Sun City Computer Club

Cyber Security SIG

September 21, 2023

Questions, Comments, Suggestions welcomed at any time

Even Now

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

Audio Recording In Progress

SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law

Ask ~~Me~~ Anything

- September 21, 2023 3:00Ask Anything
- Consider: An Ask Anything as a zoom session.
- An invite to all Computer Club members. BUT the answers come from the attendees as well as the questions. We have a lot of experience from the members. Let us put that experience together.

- Georgetown Police warn of Phone scam
-

- Georgetown police warning residents about phone scam
- By FOX 7 Austin Digital Team Published 1 hour agoFOX 7 Austin
- GEORGETOWN, Texas - The Georgetown Police Department is warning residents about a recent phone scam.

- Scammers may be claiming that they are Chief Cory Tchida or that they are with Georgetown police and that you have a warrant and need to pay a fine over the phone.

- GPD says this is a scam and they will never ask residents for money over the phone.

Cyber Security News Archive

- Thursday, September 14, 2023
- Security Updates for A LOT
- The severe security vulnerability has been addressed for a lot of things, like browsers, messaging applications, LibreOffice, Affinity, Gimp, many Android applications, any and everything that uses library codes to render WebP images.

- Chrome 116.0.5846.187 for Mac or Linux
- Chrome 116.0.5845.187/.188 for Windows

- Mozilla Firefox 117.0.1; Firefox ESR 102.15.1; Firefox ESR 115.2.1; Thunderbird 102.15.1; Thunderbird 115.2.2

- Edge 116.0.1938.81

- Brave 116.0.1938.81

- Consider viewing the update page for your major apps.
- Also check the mobile platforms: Android, Apple, and others

- And Linux.

- Apple updated their platforms a few days ago. Including the beta releases yesterday.

- Then visit the Microsoft Store and Apple Stores for updates.

- Then major apps for their update mechanism.

Cyber Security News Archive

- Tuesday, September 12, 2023
- Google Chrome Browser issues Critical Update for security Vulnerability September 12
- Goggle has released a critical update to its Chrome Browser to address a severe security vulnerability being exploited in the wild.
- Details are being withheld - implying the severity and scope of the recommended update to the Chrome browser.
- Recommended Chrome version for Windows 116.0.5845.187/.188
- Recommended version for macOS and Chrome 116.0.5845.187

Cyber Security News Archive

Current Browser Versions

- Edge Version 117.0.2045.36 (Official build) (64-bit)
- Brave Version 1.58.129 Chromium: 117.0.5938.88
- Chrome Version 117.0.5938.89
- Firefox Version 117.0.1
- Vivaldi 6.2.3105.48
- DuckDuckGo 0.53.1
- Safari 16.6
- Safari 17

- Multiple email, browser, platforms
  Bank accounts
  More and more are requesting back info
  Create another back account for ONLY those
  Multiple credit cards
  Consider bill pay services
- Caesars pays ransom $30M
- MGM also hit with ransomware
  No slots, no room keys, no fun
- iPhone 12 – France SAR level tests
- Dubai mall parking – Find My Car
- Google Authenticator Cloud synch
- LastPass – MOVE Crypto Funds

Current Issues

- T-Mobile account “leakage”
  Summer 2021 100 million customers
  October 2021 another personal info breach
  January 2023 37 million yet another
  May 2023 again

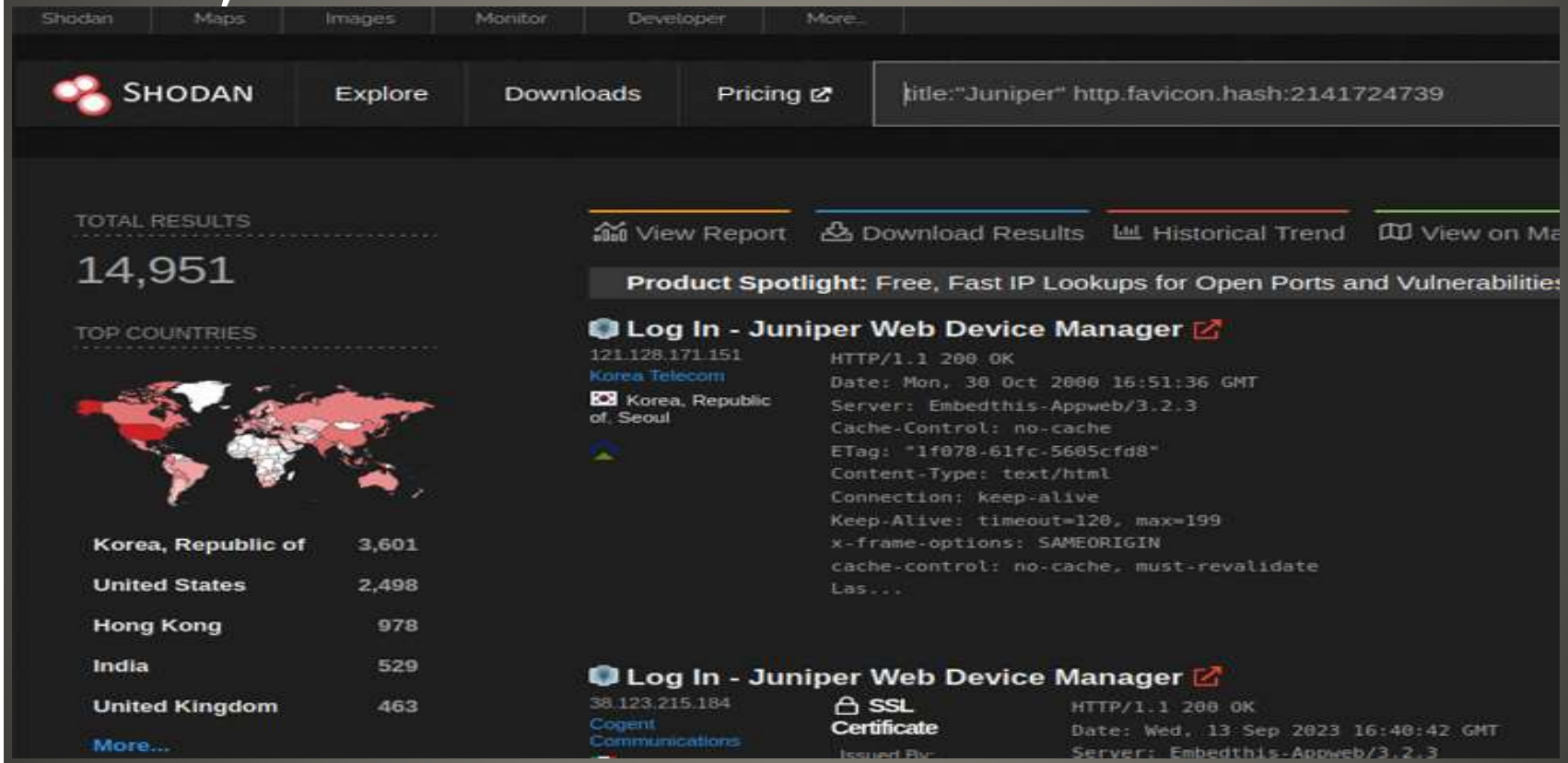
We'll get to the bottom of what information you're seeing through your app and ensure everything is correct. Please send a DM so we can sort this out and ensure your information continues to stay protected. ^CharlesOpacki https://t.co/8DIvLVByJj

— T-Mobile Help (@TMobileHelp) September 20, 2023n SSN

Leaked info: credit card details, home address, purchase history, current credit balance

Changes to new leak every 15 minutes

- Juniper Firewalls RCE vulnerability 12,000



Current Issues

- iOS 17, iPadOS 17, tvOS 17, watchOS 10
- Notification tone change
  Tri-tone > Rebound

Apple

Computer Club SIG news

- Scams and Computer Safety
  Vimeo post
- Apple SIG October 11 8:30 Retreat
- Beginners SIG 25-Sep 2:00 Annex

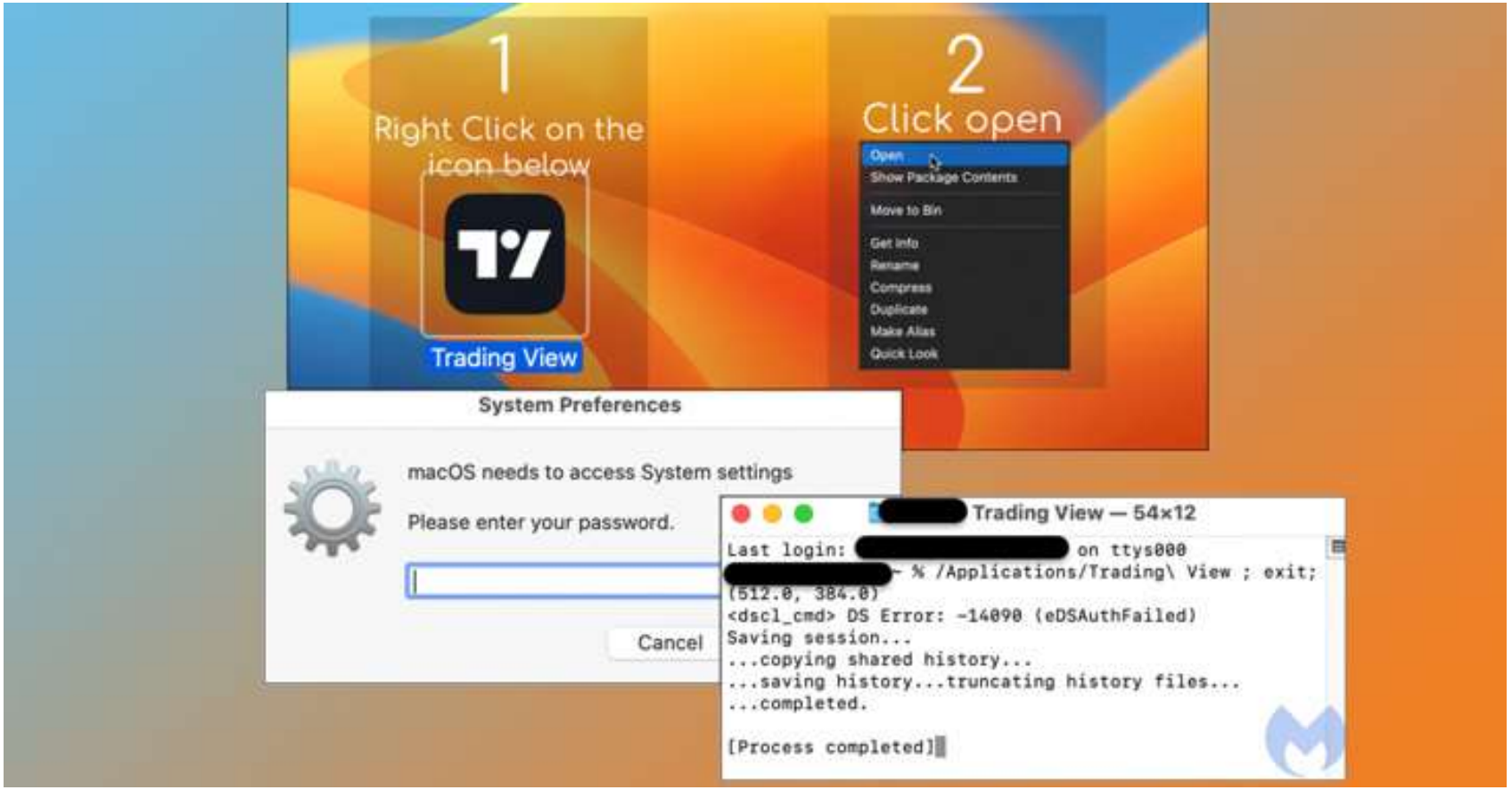
Computer Club Announcements
SIG email lists
Facebook

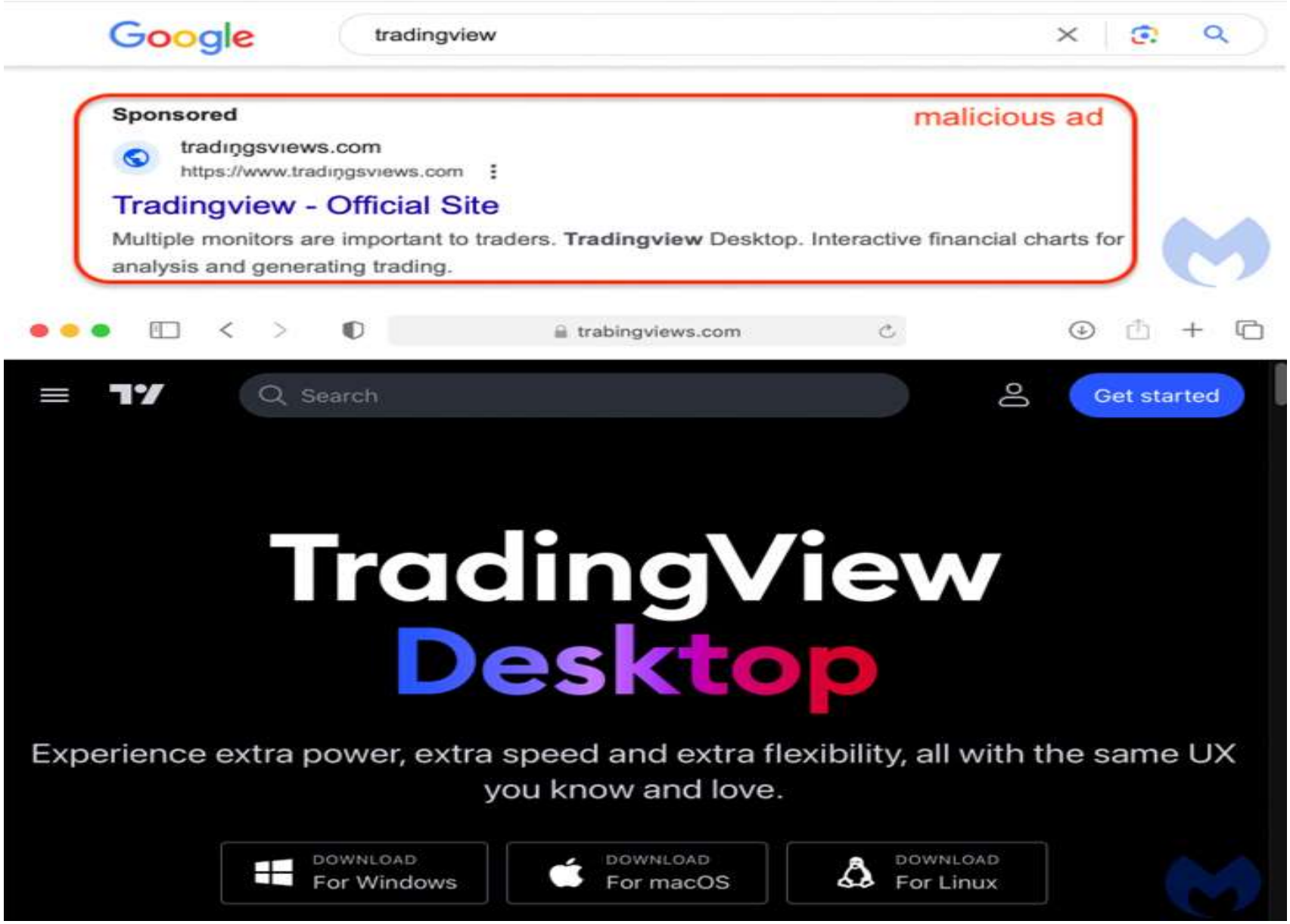
Chrome real-time phishing protection

- Safe browsing feature
- Was local list of URLs
- Enhanced Safe browsing feature
- Now cloud based list of URLs
- URLs you open sent to Google for checking
- Privacy concerns
- Better protections – Less privacy

- Azure Cloud Storage
- Stolen Microsoft Accounts
- LastPass vault

Microsoft Azure hacked


1
Right Click on the icon below
Trading View
2
Click open
Open
Show Package Contents
Move to Bin
Get Info
Rename
Compress
Duplicate
Make Alias
Quick Look
System Preferences
macOS needs to access System settings
Please enter your password.
Cancel
[redacted] Trading View — 54×12
Last login: [redacted] on ttys000
[redacted] % /Applications/Trading\ View ; exit;
(512.0, 384.0)
<dscl_cmd> DS Error: -14090 (eDSAuthFailed)
Saving session...
...copying shared history...
...saving history...truncating history files...
...completed.
[Process completed]


Google
tradingview
Sponsored
malicious ad
tradingsviews.com
https://www.tradingsviews.com
Tradingview - Official Site
Multiple monitors are important to traders. Tradingview Desktop. Interactive financial charts for analysis and generating trading.
trabingviews.com
Search
Get started
TradingView
Desktop
Experience extra power, extra speed and extra flexibility, all with the same UX you know and love.
DOWNLOAD For Windows
DOWNLOAD For macOS
DOWNLOAD For Linux

macOS

- More and More macOS malware
- Targeting Chrome & Firefox browsers
- Search result manipulation

- Atomic Stealer
- TradingView download

macOS

Current Issues

- IRS to use AI
- ChromeOS Lacros browser
  Now you see it, now you don't
  chrome://flags/#lacros-support
  chrome://flage/#lacros-primary
- VPN services 144 surveyed
  70% failed GDPR protections
  trackers
  no opt out
  logs
  payment methods
  location

VPN

- Free, unreliable VPN services
- Provider location(s)
- Overestimating VPN privacy safeguards
- No Logging
- Torrenting
- Kill switch

- Privacy Policy

Privacy Policy

- Microsoft confidential documents
- FTC vs Microsoft
- Court documents

- Many many Cloud mis-configurations

- CPB to stop buying location data
  End of September
  Other agencies?

- Automobiles

Privacy Ours Theirs

Digital Will

- Apple
  Legacy Contact
- Facebook
  Legacy Contact

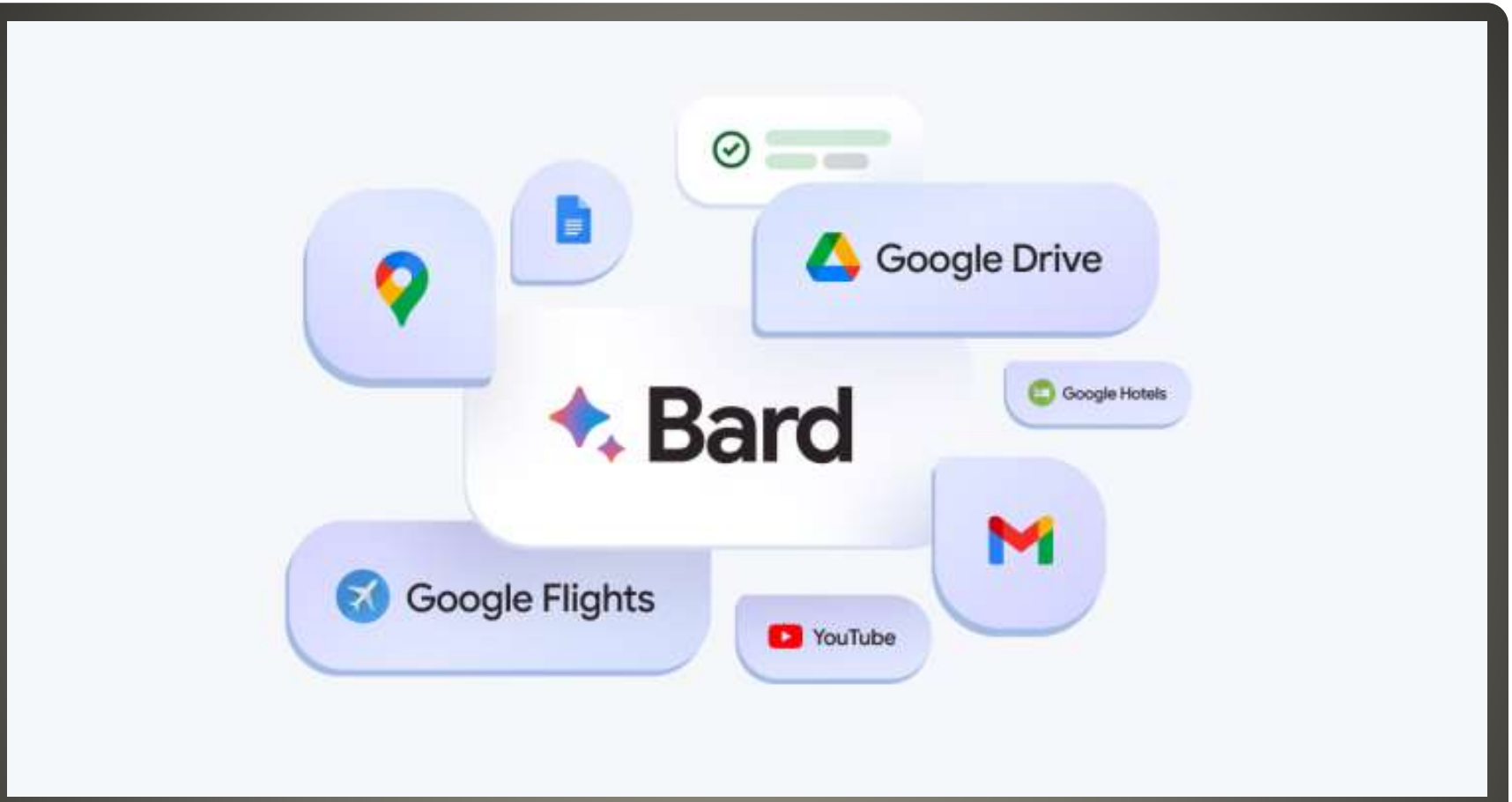
Multiple email accounts

- Spam avoidance burner email addresses
- Reduce clutter
- Better security
- Identity separation

Current Issues

- HTTPSnoop malware
  Remote Code Execution
  Microsoft HTTP kernel drivers
  Specific HTTP(s) URLs
  PipeSnoop arbitrary shell code named pipe
  ShroudedSnooper
- SprySOCKS
  Linux backdoor
- Cryptojacking for uncommon AWS services
- Amazon Echo Frames

- What can Alexa on your face do?
- What can a radio on your face do?
- *Alexa, where are my glasses?*



Google Bard

Microsoft AI researchers

- Terabytes of sensitive data
- Exposed by accident
- Yet another cloud mis-configuration

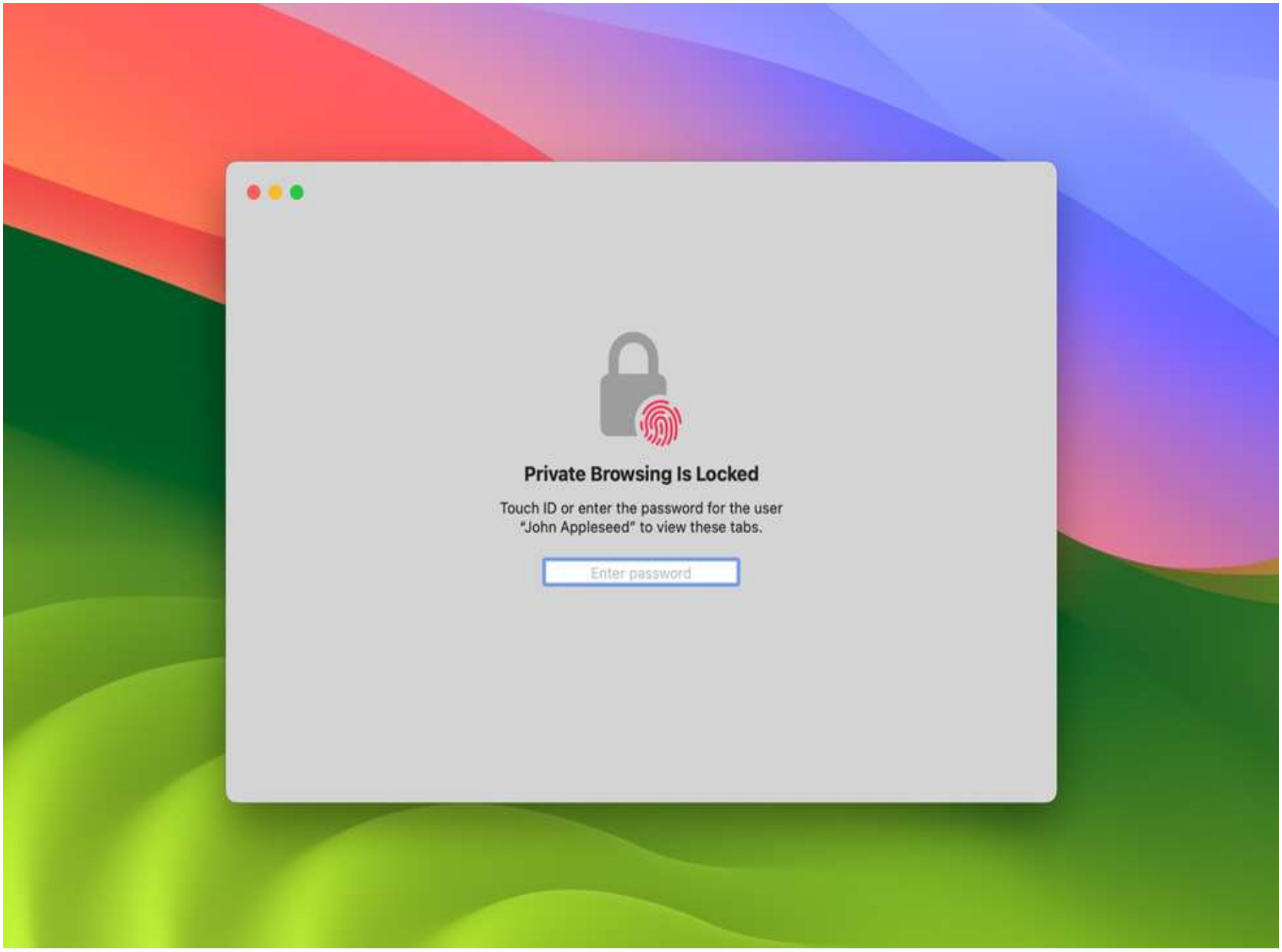
- Personal backups of 2 Microsoft employees
- Microsoft services passwords
- Secret keys
- Internal Microsoft Teams messages
- Full Control

- Opt-in EXPERIMENTAL features
- Automatic memory reclaim
- Sparse VHD
- Mirrored mode networking
  IPv6, multicast, improved VPN,
- DNS tunneling
- Hyper-V firewall
- autoProxy
- WSLg

Microsoft Subsystem for Linux

Signal App

- Update from X3DH
  - Elliptic Curve Diffie-Hellman
  - Asymmetric encryption
  - Public – Private key pair
- Post Quantum Cryptography
- PQXDH
  - X3HD + CRYSTALS-Kyber
  - NIST proposed standards

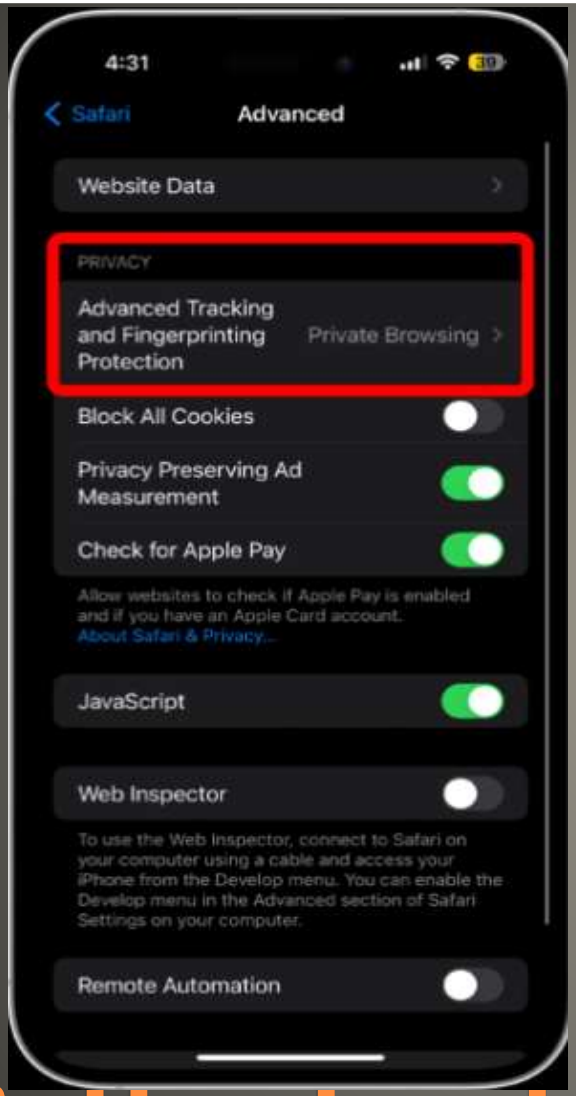

Private Browsing Is Locked
Touch ID or enter the password for the user
“John Appleseed” to view these tabs.
Enter password

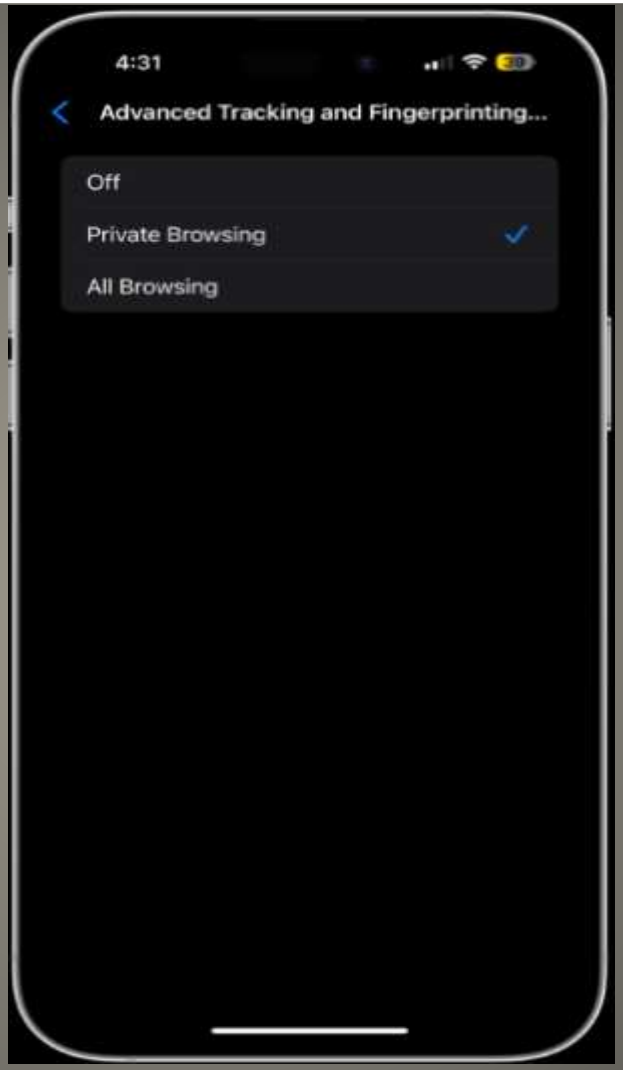
Lock Private Safari Windows

- Private Browsing
  - Browsing Details are NOT saved
  - Web sites visited are NOT shared with other Apple devices
    - iOS Safari
  - Require Face ID to unlock Private Browsing
    - Sonoma
  - Touch ID or password

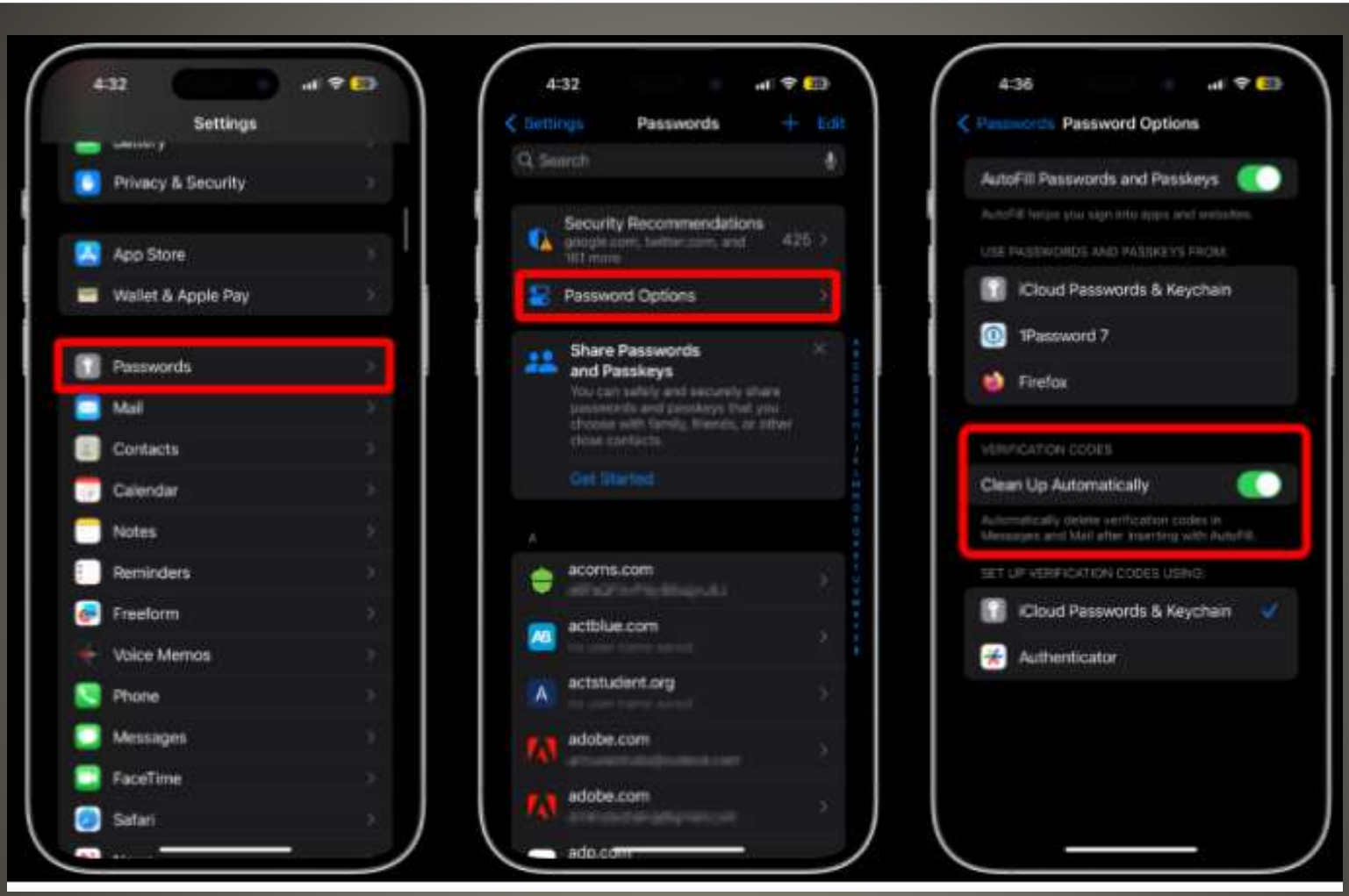
Private Browsing

- BROWSER ONLY usually
- NOT DNS
- NOT ISP
- NOT system/application/firewall/security suite logs





Better tracking prevention



Auto-delete verification codes

- Apps with Photos permissions
- 6 months or longer
- Prompt

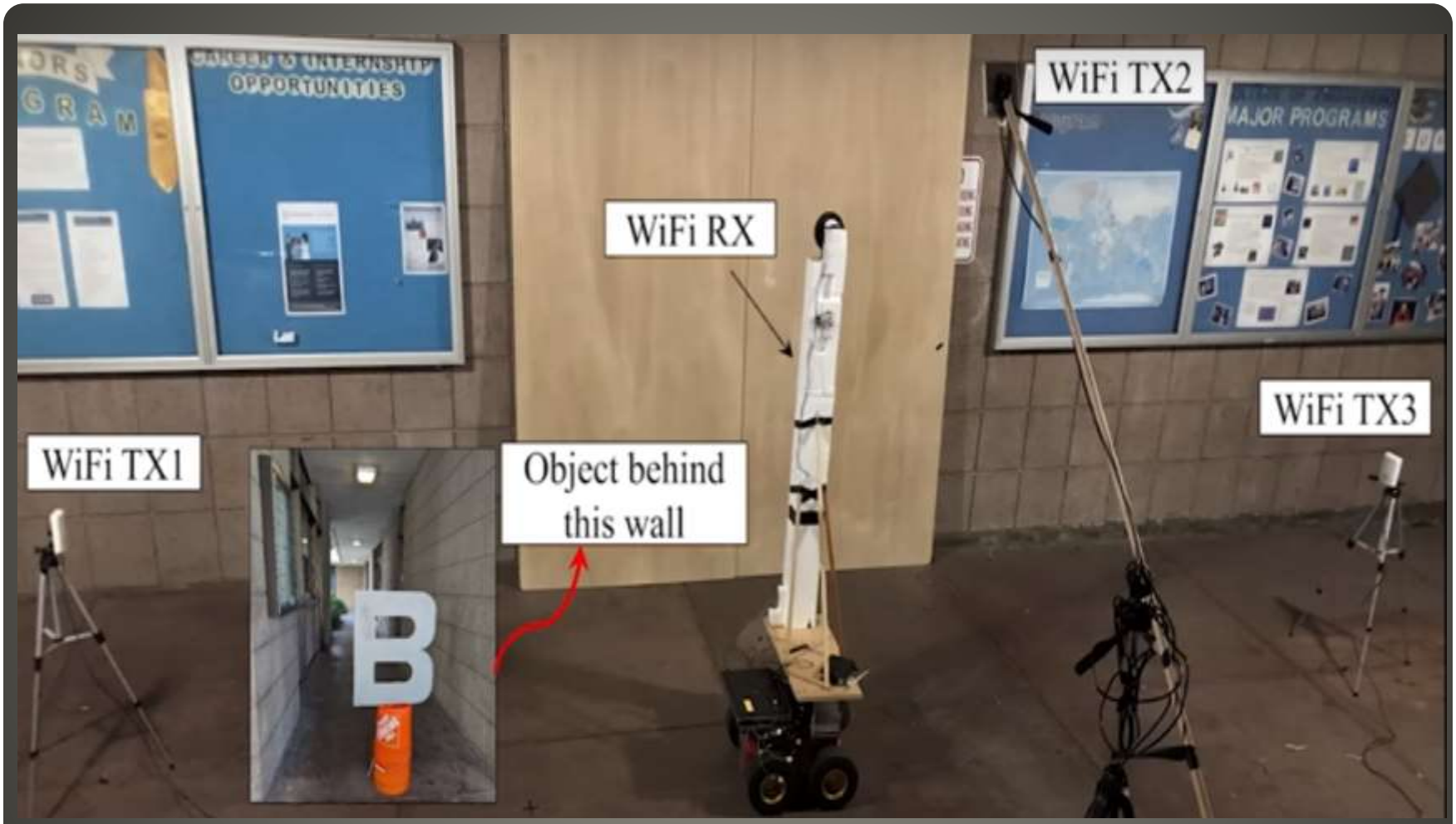
NEW photos privacy permissions

- Linux macOS
- April patch macOS

ncurses library vulnerability

Current Issues

- Windows 11 NTLM attacks over SMB
- Windows 10 OneNote Text translations November?



Wi-Fi can "read" through walls

Letters behind the wall

Our Imaging Results

*Wooden background only for demonstration purposes and not part of imaging setup

**Letters were imaged one by one.

Current Issues

- OpenAI launches DALL-E 3
- GitHub coding copilot now widely available
- Toyota Research Institute
  teach robot new skill overnight
- RenderIH reads and interprets human hand movements
- PII request remove from data brokers
  for a fee
- Generative AI Act 2
- Bard “double check”
- Google “Take a deep breath”
- Google “think step by step”
- Transform voice recordings to summarized notes
- FBI & CISA joint warning Snatch
  Ransomware as a service

Amazon & Alexa futures

- *Alexa, let's chat*
- Eye Gaze Mode hands & Voice free
- Call translation Alexa audio & video calls
- Alexa Emergency Assist
  At-Home Hands Free
  Urgent Response
  Smart Alerts
  Emergency Contacts
- Game Start routines - favorite teams
- Email family calendar
  email, invite, photo of event
  Extract, add to calendar, send confirmation
- Top Connections
- Profile-level voice customization
- AI art on Fire TV
- Wi-Fi mesh
- Ring stick-up Cam Pro - Radar based 3-D motion detection

Microsoft Futures

- AI copilot
- Outlook “sound like me”
- New Surface products
- September 26
- Windows 11 23H2
- Image Creator tool
  Content Credentials watermark

AI vs AI

- Your experiences??

- How to Remove Known Networks on iOS (nerdschalk.com)

How to remove Wi-Fi network names iOS

- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

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

- Questions, suggestions, comments?

SCCCCyber@gmail.com