Sun City Computer Club

Cyber Security SIG
June 20, 2024

Questions, Comments, Suggestions welcomed at any time

Even Now

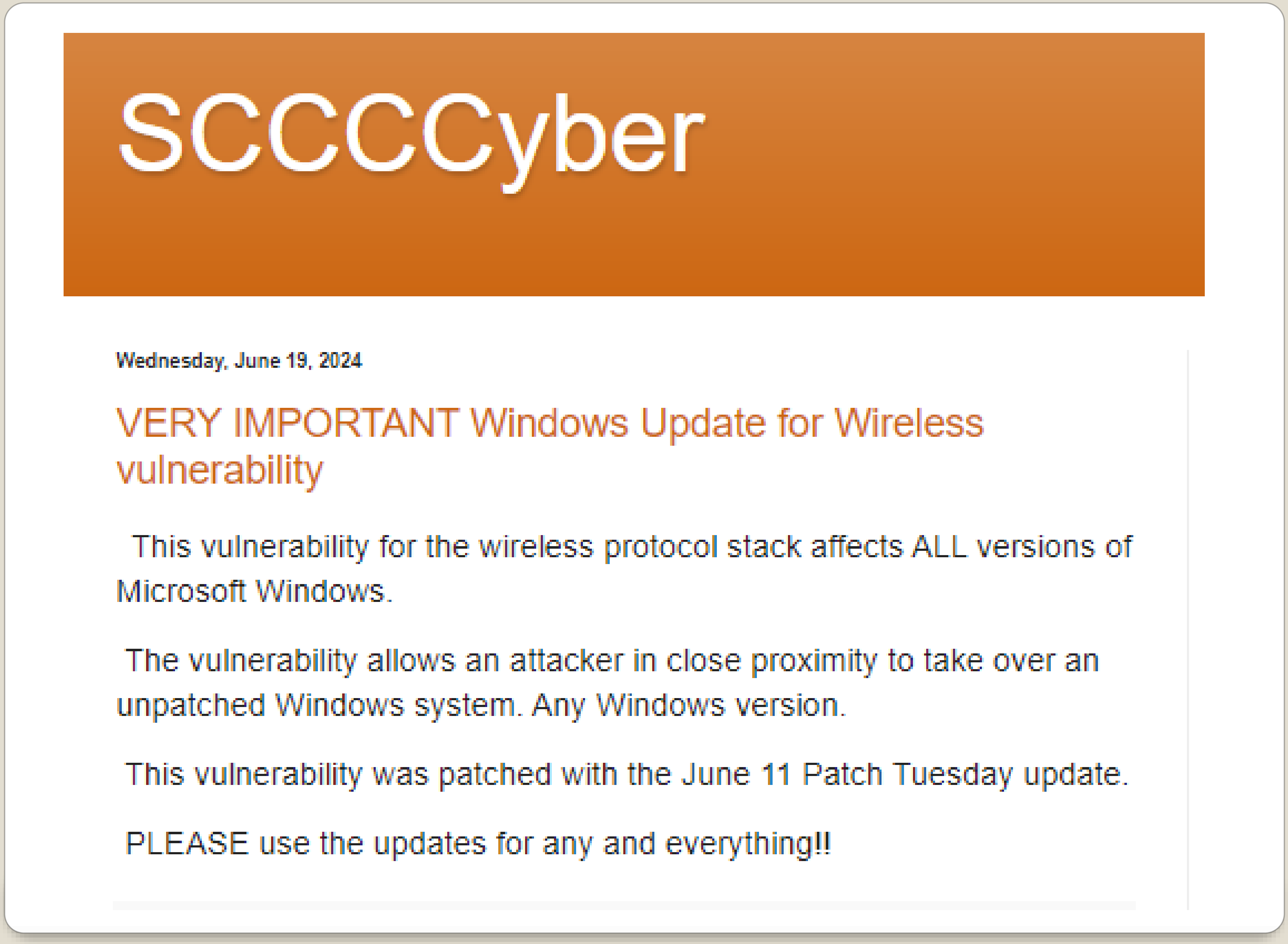
- Audio recording of this session as MP4 file
- Audio recording available at link shown above
- Wake Words

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

New Leader???



SCCCyber

Wednesday, June 19, 2024

VERY IMPORTANT Windows Update for Wireless vulnerability

This vulnerability for the wireless protocol stack affects ALL versions of Microsoft Windows.

The vulnerability allows an attacker in close proximity to take over an unpatched Windows system. Any Windows version.

This vulnerability was patched with the June 11 Patch Tuesday update.

PLEASE use the updates for any and everything!!

Windows 7?

- CVE-2024-30078 patch available for windows 7?

- Copilot
- Yes, a patch for the CVE-2024-30078 vulnerability is available. This high-severity vulnerability affects Windows operating systems. An attacker within Wi-Fi range of the computer can exploit it by sending a specially crafted network packet to the target12. To protect your Windows PC, ensure it’s updated with the patch released on June 11th as part of Microsoft’s monthly security update3. Stay secure! 😊

- Chrome Version 126.0.6478.115 (Official Build) (64-bit)
- Edge Version 126.0.2592.61 (Official build) (64-bit)
- Firefox Version 127.0.1
- Safari version 17.5 (19618.2.12.11.6)
- Brave Version 1.67.119 Chromium: 126.0.6478.114
- Vivaldi Version 6.8.3381.44
- DuckDuckGo Version 0.84.0
- Arc Version 125.0.6422.142

- ChromeOS 125.0.6422.197

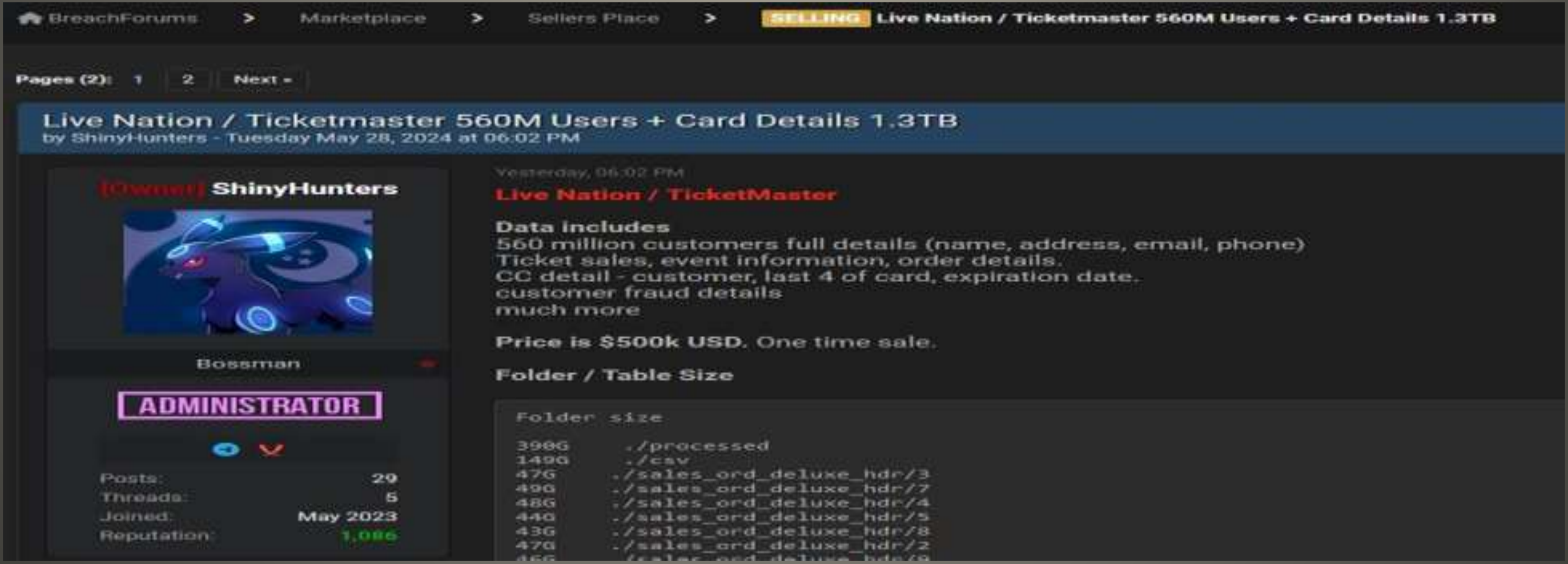
Browser Versions

Current Issues

- FBI distributes 7,000 LockBit ransomware decryption key
- PHP critical vulnerability trivially exploited Friday afternoon
- TikTok vulnerability Account takeover

  CNN success Paris Hilton failed
- Year of Identity Siege

  Identities are best sellers



BreachForums > Marketplace > Sellers Place > SELLING Live Nation / Ticketmaster 560M Users + Card Details 1.3TB
Pages (2): 1 2 Next »
[Owner] ShinyHunters
Bossman
ADMINISTRATOR

Live Nation / Ticketmaster 560M Users + Card Details 1.3TB
by ShinyHunters - Tuesday May 28, 2024 at 06:02 PM

Posts: 29
Threads: 5
Joined: May 2023
Reputation: 1,086

Yesterday, 06:02 PM

Live Nation / TicketMaster

Data includes
560 million customers full details (name, address, email, phone)
Ticket sales, event information, order details.
CC detail - customer, last 4 of card, expiration date.
customer fraud details
much more

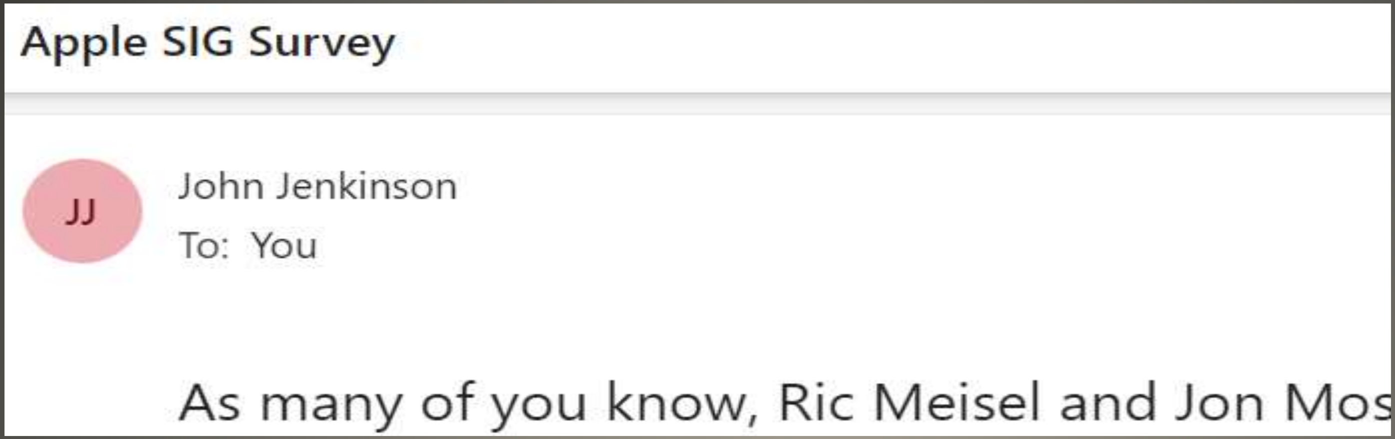
Price is $500k USD. One time sale.

Folder / Table Size

```
Folder size

398G     ./processed
149G     ./csv
47G     ./sales_ord_deluxe_hdr/3
49G     ./sales_ord_deluxe_hdr/7
48G     ./sales_ord_deluxe_hdr/4
44G     ./sales_ord_deluxe_hdr/5
43G     ./sales_ord_deluxe_hdr/8
47G     ./sales_ord_deluxe_hdr/2
```

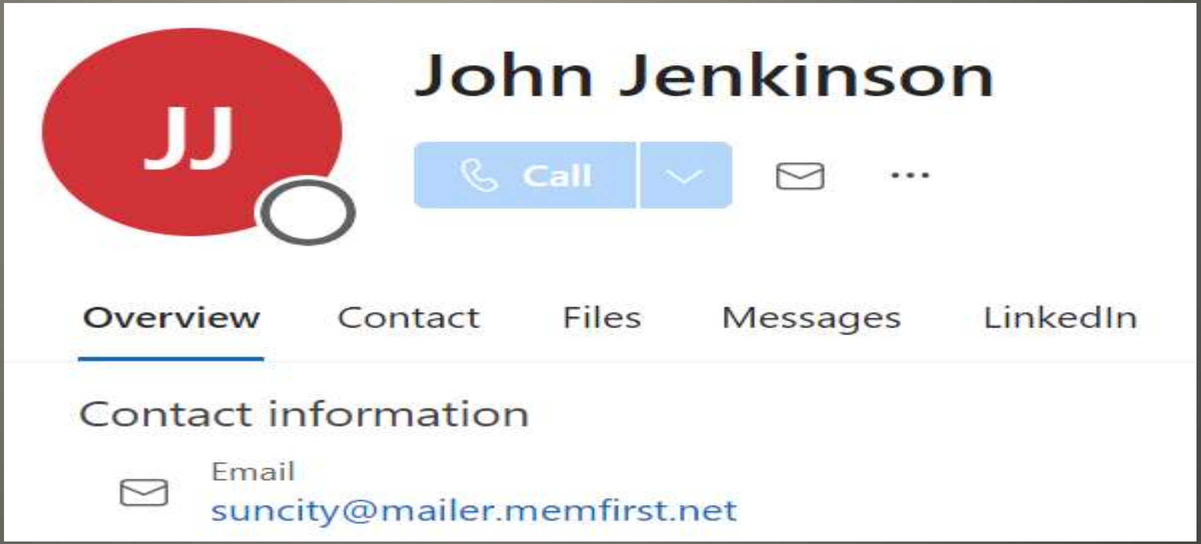
Apple SIG Survey



Apple SIG Survey

John Jenkinson
To: You

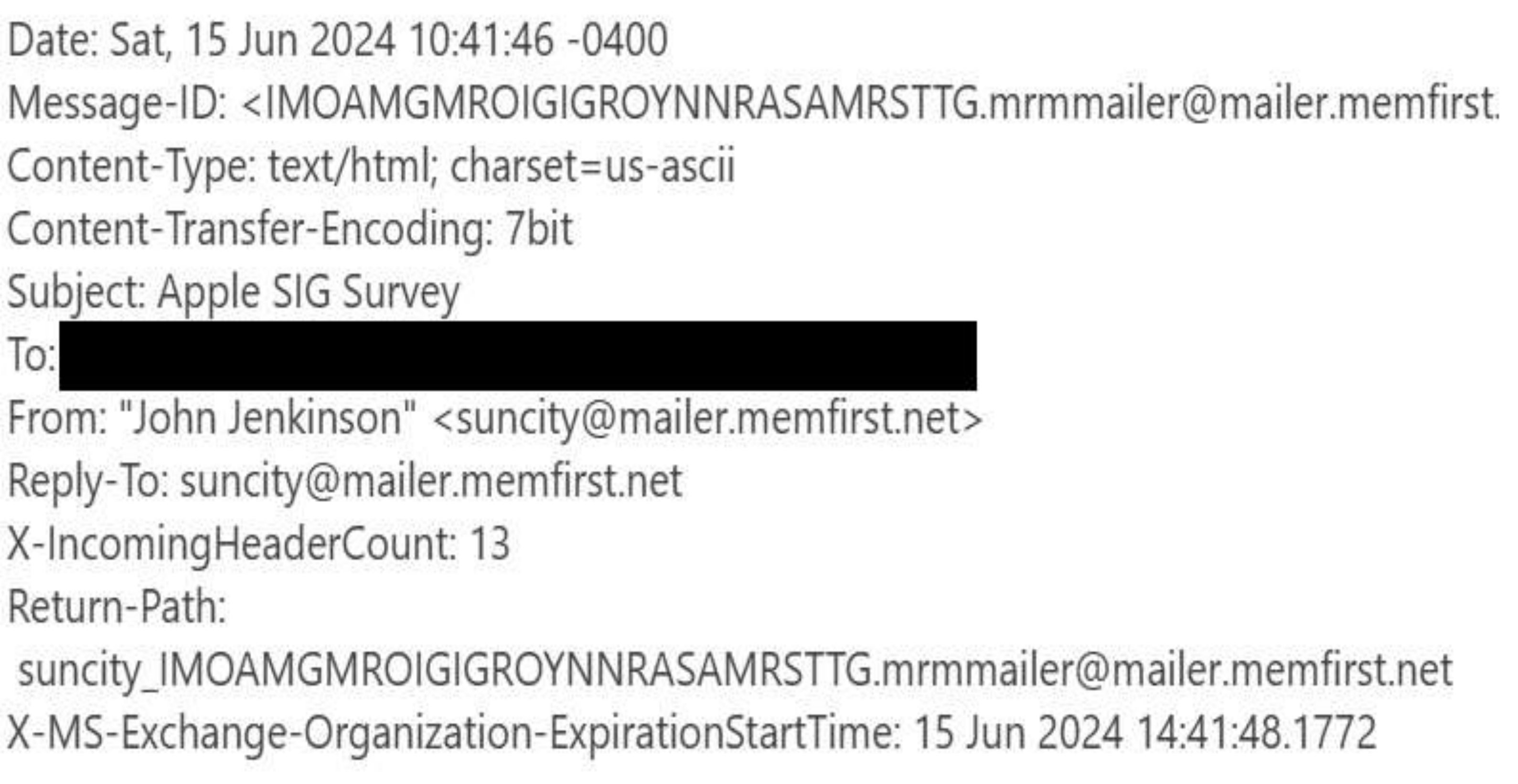
As many of you know, Ric Meisel and Jon Mos



John Jenkinson

Contact information

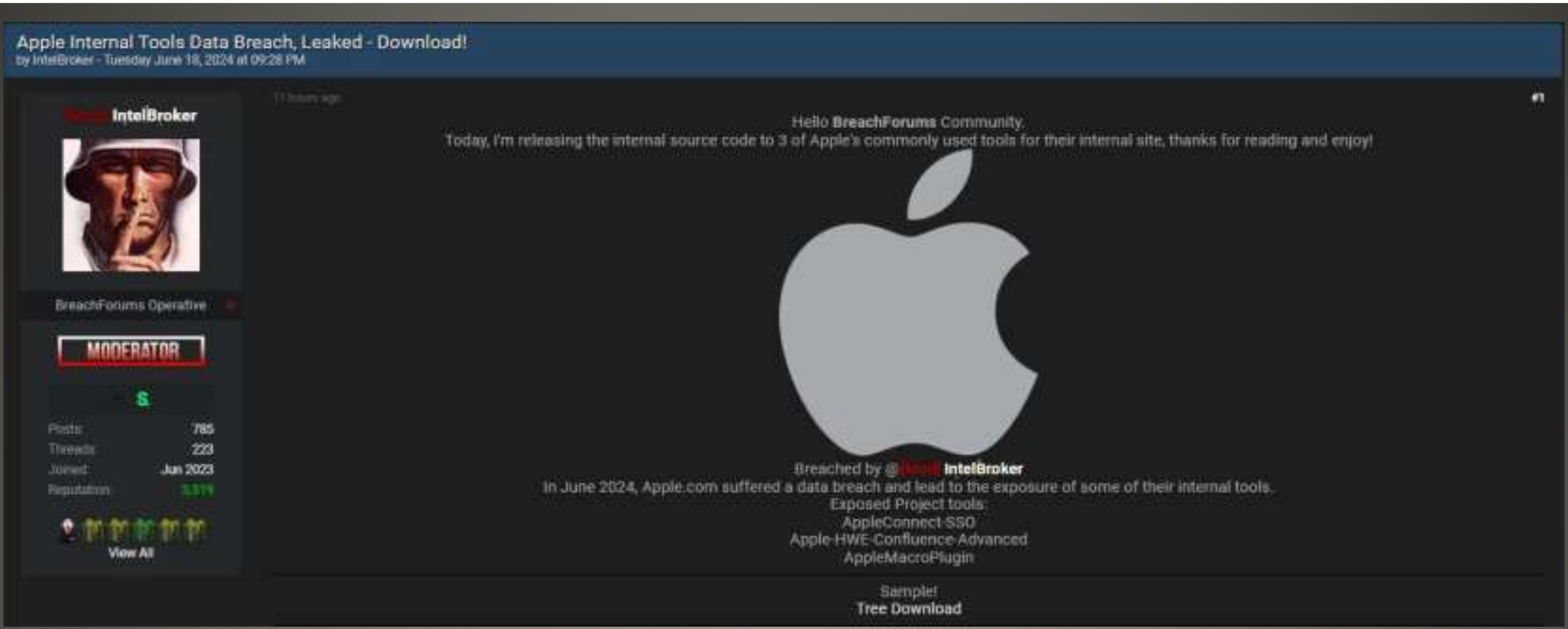
Email
suncity@mailer.memfirst.net



```
Date: Sat, 15 Jun 2024 10:41:46 -0400
Message-ID: <IMOAMGMROIGIGROYNNRASAMRSTTG.mrmmailer@mailer.memfirst.
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit
Subject: Apple SIG Survey
To: [redacted]
From: "John Jenkinson" <suncity@mailer.memfirst.net>
Reply-To: suncity@mailer.memfirst.net
X-IncomingHeaderCount: 13
Return-Path:
 suncity_IMOAMGMROIGIGROYNNRASAMRSTTG.mrmmailer@mailer.memfirst.net
X-MS-Exchange-Organization-ExpirationStartTime: 15 Jun 2024 14:41:48.1772
```

Appple SIG Survey

Apple Data Breach?



Apple Internal Tools Data Breach, Leaked - Download!
by IntelBroker - Tuesday June 18, 2024 at 09:28 PM

11 hours ago

#1

IntelBroker

BreachForums Operative

MODERATOR

Posts: 785
Threads: 223
Joined: Jun 2023
Reputation: 3,519

View All

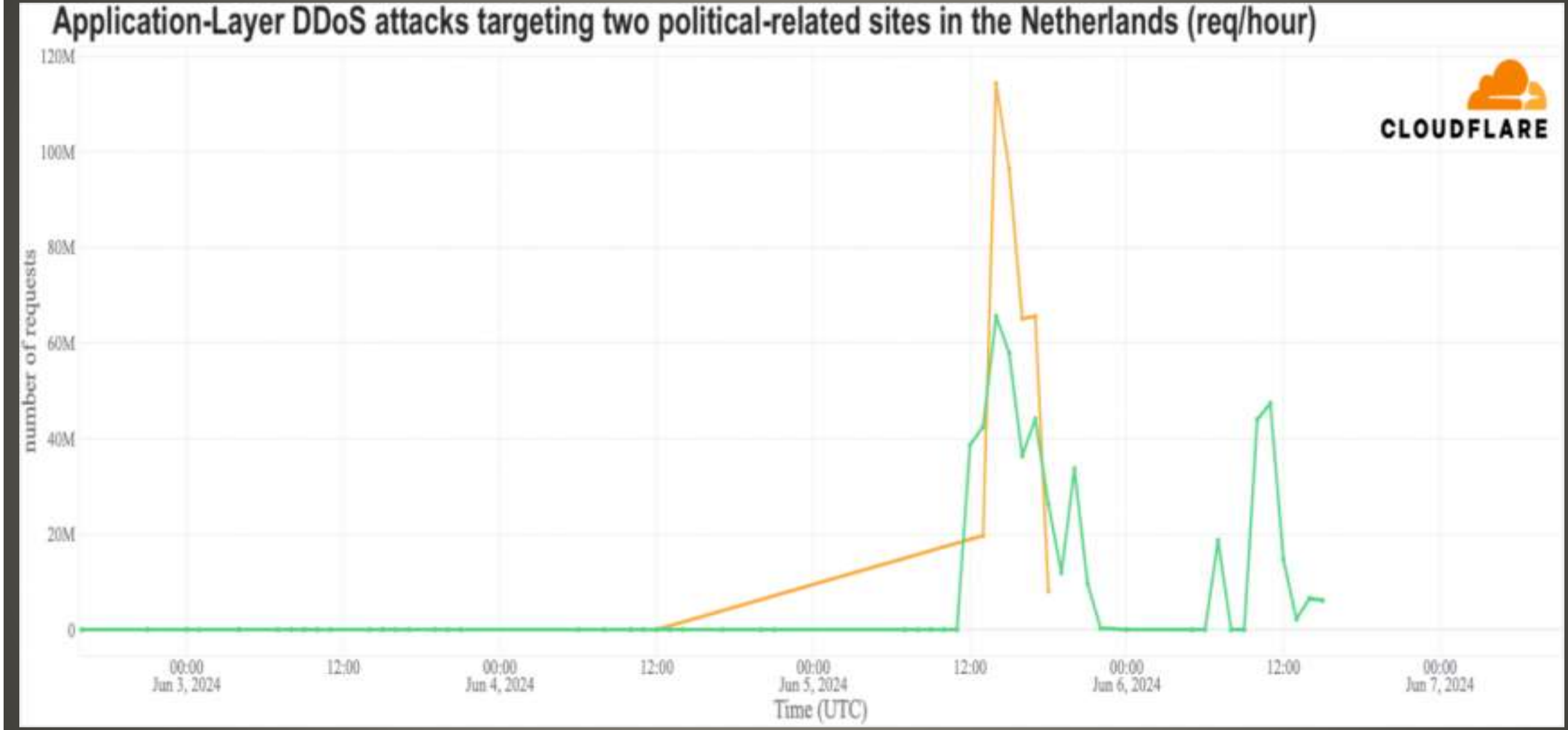
Hello **BreachForums** Community,
Today, I'm releasing the internal source code to 3 of Apple's commonly used tools for their internal site, thanks for reading and enjoy!

Breached by @ **IntelBroker**
In June 2024, Apple.com suffered a data breach and lead to the exposure of some of their internal tools.
Exposed Project tools:
AppleConnect-SSO
Apple-HWE-Confluence-Advanced
AppleMacroPlugin

Sample!
Tree Download

- IntelBroker
- AppleConnect-SSO

Political DDoS



Application-Layer DDoS attacks targeting two political-related sites in the Netherlands (req/hour)

- US Senate panel
  Permanent Subcommittee on Investigations
  Zelle

"Zelle transfers are nearly instant and irreversible, and by the time a consumer knows they've been scammed, usually it's too late to do anything about it – at least according to Zelle and according to the banks that own, control, and in effect operate Zelle…

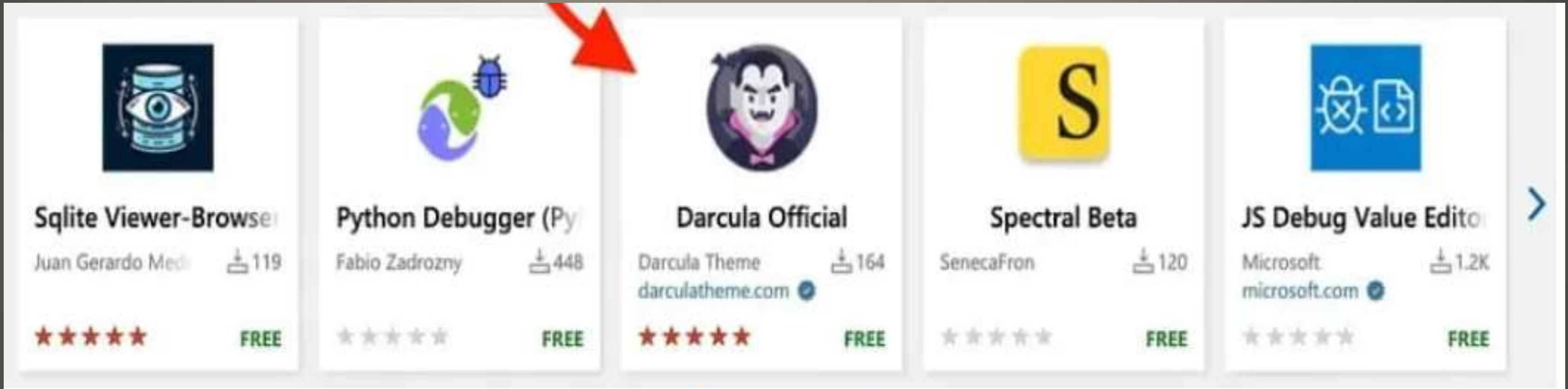
Zelle and the banks that own it offer to customers the appearance of the trust they feel they deserve. But the risks there are real and present, and they simply are failing to protect consumers in the way that they deserve."

- Chromebooks accessibility feature
  Face Control
  Mouse – tilt head
  click – scrunching lips
  Games – smiling shrugging eyebrows

Current Issues

Current Issues

- Frontier Communications 750,000 customers
  April 14th
- Visual Studio Code marketplace
  Dracula Official

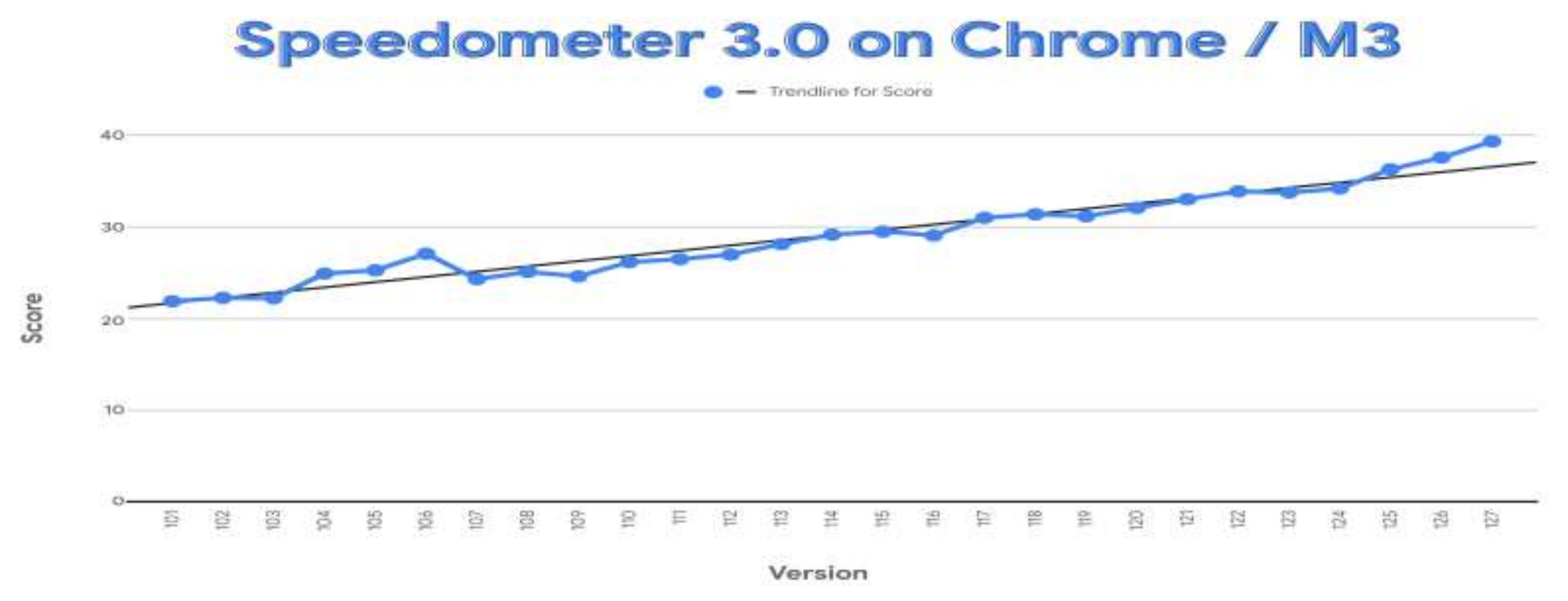


The Darcula extension on the VSCode Marketplace

- Disney hacked Internal data, advertising plans
  Club Penguin
  Club Penguin 2007 -> Club Penguin Island 2018 shutdown

Current Issues

- GPT-4 bots attack n-day vulnerabilities with high success rate
- New York Times internal source code and data stolen
- Google Chrome getting faster?



- Google internal database leaked
  6 year span
  Google internal review
  Socratic homework helper data
  Children's voices
  Auto license plates with geolocations
  Nintendo YouTube announcements
- DuckDuckGo to AI chatbots
  OpenAI GPT 3.5, Claude, Meta Llamba
  DuckDuckGo's IP address
- State sponsored threat actors accesses 20,000 Fortinet Fortigate systems Western governments, defense
  COATHANGER – persistent remote access
  Edge appliances

Current Issues

- National Public Data

  One of biggest providers of public records on the Internet
  People Finder SSN, DoB, address, phone number(s), …
  US Consumer data
  Voter registration data
  Criminal records
  3 decades of records
  Verification spotty
- Snowflake Pure Storage
  165 organizations?
- Cybersecurity and Infrastructure Security Agency (CISA)
  Scammers impersonating CISA
  Do NOT pay the caller Note phone number Hang up

Current Issues

- Update ???
- Snowflake data storage & analysis
  Derive intelligence & insight from data
- Third-party contractors
- EPAM Systems 55,000 employees
  Ukraine, Belarus, Russia
  Russia employees relocated
  EPAM employee’s computer infected with info-stealer
  That info sold
- Business Process Outsourcing companies
- One employee’s computer – Multiple BPO customers
- Information gives no indication of being stolen

Snowflake

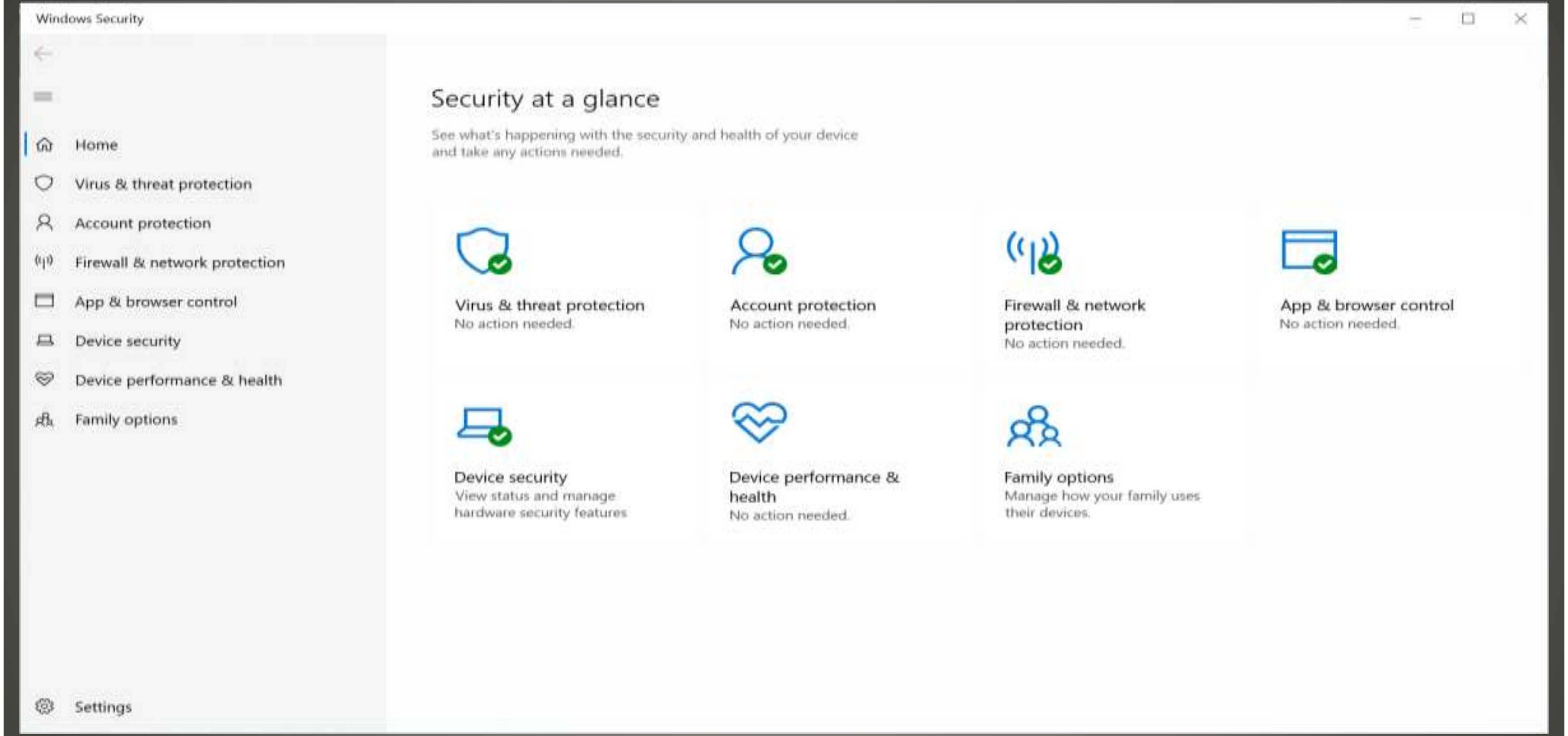
- ChromeOS to be developed on portion of Android stack
  Roll out AI features at faster pace
- Proton Drive New file sharing options
  Viewer or editor permissions via email
  Full privacy & control
  Via web currently – mobile versions later
- Sonos change to US user agreement

"Sonos does not and will not sell personal information about our customers,"
No opt-out - Return products

- Compromised legitimate websites deliver windows backdoor
  BadSpace
  Phony Google Chrome Update via overlay
- Google Chrome on Android "Listen to this page"
- TDK battery smaller size higher energy density

Current Issues

- Windows Defender -> Windows Security



Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
No action needed.

Account protection
No action needed.

Firewall & network protection
No action needed.

App & browser control
No action needed.

Device security
View status and manage hardware security features

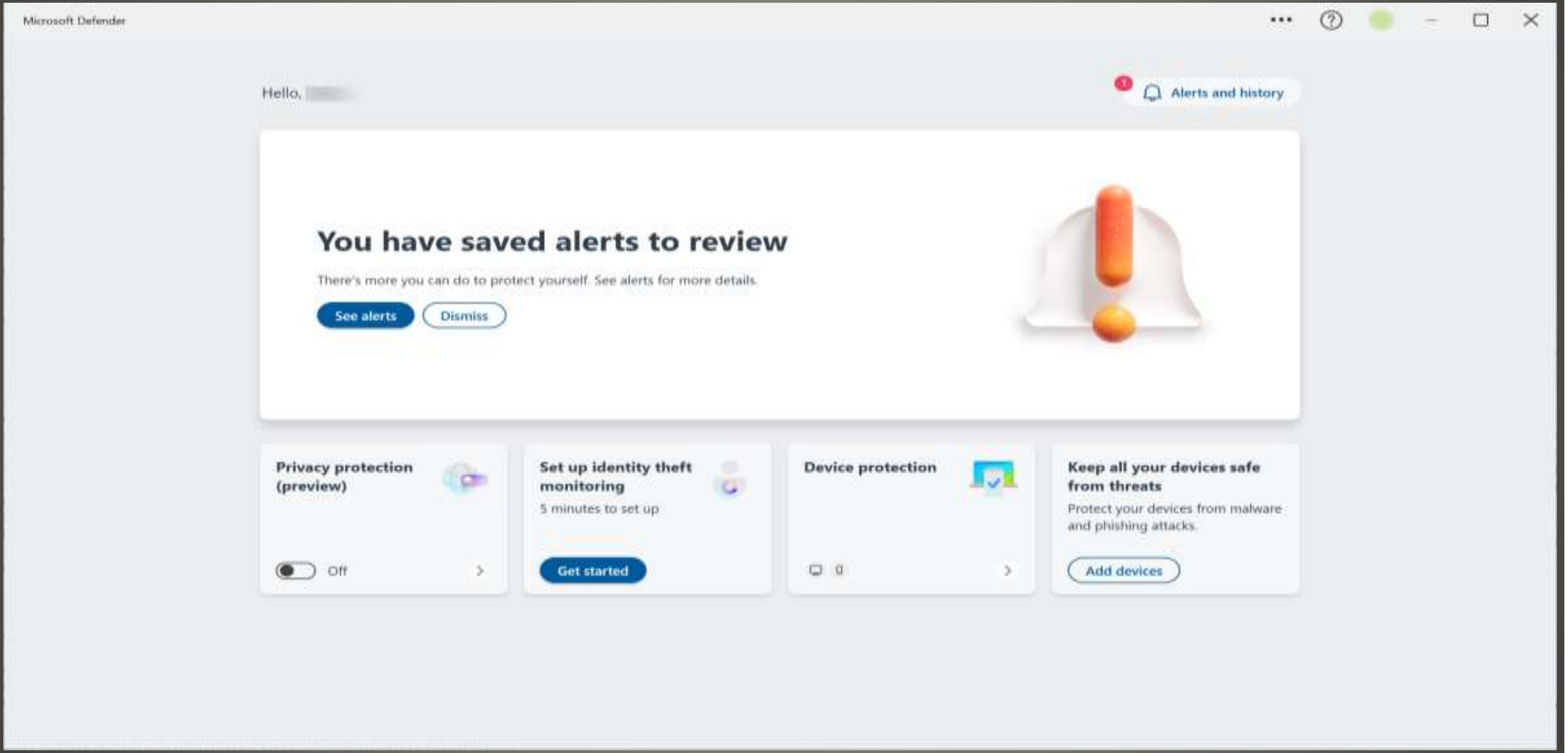
Device performance & health
No action needed.

Family options
Manage how your family uses their devices.

Windows Security

Microsoft Defender

- Microsoft Defender Antivirus engine
- Microsoft Defender App Microsoft 365 subscription



Hello, [redacted]

You have saved alerts to review

There's more you can do to protect yourself. See alerts for more details.

Privacy protection (preview)

Set up identity theft monitoring

5 minutes to set up

Device protection

0

Keep all your devices safe from threats

Protect your devices from malware and phishing attacks.

Microsoft Defender App

Windows Security Microsoft Defender

- Complementary
- Windows Security online threats
- Microsoft Defender Same network shield

- Microsoft Copilot Plus PC
  Recall
  Local tool
  search and retrieve content you’ve interacted with
  Opt-in   required NPU

Current Issues

- Microsoft Windows 11 Copilot+ laptop PCs
- Content you have viewed on your device
- Language aware searches 160 languages
- Text-to-Text
- Linux command history Windows 10 Timeline 2021
- AI + Machine Learning

===================================

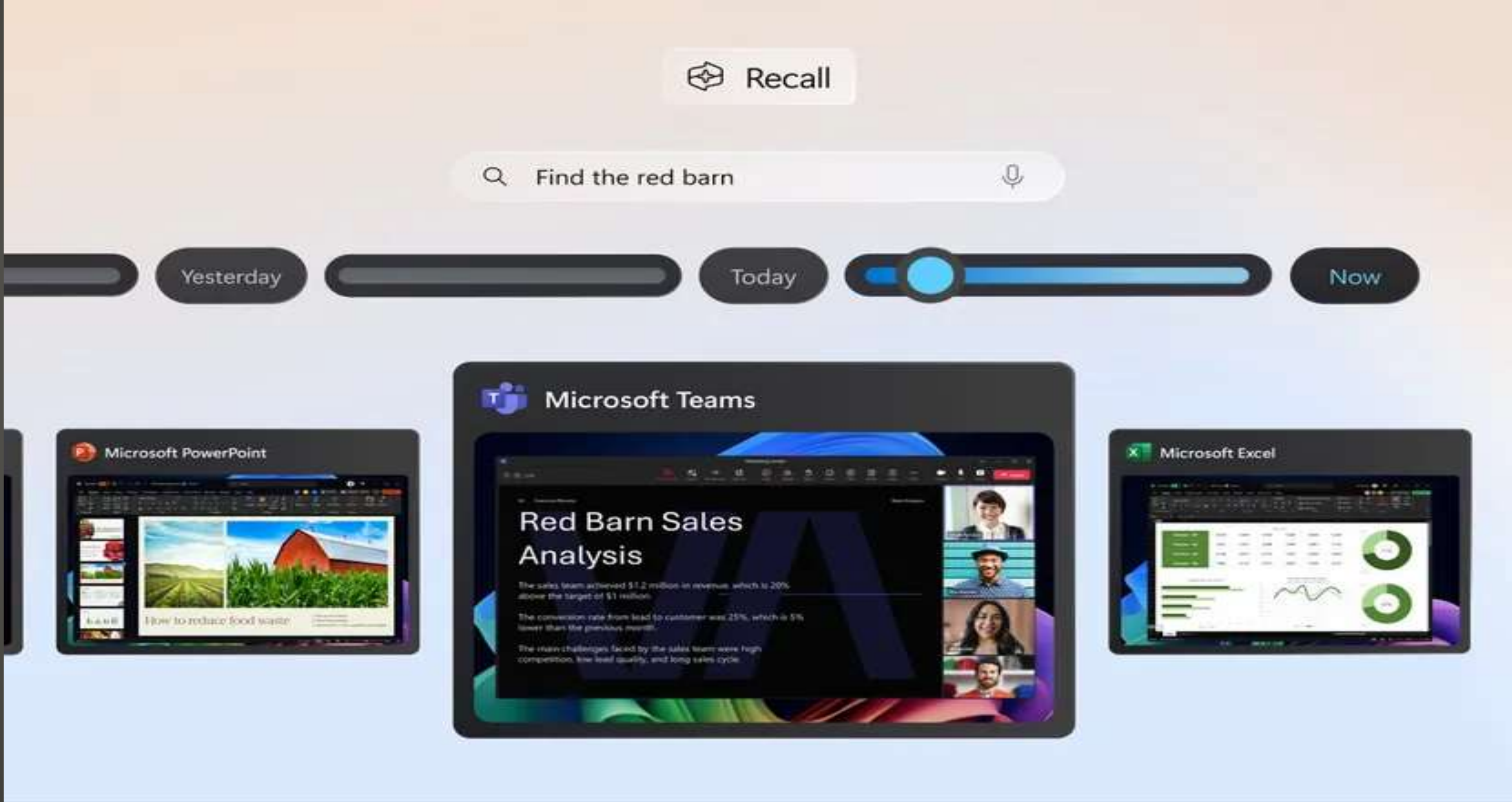
Copilot+ with advanced processing capabilities
Active images of screen every few seconds
Encrypted and saved to hard drive 50GB available
Scroll through snapshots -> Select -> Interact
Helpful <-> Harmful
Recall Settings Control
Edge InPrivate sessions DRM protections
BUT no content moderation “Show Password” Account Numbers

Microsoft Recall

- 16GB RAM
- 40+ TOPS NPU
- Qualcomm Snapdragon X Plus
- Qualcomm Snapdragon X Elite
- ARM
- Recall
- Cocreator Start in Paint + AI
- Cocreator existing photo / image change style
- Studio Effects app
- Live captions 40 languages
- Gaming with Automatic Super Resolution
- Copilot runtime
- Semantic Index
- Adobe Photoshop, Lightroom, Express

Copilot+ PCs

- Encrypted – Associated profile - local hard disk
- Videos -> transcribed & translated speech



Microsoft Recall

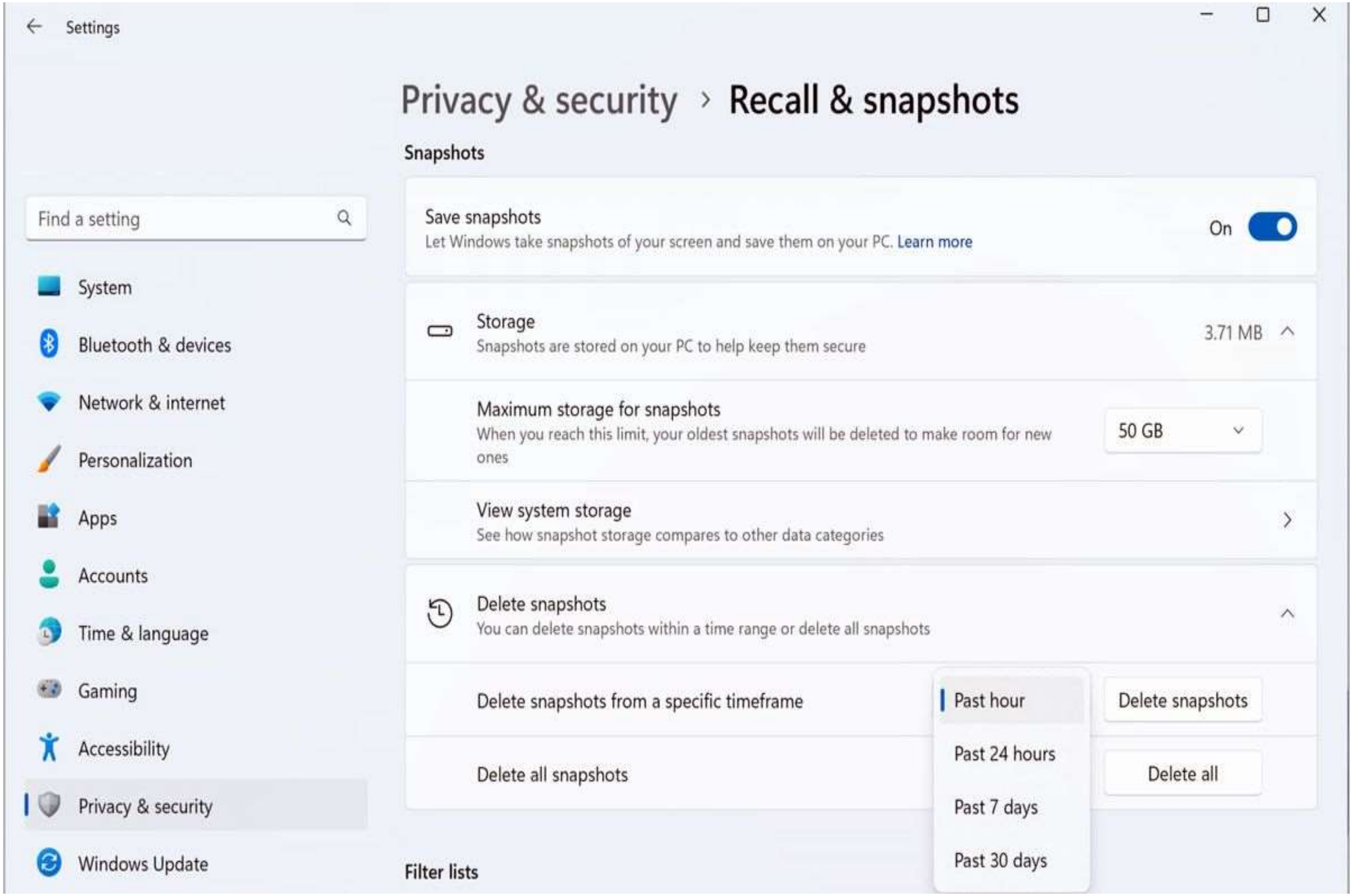
- End-to-End encrypted messages GOT IT
- Disappearing messages GOT It
- Grandma got run over by a reindeer GOT IT

- If Recall can search …..
- TotalRecall

- Off by default?

- Windows Hello
- Just-in-time decryption

Microsoft Recall



Privacy & security › Recall & snapshots

Snapshots

Save snapshots
Let Windows take snapshots of your screen and save them on your PC. Learn more
On

Storage
Snapshots are stored on your PC to help keep them secure
3.71 MB

Maximum storage for snapshots
When you reach this limit, your oldest snapshots will be deleted to make room for new ones
50 GB

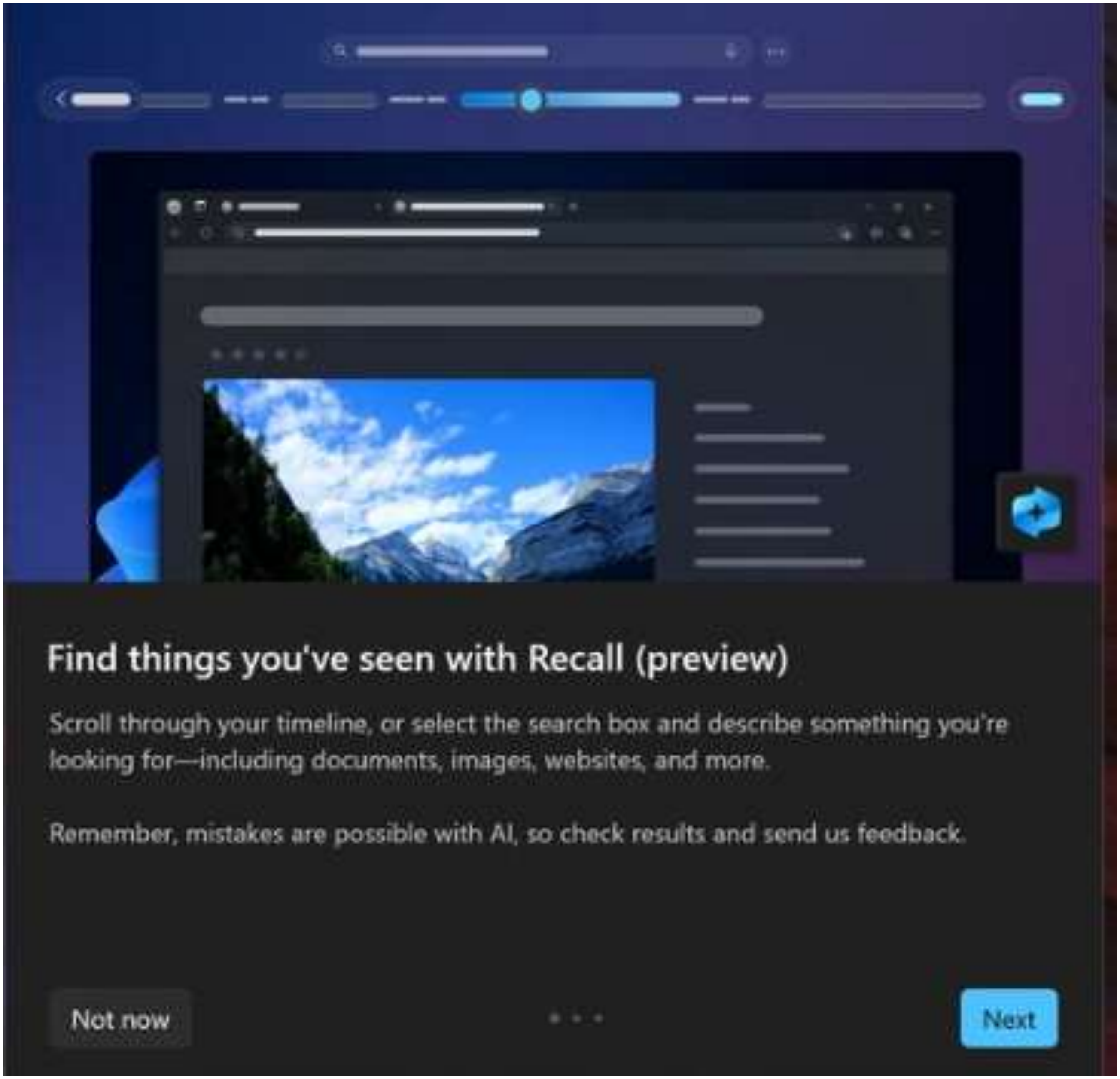
View system storage
See how snapshot storage compares to other data categories

Delete snapshots
You can delete snapshots within a time range or delete all snapshots

Delete snapshots from a specific timeframe

Delete all snapshots

Filter lists



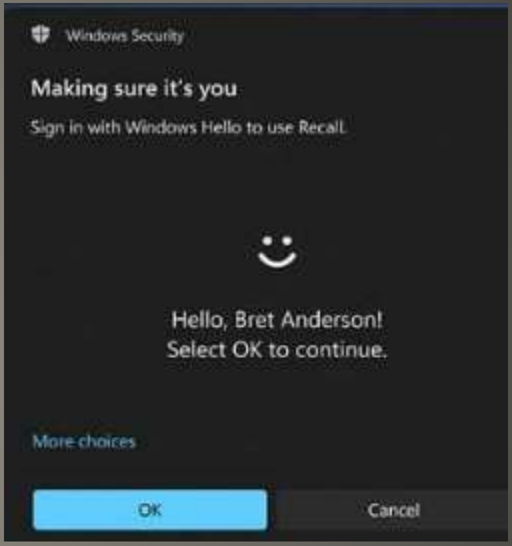
Find things you've seen with Recall (preview)

Scroll through your timeline, or select the search box and describe something you're looking for—including documents, images, websites, and more.

Remember, mistakes are possible with AI, so check results and send us feedback.

Microsoft Recall

- Opt-out -> Opt-In
- Proof of Presence to view timeline & Search in Recall
- Windows Hello to enable
- Just-in-Time decryption
- 18-June-2024

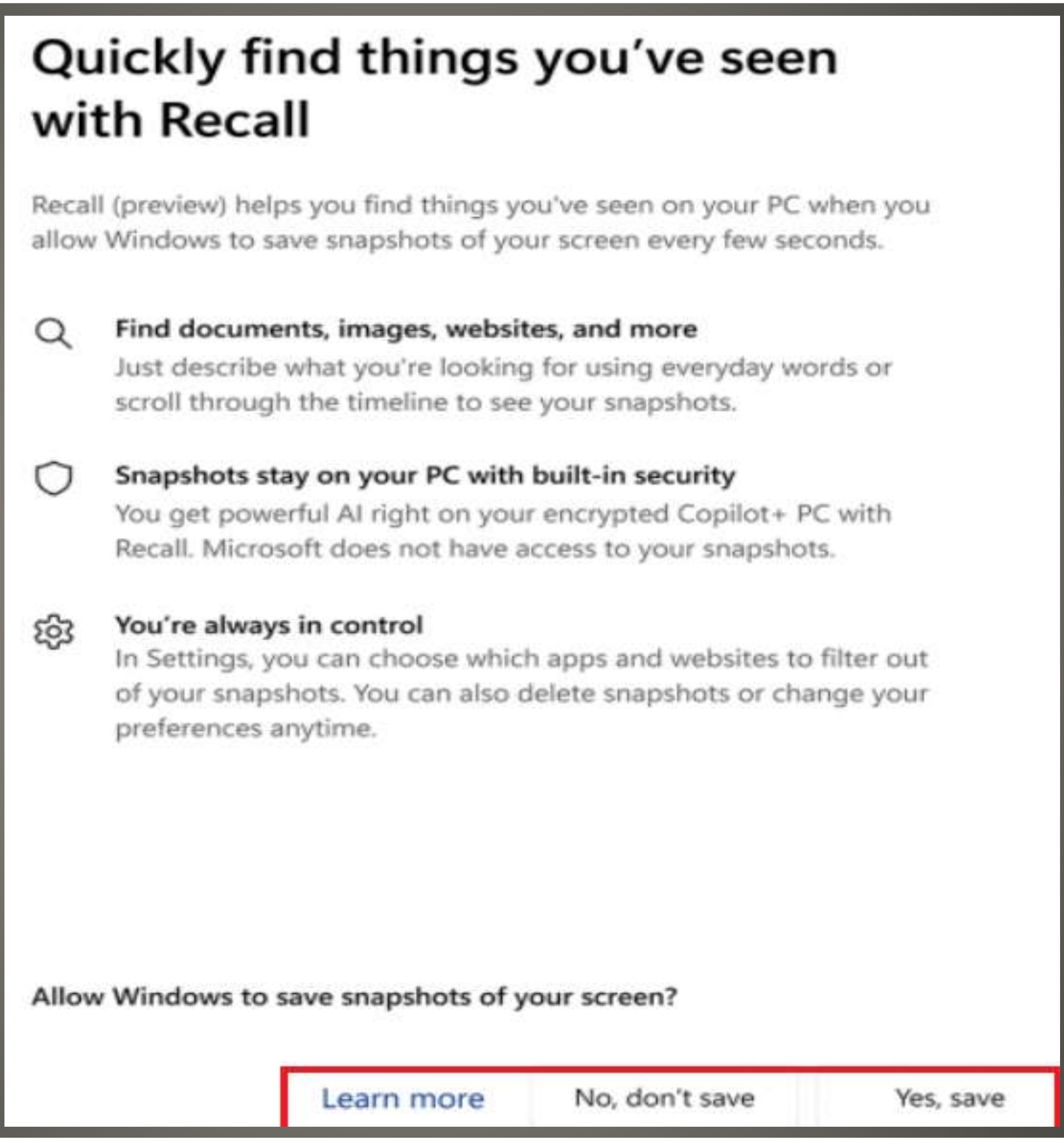


Making sure it's you

Sign in with Windows Hello to use Recall.

Hello, Bret Anderson!
Select OK to continue.

Recall



Quickly find things you've seen with Recall

Recall (preview) helps you find things you've seen on your PC when you allow Windows to save snapshots of your screen every few seconds.

Find documents, images, websites, and more
Just describe what you're looking for using everyday words or scroll through the timeline to see your snapshots.

Snapshots stay on your PC with built-in security
You get powerful AI right on your encrypted Copilot+ PC with Recall. Microsoft does not have access to your snapshots.

You're always in control
In Settings, you can choose which apps and websites to filter out of your snapshots. You can also delete snapshots or change your preferences anytime.

Allow Windows to save snapshots of your screen?

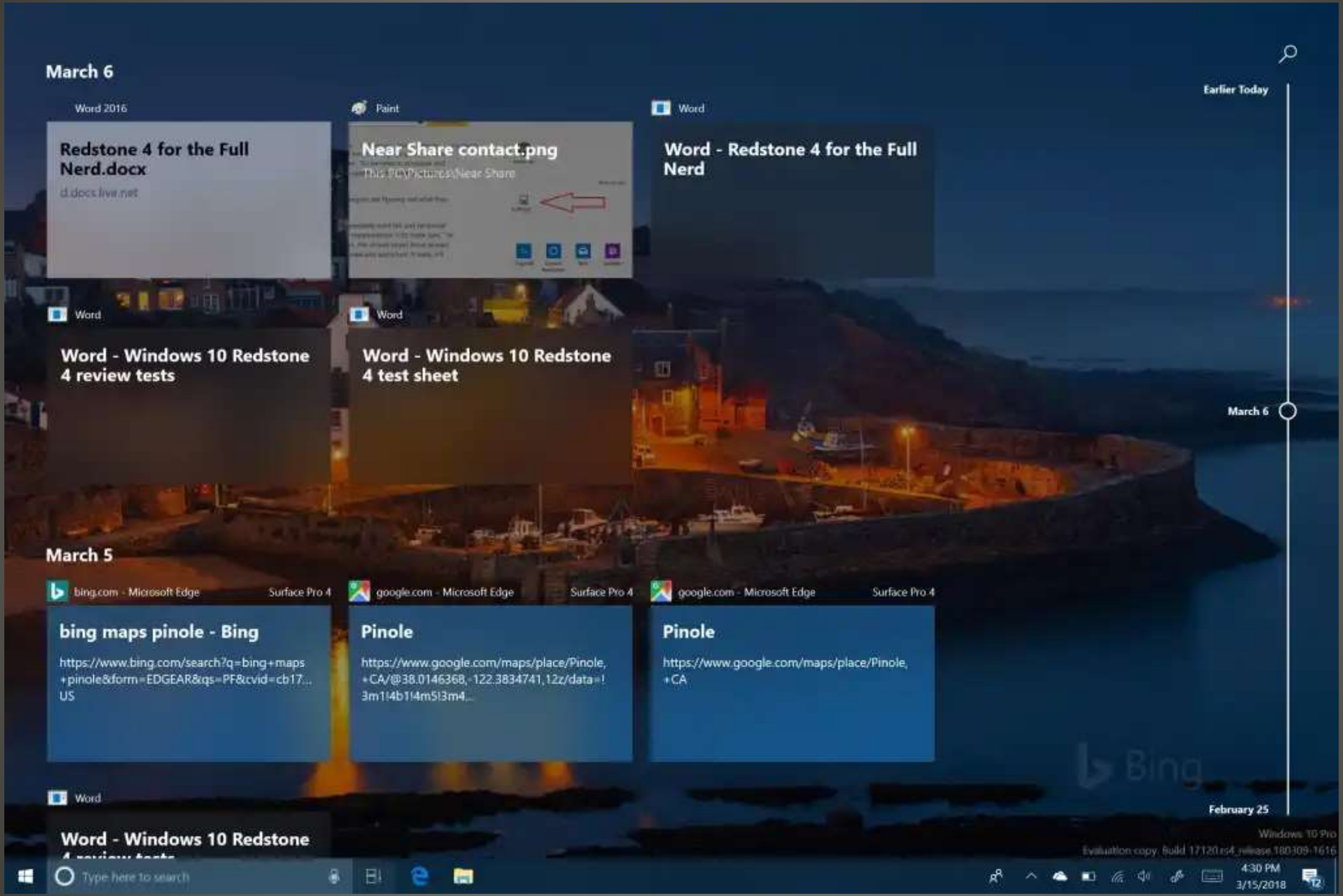
Windows 11
Recall
10:13 PM
Yesterday
Today

- Open-Source Recall equivalent
- Cross Platform Windows, Linux, macOS

- OpenRecall captures your digital history through regularly taken snapshots, which are essentially screenshots. The text and images within these screenshots are analyzed and made searchable, allowing you to quickly find specific information by typing relevant keywords into OpenRecall. You can also manually scroll back through your history to revisit past activities.

- If Microsoft recall gives you pause …
- A third party ….

OpenRecall



March 6

Word 2016

Redstone 4 for the Full Nerd.docx

d.docs.live.net

Paint

Near Share contact.png

This PC\Pictures\Near Share

Word

Word - Redstone 4 for the Full Nerd

Word

Word - Windows 10 Redstone 4 review tests

Word

Word - Windows 10 Redstone 4 test sheet

March 5

bing.com - Microsoft Edge Surface Pro 4

bing maps pinole - Bing

https://www.bing.com/search?q=bing+maps+pinole&form=EDGEAR&qs=PF&cvid=cb17... US

google.com - Microsoft Edge Surface Pro 4

Pinole

https://www.google.com/maps/place/Pinole,+CA/@38.0146368,-122.3834741,12z/data=!3m1!4b1!4m5!3m4...

google.com - Microsoft Edge Surface Pro 4

Pinole

https://www.google.com/maps/place/Pinole,+CA

Word

Word - Windows 10 Redstone

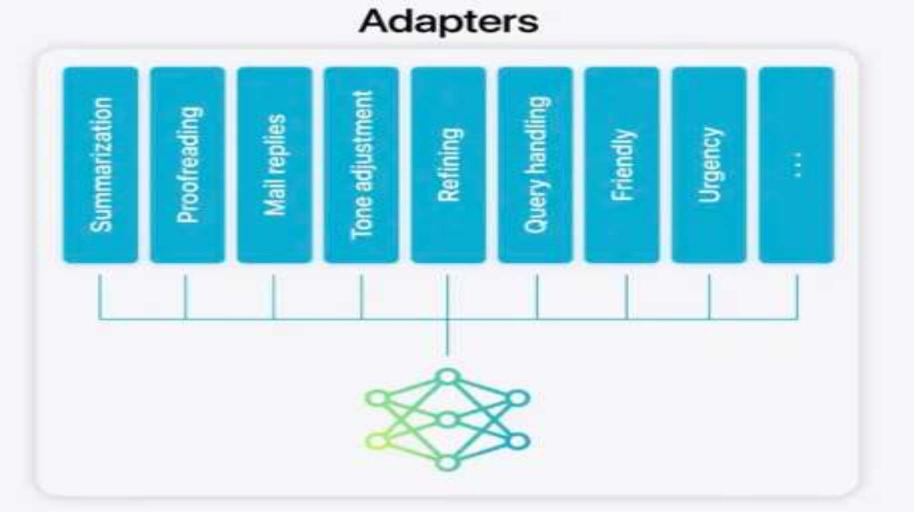
Windows 10 Timeline

- In iOS 18, Apple Intelligence is codenamed Graymatter. There are references to a waitlist, with specific strings that say "Join the Graymatter Waiting List" and "Joined Waitlist." There is also wording that refers to it as a "limited preview."
- "While Graymatter is in limited preview, you may experience unusually slow responses when not in a supported region."
- Apple Intelligence is free for users and will be available in beta as part of iOS 18, iPadOS 18, and macOS Sequoia this fall in U.S. English.

Apple Intelligence

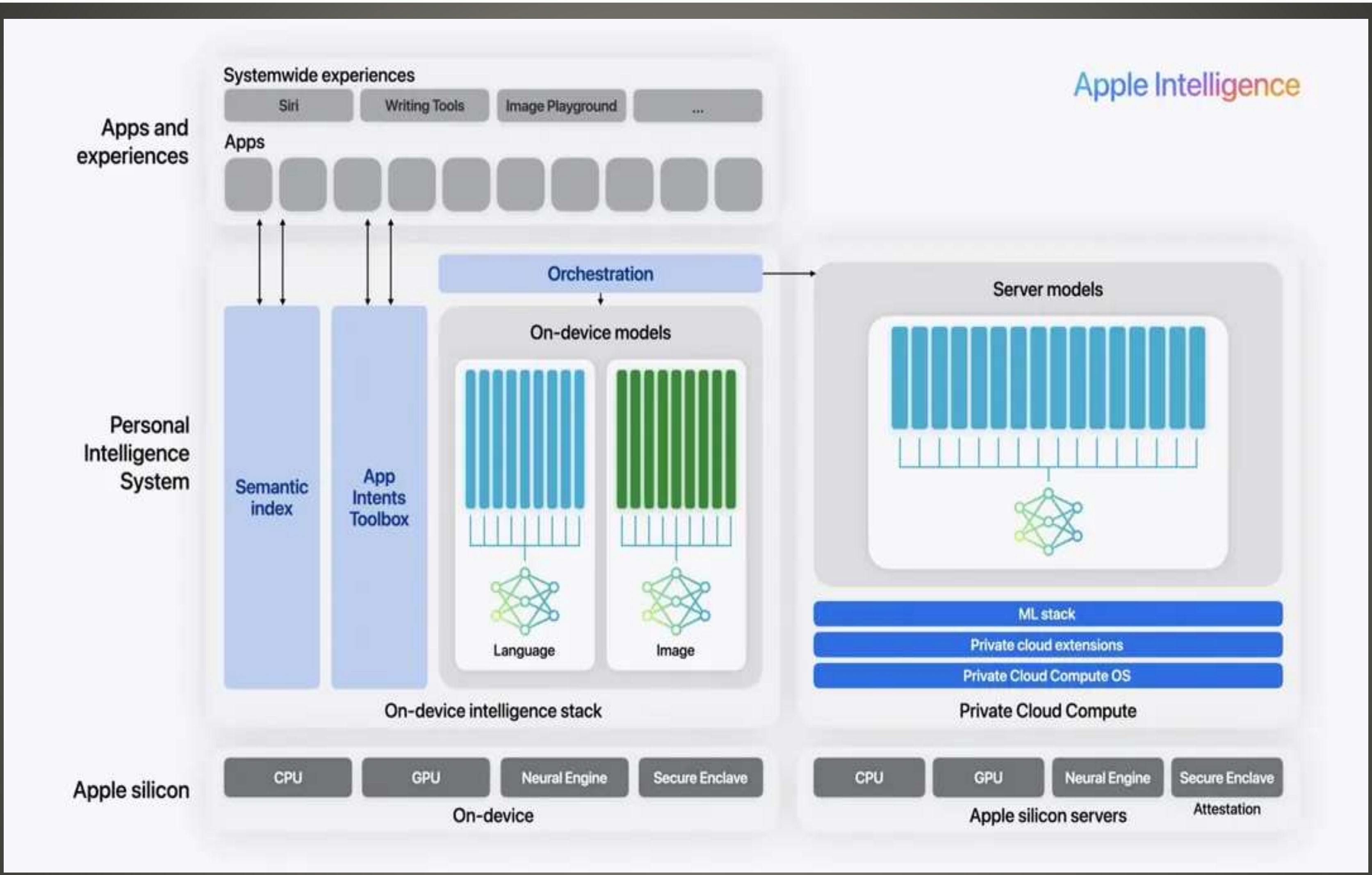
Apple Intelligence

- Local Adapters



- Speculative Decoding
- Context Pruning
- Group Query Attention

NPU Required
M-Series macs & iPads iPhone 15 Pro & Pro Max



Apple Intelligence

- Private Cloud Compute servers
- Own OS iOS foundations - no shell
- Secure Boot Secure Enclave encryption keys/device
- Trusted Execution Monitor signed & verified code can run
- No persistent storage
- Orchestration – Cloud or Local
- ChatGPT with user permission

Apple Intelligence

- Apple will not share Apple user data with OpenAI
- OpenAI will not train its models with Apple user data

Apple and OpenAI

- On Device
- Secure cloud infrastructure private to individual
- Users content & data

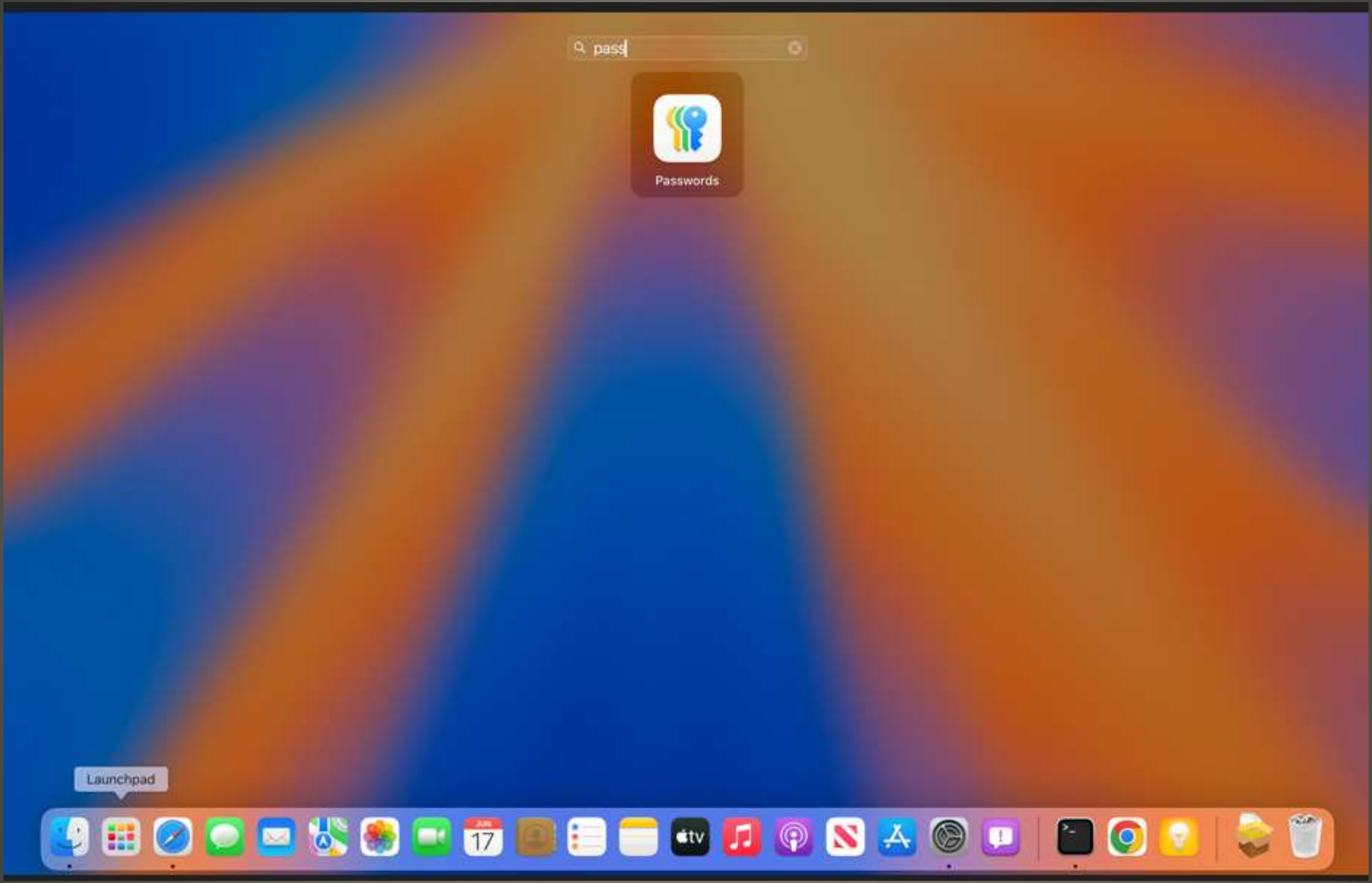
AND

- User can grant permission to access ChatGPT 4o

- Apple Intelligence   Siri Intelligence   Siri Intents

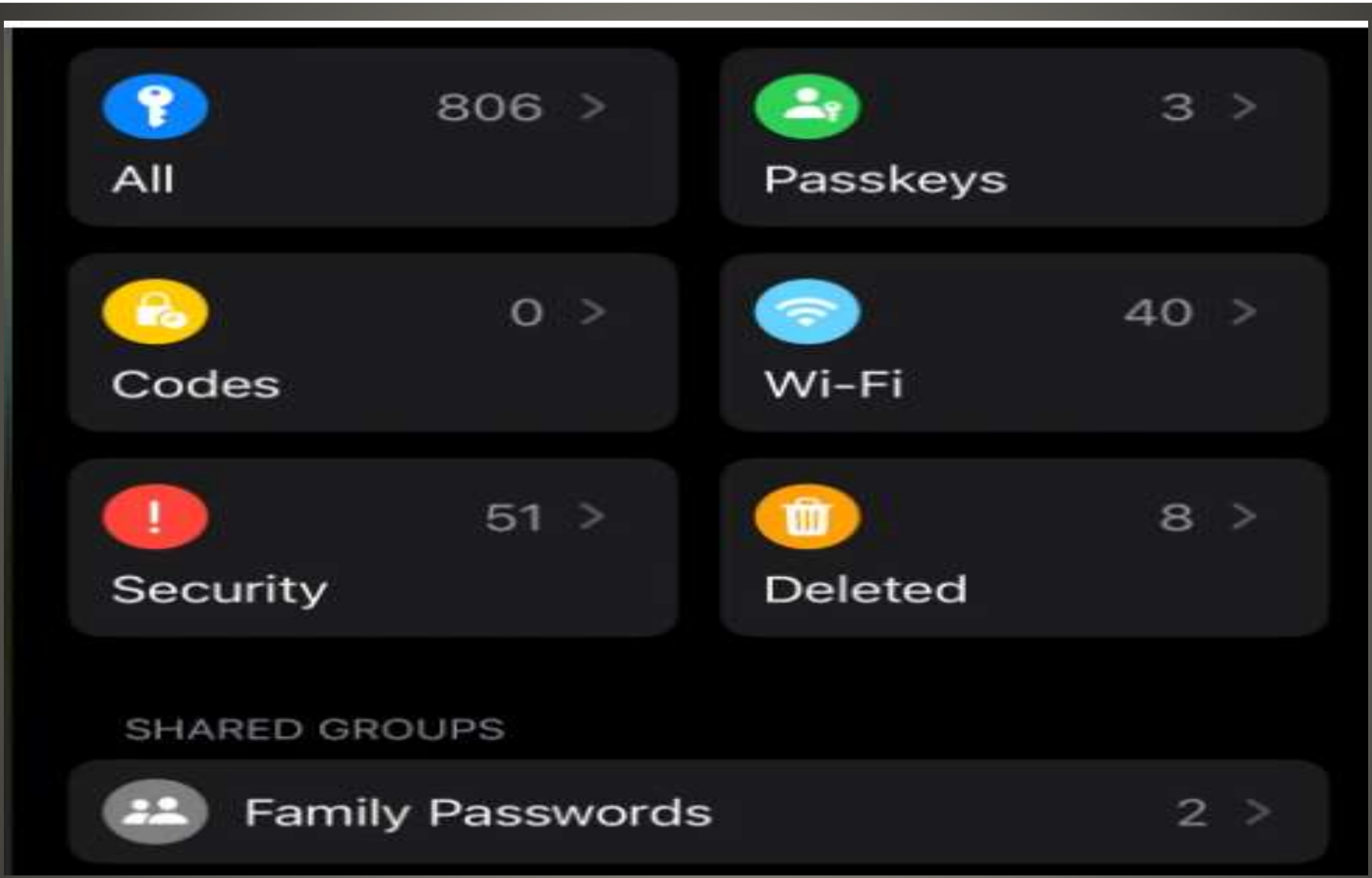
Apple Intelligence

Apple Password



- Passwords App locked
- Import Passwords? .csv format
- Should not replace existing passwords
- Ability to review saved passwords
- Enable Password Notifications?
- View saved credentials
- Manage Passkeys
- Create rotating verification codes
- Review saved Wi-Fi logins
- Receive alerts for passwords in compromised data leaks
- Family Passwords

Apple Passwords



Apple Password

- Apple Devices
- AND iCloud Windows App

- Not offered:

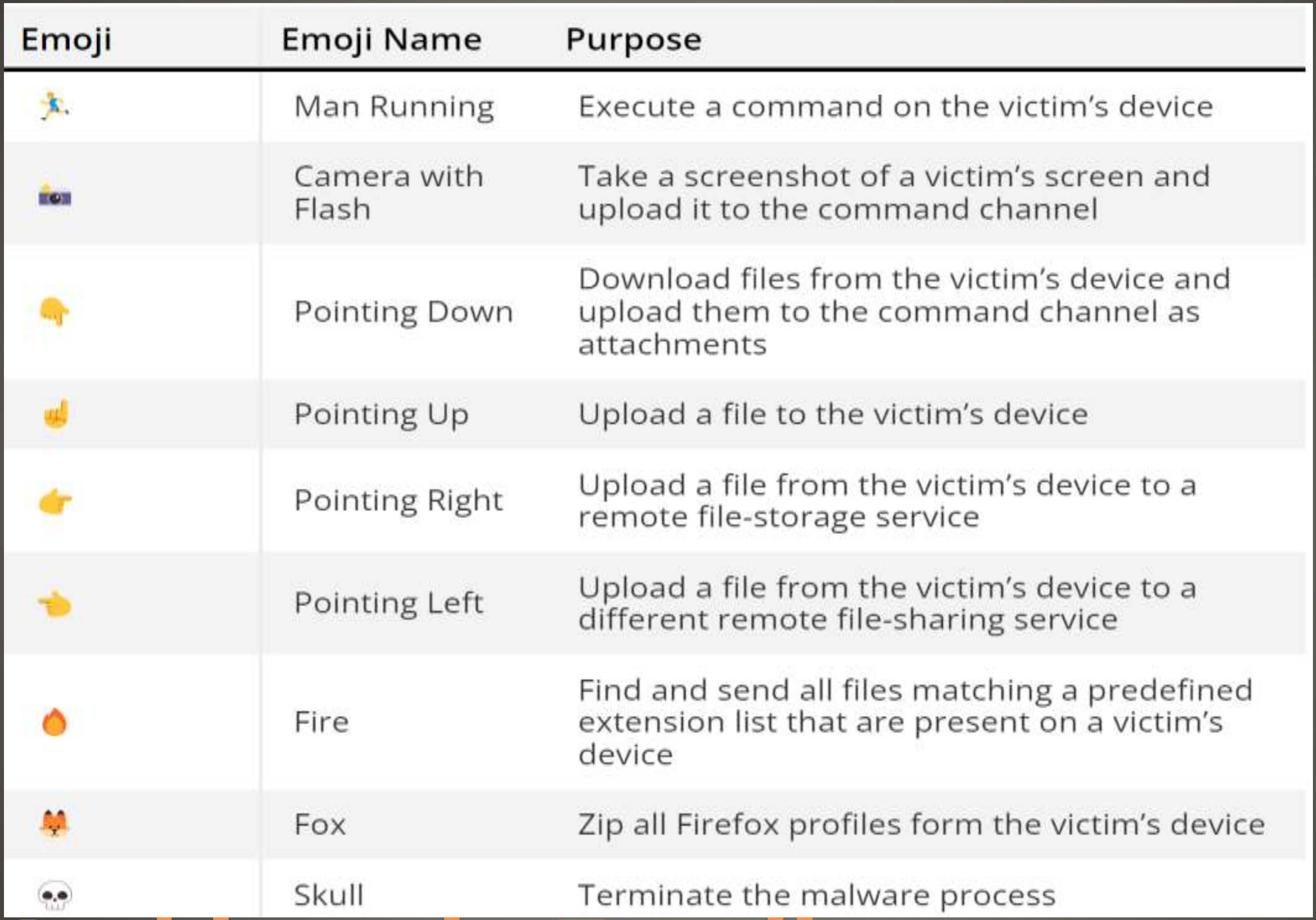
  secure notes

  Cross Browser authentication

  2-factor authentication

Apple Password

Hacking via Emojis



Emoji	Emoji Name	Purpose
🏃	Man Running	Execute a command on the victim's device
📸	Camera with Flash	Take a screenshot of a victim's screen and upload it to the command channel
👇	Pointing Down	Download files from the victim's device and upload them to the command channel as attachments
☝	Pointing Up	Upload a file to the victim's device
👉	Pointing Right	Upload a file from the victim's device to a remote file-storage service
👈	Pointing Left	Upload a file from the victim's device to a different remote file-sharing service
🔥	Fire	Find and send all files matching a predefined extension list that are present on a victim's device
🦊	Fox	Zip all Firefox profiles form the victim's device
💀	Skull	Terminate the malware process

- Microsoft Wi-Fi driver remote code execution vulnerability CVE-2024-30078

Crafted network packet

Public Wi-Fi

Windows 10, Windows 11, Windows Server 2008 & onward

Patched June 11

Windows 7, 8.1

UPDATE HIGHLY RECOMMENDED!!!

- Cencora notifying affected individuals Feb 21 attack
  23 pharmaceutical & biotech companies
- Truist Bank confirms October data breach
  65,000 names, account numbers, transaction history, balance
  Source code for interactive voice response system
- FTC files suit against Adobe
  Early termination fees Difficult to cancel

Current Issues

- AWS to require MFA for privileged accounts
- Microsoft security related changes to Outlook
  Secure Future Initiative
  deprecate basic authentication   Mid-September
  deprecate Outlook Light
  end support for Mail & Calendar apps
  end access to Gmail through Outlook.com
  Outlook/Hotmail/Live.com
- Synnovis breach UK pathology service provider
  Hundreds of users impacted
- Ascension acknowledges personal data stolen
  May attack, June 12 disclosure
  1 employee downloaded malware
- Key Tronic reports cyber incident

Current Issues

- Globe Life data breach
  Disclosed after regulator query
- LA County Public Health data breach
  200,000 PII
  Stolen employee credentials
  All access   No Alerts
- Asus router firmware updates June 14
  And D-Link
- Scattered Spider suspected ringleader arrested
- Insider threat fired employee deleted 180 virtual servers
  IT, Security, HR, Legal
- CDK car dealerships cyber attack
- Findley Auto Group last week
- AMD cyber attack

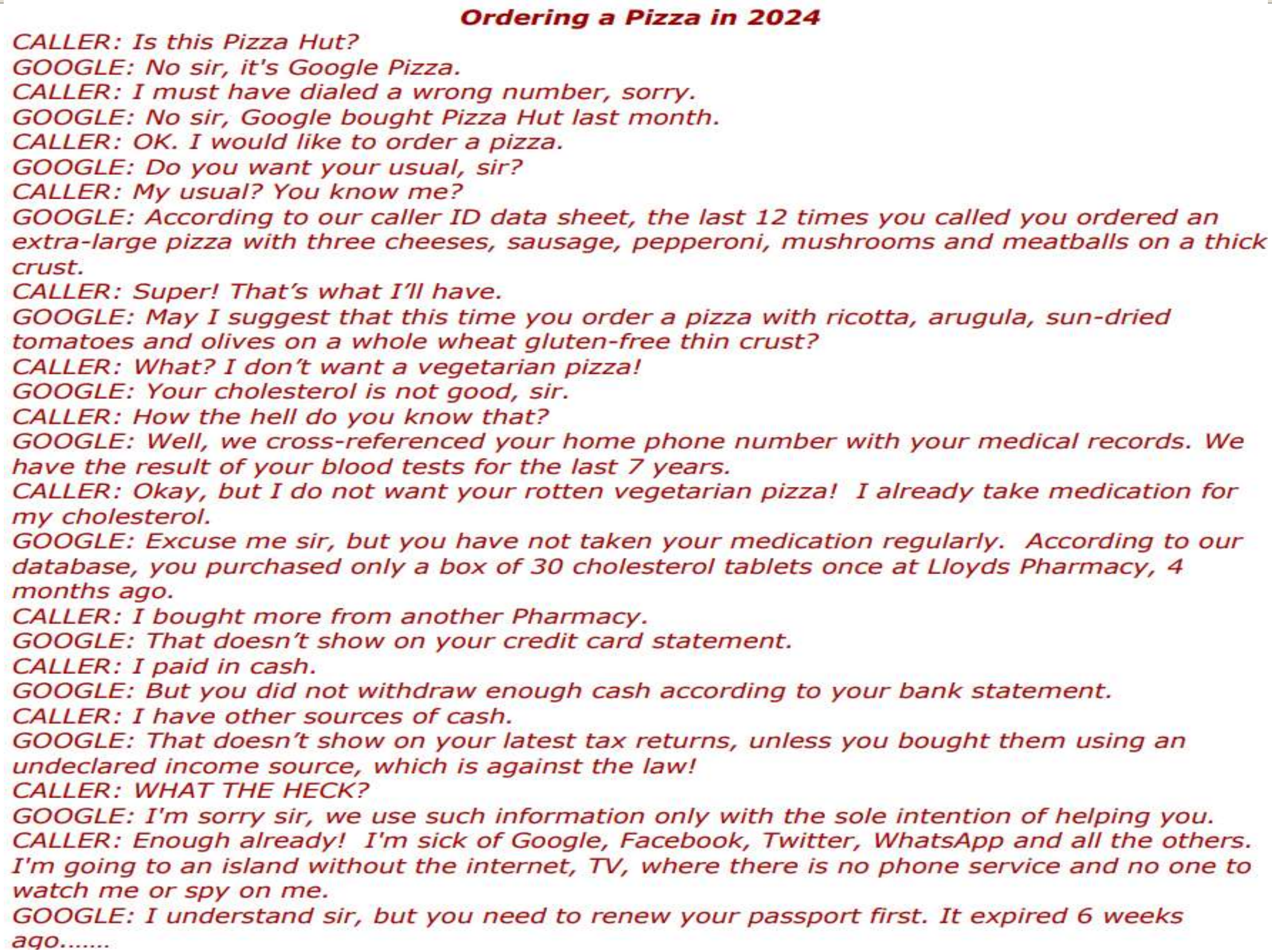
Current Issues

- Kraken Crypto Exchange $3M stolen
- Smart guessing 87 million passwords 60 seconds
  Trained on known passwords
- Chase Bank wire fraud
  Consumer Financial Protection Bureau
  6 figure transfer
  Out of country
  Bank of America refused transfer
- Accenture data breach
- Biden executive order to Ban Kaspersky Anti-Virus in US
  September 29
- UK Total Fitness leaking personal images & private data
  Unprotected membership database
  And their children

Current Issues

Current Issues

- New AI company Safe Superintelligence Inc.
- Roblox 4D Generative AI
- Canal+ French sports broadcaster
  DNS providers Google, Cloudflare, Cisco
  Block 117 pirate sports streaming services



Ordering a Pizza in 2024

CALLER: Is this Pizza Hut?

GOOGLE: No sir, it's Google Pizza.

CALLER: I must have dialed a wrong number, sorry.

GOOGLE: No sir, Google bought Pizza Hut last month.

CALLER: OK. I would like to order a pizza.

GOOGLE: Do you want your usual, sir?

CALLER: My usual? You know me?

GOOGLE: According to our caller ID data sheet, the last 12 times you called you ordered an extra-large pizza with three cheeses, sausage, pepperoni, mushrooms and meatballs on a thick crust.

CALLER: Super! That's what I'll have.

GOOGLE: May I suggest that this time you order a pizza with ricotta, arugula, sun-dried tomatoes and olives on a whole wheat gluten-free thin crust?

CALLER: What? I don't want a vegetarian pizza!

GOOGLE: Your cholesterol is not good, sir.

CALLER: How the hell do you know that?

GOOGLE: Well, we cross-referenced your home phone number with your medical records. We have the result of your blood tests for the last 7 years.

CALLER: Okay, but I do not want your rotten vegetarian pizza! I already take medication for my cholesterol.

GOOGLE: Excuse me sir, but you have not taken your medication regularly. According to our database, you purchased only a box of 30 cholesterol tablets once at Lloyds Pharmacy, 4 months ago.

CALLER: I bought more from another Pharmacy.

GOOGLE: That doesn't show on your credit card statement.

CALLER: I paid in cash.

GOOGLE: But you did not withdraw enough cash according to your bank statement.

CALLER: I have other sources of cash.

GOOGLE: That doesn't show on your latest tax returns, unless you bought them using an undeclared income source, which is against the law!

CALLER: WHAT THE HECK?

GOOGLE: I'm sorry sir, we use such information only with the sole intention of helping you.

CALLER: Enough already! I'm sick of Google, Facebook, Twitter, WhatsApp and all the others. I'm going to an island without the internet, TV, where there is no phone service and no one to watch me or spy on me.

GOOGLE: I understand sir, but you need to renew your passport first. It expired 6 weeks ago.......

- 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