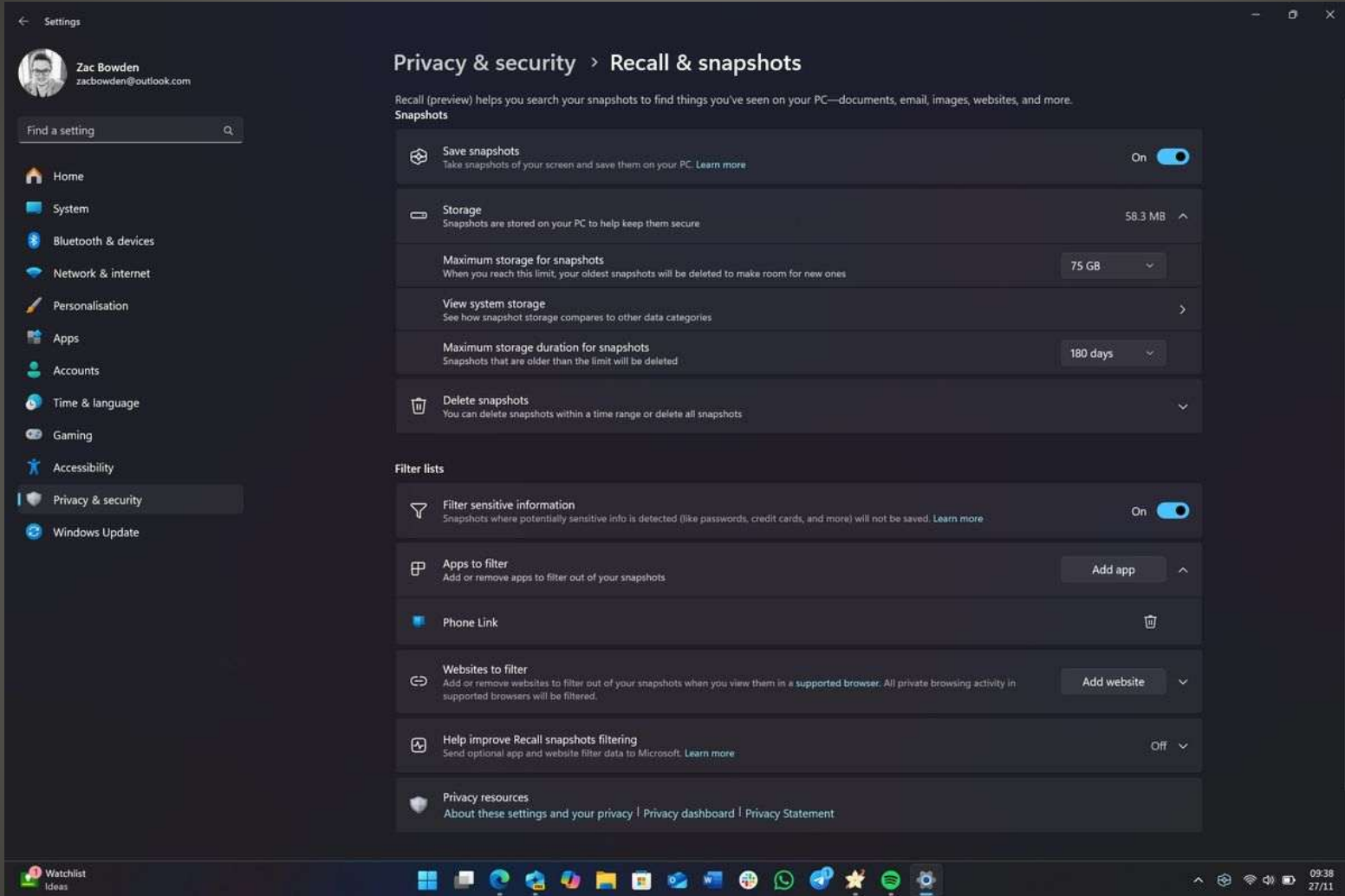
Steven Hosking, Senior Product Manager at Microsoft

## Current Issues



- New discovery    Universal memory  
Indium-Selenide ( $\text{In}_2\text{Se}_3$ )    Phase-change memory  
Store data without power

## Current Issues



# Windows Recall Search settings

- Microsoft Connected Experience

Microsoft Office Word and Excel document content AI

“Connected experiences that analyze your content are experiences that use your Office content to provide you with design recommendations, editing suggestions, data insights, and similar features.”

ON BY DEFAULT

File -> Options -> Trust Center -> Trust Center Settings

-> Privacy Options -> Privacy Settings -> Connected experiences


# Microsoft Connected Experience

## Experiences that download online content

Office can provide you with searchable, downloadable online content like templates, images, and videos. For example, experiences that help you search for online pictures to add to your slides.

[Learn more](#)

☐ Turn on experiences that download online content

 If you turn this off, some experiences won't be available to you.


## All connected experiences

Connected experiences include things like analyzing content, downloading online content, and online file storage. Outlook email services and essential services, such as downloading updates, will still work even when this setting is not turned on. This setting also allows you to apply your account privacy settings across devices.

[Learn more about connected experiences](#)

[Learn more about where your settings apply](#)

☒ Turn on all connected experiences

 If you turn this off, Outlook email services and essential services will continue to work. Other connected experiences won't be available, and your account privacy settings won't apply across devices.

# • ON BY DEFAULT

Privacy Settings

[Learn more](#)

☐ Turn on experiences that download online content

**i** If you turn this off, some experiences won't be available to you.

**All connected experiences**

Connected experiences include things like analyzing content, downloading online content, and online file storage. Outlook email services and essential services, such as downloading updates, will still work even when this setting is not turned on. This setting also allows you to apply your account privacy settings across devices.

[Learn more about connected experiences](#)  
[Learn more about where your settings apply](#)

☐ **Turn on all connected experiences**

**i** If you turn this off, Outlook email services and essential services will continue to work. Other connected experiences won't be available, and your account privacy settings won't apply across devices.

Personalized offers and discounts for Microsoft products

OK Cancel

## Microsoft Connected Experience

- Office App

File -> Account -> Account Privacy -> Manage Settings

Connected Experience OFF

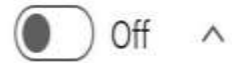
# Microsoft Account

## Connected experiences



### Experiences that analyze your content


Allow experiences that provide you with helpful resources, info, and ideas by analyzing your...



Some connected experiences in Microsoft 365 will use your content to help you create, communicate, and collaborate more effectively. For example, experiences that find information available online about a word or phrase used in a document.

[Learn more](#)



 If you turn this off, some experiences won't be available to you.

# And everywhere?



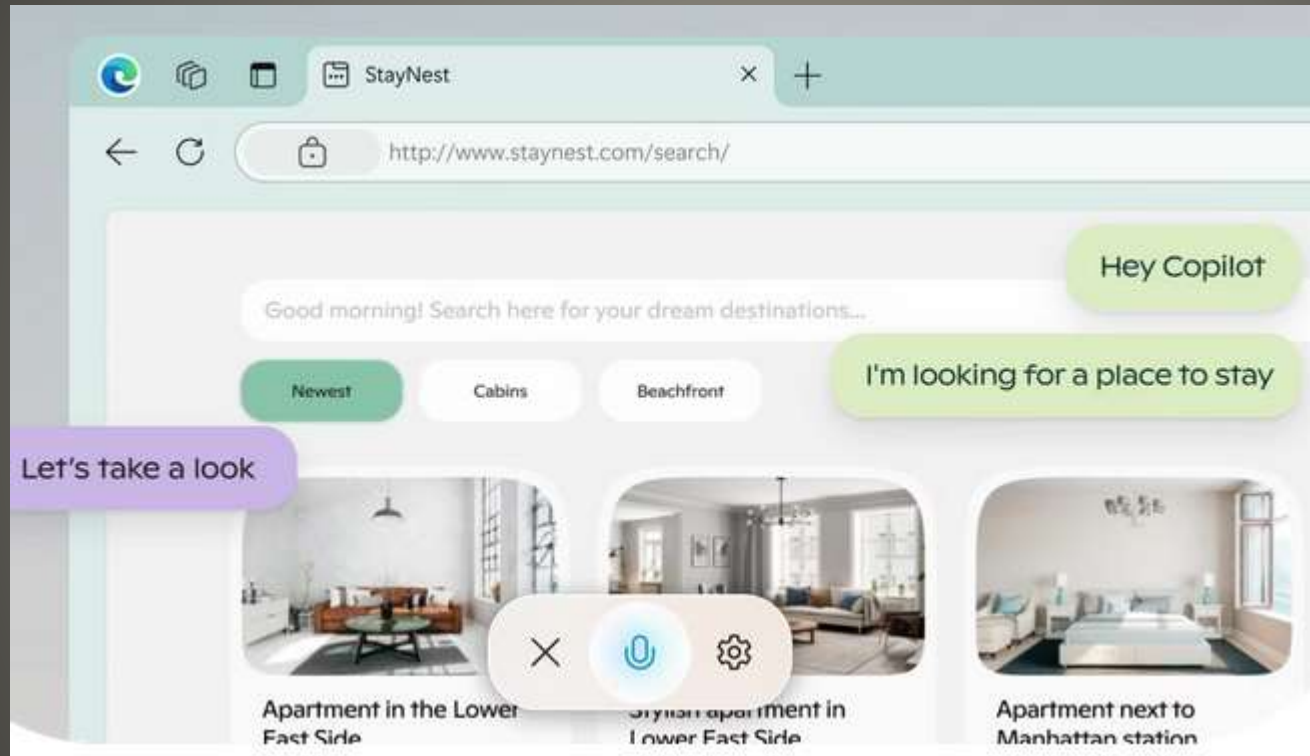
- AI any/everywhere

The Connected Experiences setting enables cloud-backed features designed to increase your productivity in the Microsoft 365 apps like suggesting relevant information and images from the web, real-time co-authoring and cloud storage, and tools like Editor in Word that provide spelling and grammar suggestions.

Microsoft has been using AI in Microsoft 365 for years to enhance productivity and creativity through features like Designer in PowerPoint, which helps create visually compelling slides, and Editor in Word, which provides grammar and writing suggestions. These features do not rely on generative AI or Large Language Models but rather use simpler machine learning algorithms."

**Microsoft**

- Microsoft Vision  
Understand & respond to Microsoft Edge screens



## Current Issues

- Recovery Seminar
- <https://vimeo.com/882272974?share=copy>
- NOW, Your input, experiences, ...
- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

Computer Club, Help Center, SIGs, Presentations, classes  
Cyber Security SIG meetings, NEWSBLOG  
Internet

- Questions, suggestions, comments?

**SCCCCyber@gmail.com**