Sun City Computer Club

Cyber Security SIG
May 2, 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)???

New Leader???

- Cyber Security News Blog/Archive
- Announcements
- Message Board
- Computer Club Wiki
- Scams and Computer Security SIG
- Anti-Fraud Town Hall 6-May-2024
  Ballroom 8:30 09:00 – 11:00

- Edge Version 124.0.2478.67 (Official build) (64-bit)
- Chrome Version 124.0.6367.119 (Official Build) (64-bit)
- Firefox Version 125.0.3
- Brave Version 1.65.126 Chromium: 124.0.6367.118
- Tor 13.0.14 (based on Mozilla Firefox 115.10.0esr)
- Vivaldi 6.7.3329.24
- DuckDuckGo 0.78.1
- Safari 17.4.1 (19618.1.15.11.14)

Current Browser Versions

- Hacker free-for-all fights for control of home and office routers everywhere
- How and why nation-state hackers and cybercriminals coexist in the same router botnet.
- Read in Ars Technica:
- https://apple.news/AVv7ens0rTYeoXLrK_fsOzA

Member Contributed

Current Issues

- LastPass call Press 1 to stop attacker
  Follow-up call
  "We will check it for you, your account info?"
  Site shutdown April 16
- FBI warning Chinese Hackers & US Infrastructure
  Volt Typhoon
- Frontier Communications cyber attack
- Palo Alto firewalls
- Microsoft VASA-1
  still image + cloned voice + text script > video of person talking
- SEC sued New Civil Liberties Alliance (NCLA)
  Consolidated Audit Trail (CAT)
  Capture and send detailed information on every investor's trades in U.S. markets to a centralized database. Paid for with fees. Fourth Amendment violation

Facebook users warning

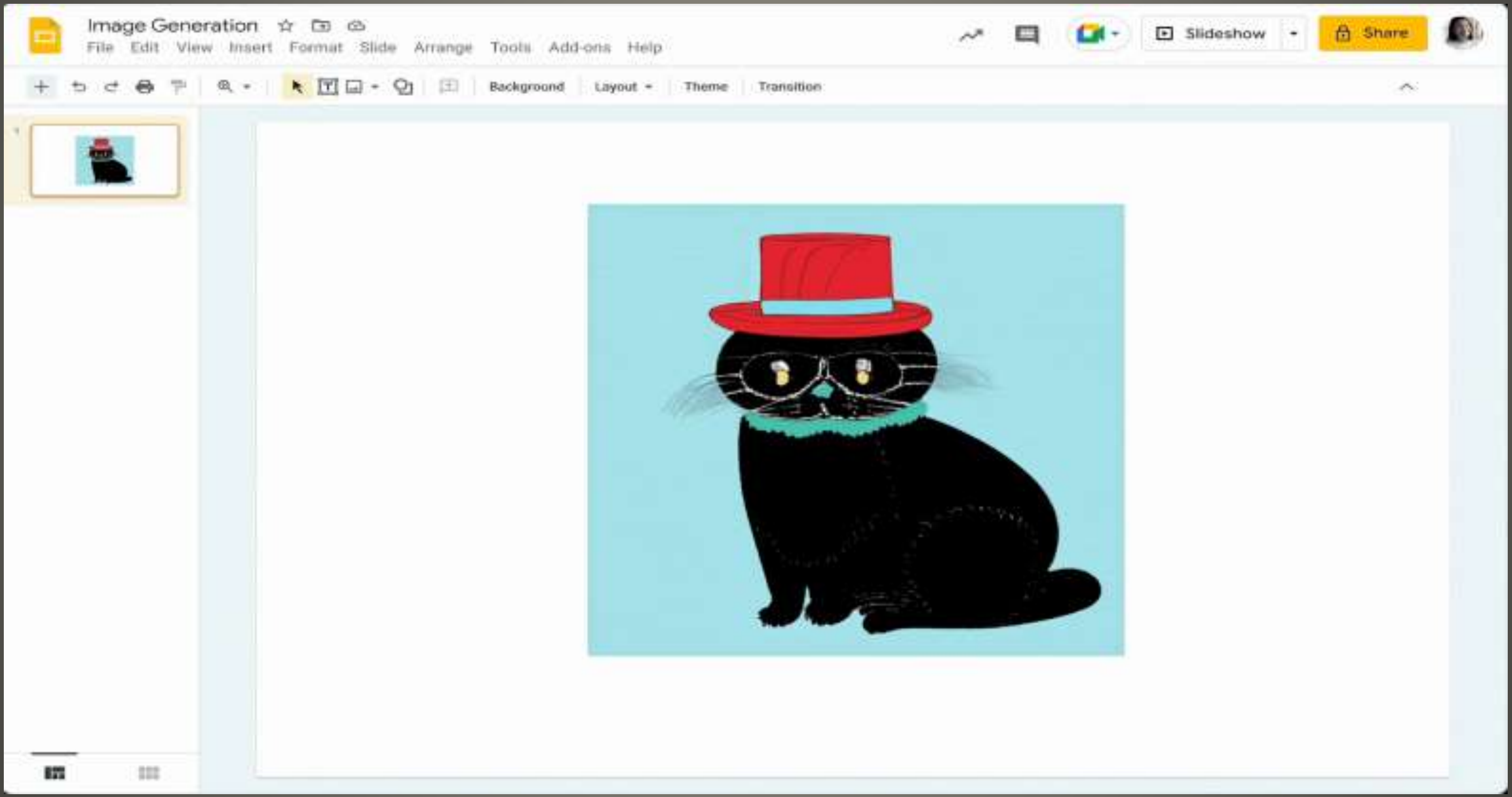
- Bitdefender report:
- Fake Facebook page for Mindjourney
- 1 million Facebook followers
- Hacker takeover
- Infostealer
- Also: Sora Ai, Dall-E 3, Evoto, ChatGPT 5

- AVOID clicking on download links on Facebook

- Section 702 of FISA reauthorized
  Retry 2026
- XZ utilities & Open Source – NOT end of story
- United Healthcare
  Hackers stole some quantity of patient data
  Chase Healthcare hit with second ransomware attack
  Citrix vulnerability in Feb 12 Lockout Feb 21
  One account without MFA
- Sandworm -> APT44
- New U.K cybersecurity law for Internet of Things
  Product Security and Telecommunications Infrastructure Act
  No default passwords, security update requirements, etc.
  April 29, 2024 ETSI
  Criminal offense 4% revenue or £10 million
  US Cyber Trust Mark
- Duo SMS service data breach – customer phone numbers
- World-Check database for future customer screening
  Customer's bank accounts shutdown - no public reason
- Austria arrests former intelligence officer for spying
- Google Device Bound Session Credentials
  defense for stollen session cookies

Current Issues

- HTTP/2 Continuation Frame vulnerability Dos attack
- Goggle Slides -remove background from images

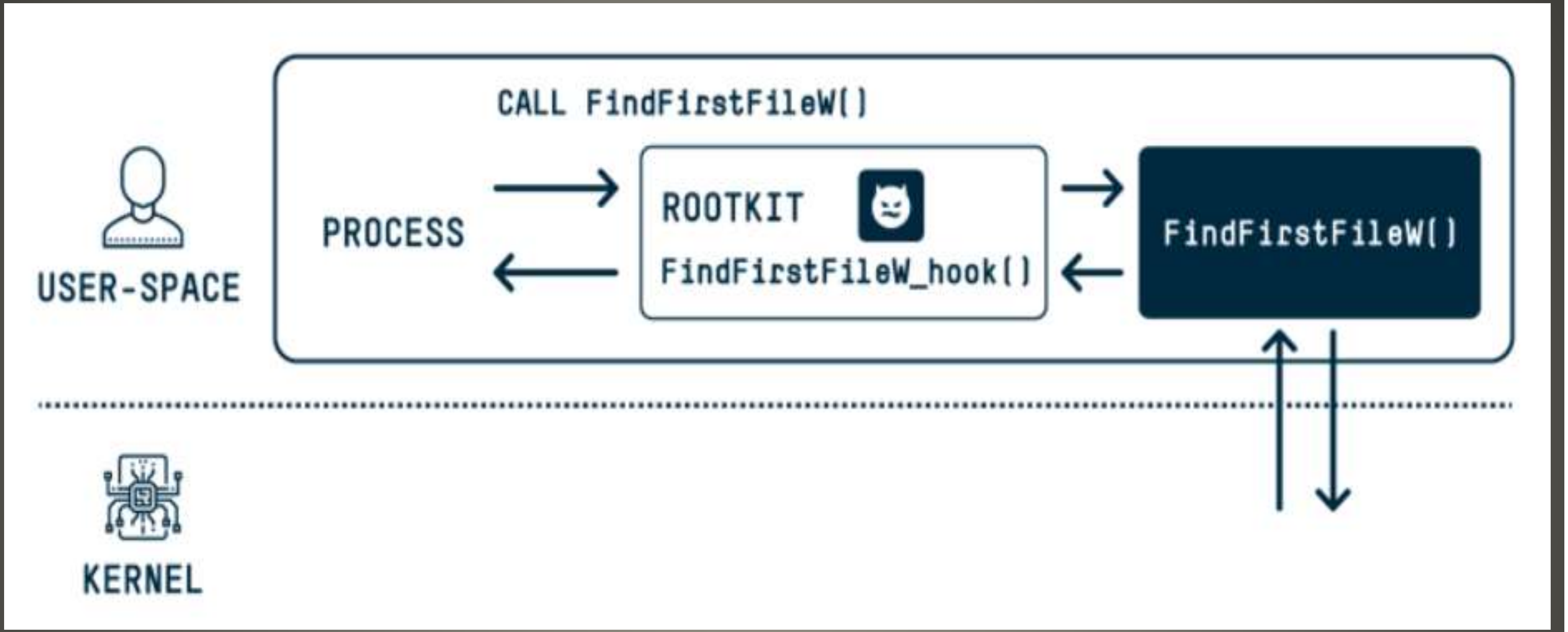


Current Issues

- Home Depot employee’s personal data exposed
- Israeli cyber spy unit head exposed   one error
  Unit 8200
  2021 book *The Human Machine Team* Brigadier General YS
  Amazon copy with email address tied to real name
  One mistake …
- Capture FaceID to fake bank access
- Mona Lisa Rap   Microsoft VASA-1
- AI Image to Text   capture text for access
- Microsoft Print Spooler vulnerability   CVE-2022-38028
  GooseEgg April 2019
- Windows flaw DOS-to-NT path conversion
- Proton Mail Dark Web monitoring

Current Issues

- Windows flaw DOS-to-NT path conversion

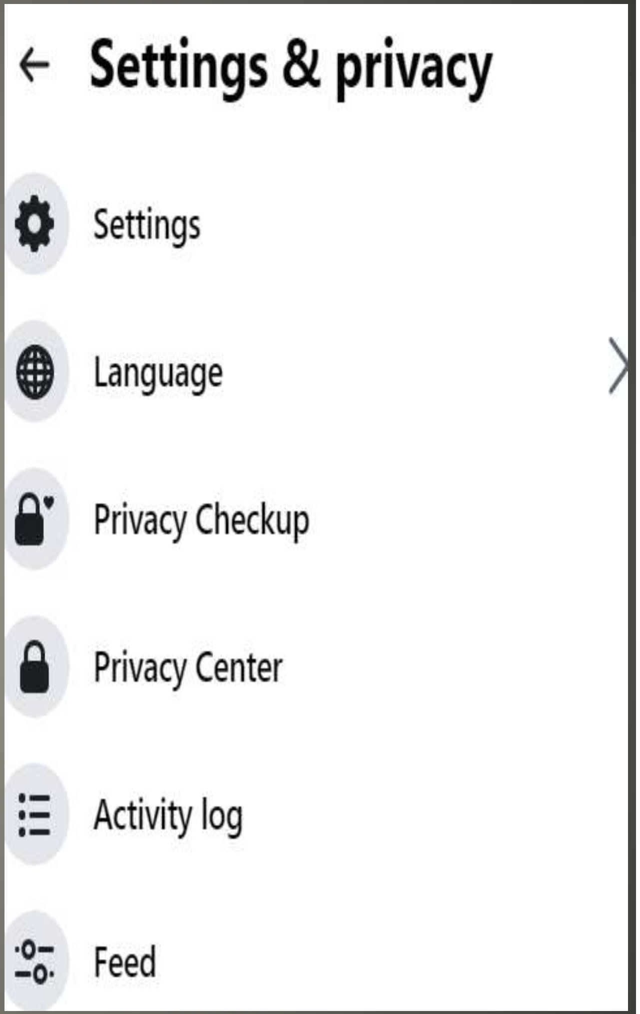


- 4 security issues 3 addressed

Current Issues

Facebook Privacy Settings

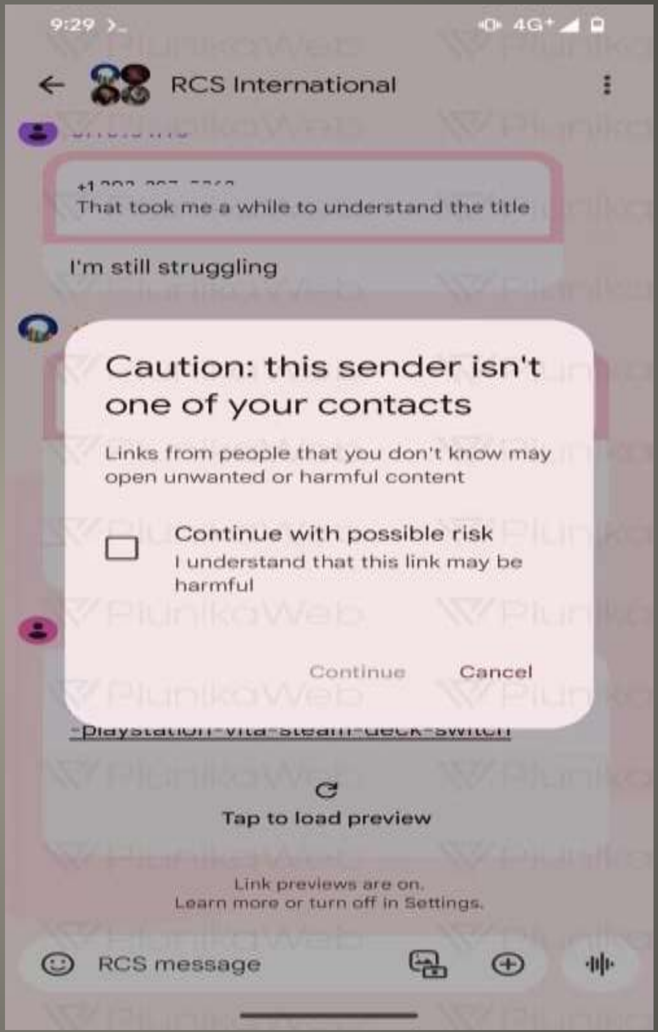
- Facebook Privacy oxymoron?
- Privacy Checkup Tool
- Anyone can create with Your name
- Check and Re-Check
- Profile Visibility
  Audience and visibility
  Profile Details
- Friends List and Searchability
- Posts and Tagging permissions
- Third-Party access
- Ad Preferences and Security Settings



- RCS spammy
- Google disabled RCS for a period of time

Google RCS spam change

- Unknown number
- Apple to add RCS



Google Message RCS Spam

Macs need Anti-virus?

- Anti-virus => Security Suites
- XProtect signature based
  0-day signatures
  Delay in XProtect data
  XProtect data blocked/altered
- Gatekeeper
  Application signing
  Developer's signing certificate compromised
  User able to bypass Gatekeeper
- User Social engineering
  Click through warnings
  "Follow directions"
- Browser protections

Macs need Anti-Virus?

- Resources needed
- Resources used
- Anti-virus can “see” data you can not
- Helpful <-> Harmful
- Rosetta 2 Apple silicon run Intel based code
- Apple silicon Secure Boot vs Intel EFI
- Recovery mode
- Device Firmware Update Mode (DFU)

- Recovery Mode
  Most Apple devices
  Uses bootloader
  Connect to Mac Install iOS/iPadOS
- Device Firmware Update
  Secret handshake
  Corrupt boot loader
- Mac T2 security chip
  Restore using another Mac

Wait, Recovery Mode   DFU?

- Was Mac only
- Apple App Store protections not 100%
- Files loaded from Internet warning
- Files loaded from Internet setting
- Apps can infect post-install
- Discounted Tax return software
- Be Aware

Apps Sideloading

Migraine

- System Integrity Protection (SIP)
- Normal SIP bypass
  - Restart in Recovery Mode
  - Setup
  - Restart   i.e. physical access
- Migration Assistant
- Add exception to SIP exclusion list
- Apple macOS updates
  - Ventura 13.4, Monterey 12.6.6, Big Sur 11.7.7

- Hisense TV
  Random UUIDs for UPNP
  Windows adds all to registry

Smart TV

- eScan AV updates over HTTP
- FCC to restore Net neutrality rules
- Physical access to Android TV can yield access to your entire Google Account

Android designed for Smart Phones – single user

Google centralized account system

(side)load Chrome on TV

ALL Google account access CC, email, browsing history, …

Discard Android TV – Wipe first

Abandonware

Android TV, dongles, set-top boxes, Chromecast

Sign-in hotel room Android TV Airbnb

Logged into Android TV lately? LOG OUT

Account > Security > Manage all devices

Current Issues

Sign out of Gmail remotely

- NUCA cameras remove clothing
  Smart camera in shell
  AI processing in cloud
- Many countries have banned TikTok
- WordPress Automatic CVE-2024-279
  Very Heavy scanning underway
- T-Mobile to use GPS May 8
  and throttling

Home Internet Service Address Validation

Our Home Internet plan is designed to be used at specific addresses in places with enough network capacity to ensure all our customers have good network experiences. Starting May 8, we'll notify customers using Home Internet at a different location than the one they signed up at to either recheck their current address eligibility, move their gateway back to the address they signed up at, or switch to another plan that suits their needs.

- On April 28, customers' originally approved Internet addresses will be visible within the troubleshooting tab in Atlas, along with their current gateway's location.
  - Customers using their gateway at a different address will have a flag displayed.
  - Refer to Address Changes: Home Internet for steps on validating and updating your customer's place of use.

Current Issues

- Godfather banking trojan
  Hundreds of samples AI?
  record screen, keystrokes, 2FA, calls, text
- Kaiser health data share
  Millions of current and former customers
  Data shared with Google, Microsoft, X
  Shared analytics
- WhatsApp to use passkeys on iDevices
- Fingerprint sensors
  Optical, capacitive, ultrasonic
  Optical CCD CMOS
    Accurate, robust, simple
    Spoofing, scanner or finger surface issues
  Capacitive iPhone 5S
    Less susceptible to spoofing movement detection
    Skin sensitivity
  Ultrasonic
    Sound
    Pricy

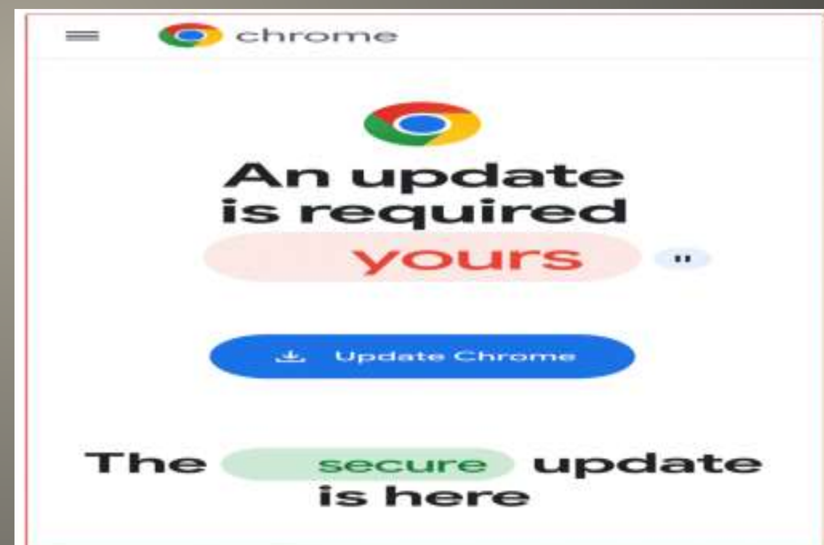
Current Issues

- Cisco Adaptive Security Appliance 2 0-days
- T-Mobile new Account Change Engine

  SIM change notification via SMS   10 minutes to deny auto approved

  SIM change notification via SMS 10 minutes to approve auto deny
- Brokewell Android banking trojan

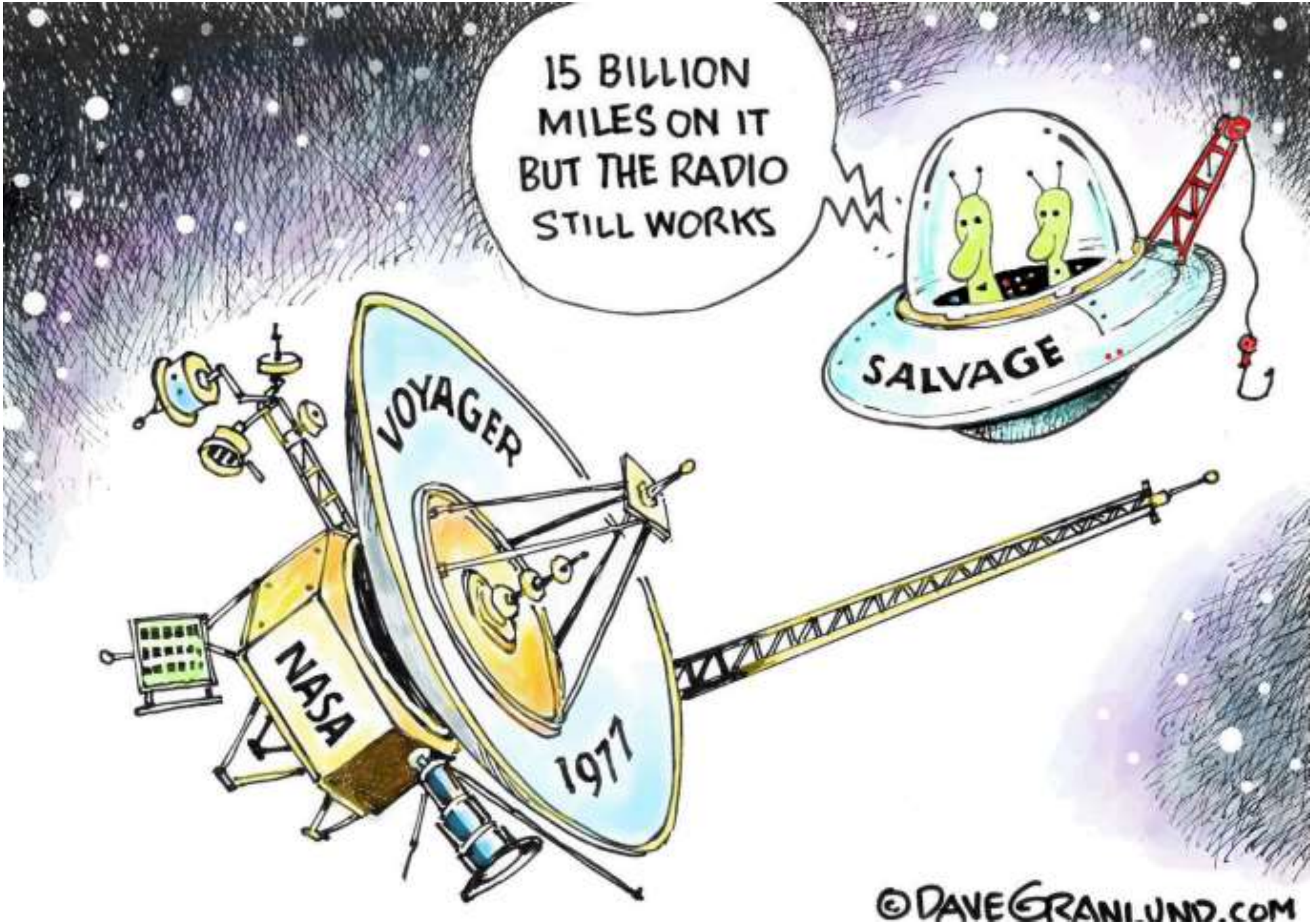
  Fake Google Chrome update



Current Issues

- Tipton, Indiana wastewater treatment plant cyber attack
  April 19 People's Cyber Army of Russia
- Android 15 Private Space feature
  Files and Apps
- Android 15 application quarantine
- iSharing app - too much sharing
- Stuxnet on steroids
  Ukraine security services attack on Russian infrastructure
  Industrial sensor and monitoring physically destroyed remotely
  Excluding hospitals, airports, and civilian targets
- Voyager 1 resumes sending data 22.5 light hours away
  Rework flight data system
- China bans Threads, Signal, Telegram, WhatsApp Apple App store

Current Issues


15 BILLION
MILES ON IT
BUT THE RADIO
STILL WORKS
SALVAGE
VOYAGER
NASA
1977
©DAVEGRANLUND.COM

- Hyundai Bluelink app

  No driver discount   Data sharing declined

  Lexis Nexis – no data

  Verisk - wow

  dates, minutes, braking, acceleration

  Save driving dongles – misinformation

  Hyundai customer service:

"Thank you for contacting Hyundai Customer Care about your security concerns. As a confirmation, we have been notified today that the driver's score feature and all data collecting software has permanently disabled. We do care. As always, if you ever need additional assistance, you can do so either by email or phone. Case number…"

Data Source: Hyundai

Driving Event Summary

Driving Data	Value
Trip Count: Vehicle ignition on to ignition off	242
Speeding Events: Vehicle speed is greater than 80 mph	N/A
Hard Braking Events: Change in speed < -9.5kph/s	24
Rapid Acceleration Events: Change in speed > 9.5kph/s	26
Daytime Driving Minutes between 5AM - 11PM	6,223
Nighttime Driving Minutes between 11PM - 5AM	25
Miles Driven	5,167.60

Daily Driving Log

Date	Number of Trips	Speeding Events	Hard Braking Events	Rapid Acceleration Events	Daytime Driving Minutes	Nighttime Driving Minutes	Mileage
Mar 10, 2024	2	N/A	1	0	32	0	19.74
Mar 09, 2024	2	N/A	0	0	23	0	13.44
Mar 06, 2024	4	N/A	0	1	69	0	46.14
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	41	0	18.14

Hyundai Bluelink

- OnStar
- Smart Driver   Digital Badges
- Owner One data collected   One not
- LexisNexis
- Verisk
- Data unavailable to owner
- Detailed data from data brokers

Number of trips, distance, start/end times, hard braking, rapid accelerations

- High level summary

Miles driven, driving minutes, hard braking, rapid accelerations

- NYT reporter checked – NOT enrolled
- App No   Website Yes   Bug?
- Insurance rate increased
- Screen with details presented   if salesperson showed it

GM

- Salespersons incentives
- Dealership report “sell connected cars”
- Connected Access

OnStar – Yes

Text to customer – yes

GM Insurance product – No

The customer must personally review and accept (or decline) the terms below. **This action is legally binding** and cannot be done by dealer personnel.

Enrollment Preferences

(Smart Driver and Notifications opt-in)

One-click Enroll into OnStar Smart Driver and Notifications

OnStar Smart Driver†

Improve your ownership experience with access to OnStar Smart Driver.

We'll keep you informed about the following:

- Up-to-date information about your driving skills
- Low tire pressure or oil change needed
- Potential maintenance or performance issues
- Service notifications from your dealer
- Theft Alarm Notifications if your alarm is triggered
- Wi-Fi® data running out

Details

By providing an email and opting into notifications, we can keep you informed on the following services and features, based on your vehicle's capability/eligibility:

Diagnostics Report† – reports each month showing you the status of your vehicle's key operating systems.

Diagnostic Alerts† – alerts regarding issues with your vehicle's key operating systems.

vehicle.

Please visit my.cadillac.com for more information about your OnStar and Cadillac Connected Services. You can also change your communication preferences or un-enroll from any of these services at any time on my.cadillac.com or through an Advisor. Messaging and data rates may apply.

By checking "Accept", you will be enrolled in OnStar Smart Driver and we may also send you notifications related to all of the above services.

I Accept: I agree to enroll in OnStar Smart Driver and the notification services listed above.

I Decline: I do not agree to enroll in OnStar Smart Driver and the notification services listed above.

GM

- Smart Driver 2.0

Hard cornering, forward collision alerts, lane departure warnings, seatbelt reminders

- Data about car – GM
- Data about driver – Personal data
- Multiple drivers?
- What are hard braking & rapid acceleration events?
- Speeding over 80 mph (Texas 85 mph)
- LexisNexis GM, Kia Subaru, Mitsubishi
- Verisk Ford, Honda, Hyundai and millions of vehicles

- Request your report(s)
- LexisNexis

https://consumer.risk.lexisnexis.com/consumer

- Verisk

https://fcra.verisk.com/#/

GM

FCRA Disclosure Forms

How to order your free consumer reports. Verisk will provide one free report in any 12-month period.

Important Notice to Consumers regarding Driving Behavior Reports

Verisk no longer receives driving behavior data from automakers to generate Driving Behavior Data History Reports. Verisk no longer provides Driving Behavior Data History Reports to insurers. If you're interested in receiving a copy of your Driving Behavior Data History Report, please click on the link at the bottom of the page. The driving behavior related data Verisk can offer you will vary by auto manufacturer. See table below.

Auto Manufacturer	**Verisk stopped receiving driving behavior data to produce Driving Behavior Data History Reports as of**
General Motors	March 18, 2024
Honda	April 9, 2024
Hyundai	April 9, 2024

- Credit reporting freeze
  Unfreeze without PIN
  Supply information available in data breach
  Unfreeze notification - postal mail?
  Harder to intercept
  https://grc.sc/credit
- GitHub
  Flaw/Design decision
  malware appear Microsoft official code repository
- Dauthi – attack framework against MDM platforms
- U.K Investigatory Powers Bill *Snoopers' Charter*
- EU *Chat Control*
  screen CSAM no exclusion for feasibility
  UK "technically feasible"
  EU "except for us and LE and military and …
- CISA *Ransomware Vulnerability Warning Pilot Program*

Current Issues

- CISA *Ransomware Vulnerability Warning Pilot Program*
  Administrative Subpoena
  No judicial review
  No opt-out / decline
- Muddling Meerkat
  China Great Firewall
- Shein mystery box

Current Issues

AT&T

Dear Customer,

At AT&T, we prioritize the security of our customers' information and are committed to maintaining transparency in all matters related to your privacy and data protection.

We are writing to inform you of a recent security incident involving a third-party vendor. Despite our rigorous security measures, unauthorized access was gained to some of our customer data stored by this vendor. This incident might have involved your names, addresses, email addresses, social security numbers, and dates of birth.

We want to assure you that your account passwords were not exposed in this breach.We have notified federal law enforcement about the unauthorized access.

Please accept our apology for this incident.

To determine if your personal information was affected, we encourage you to follow the link below to log into your account:

Sign In

Thanks for choosing us,

AT&T

- Be careful with download files
- Be careful with uploading files
- Chromium based browsers

Browsers are compute engines
File System Access Application Interface
APIs
Access files on computers to upload
Photos to edit
Files to encrypt for cloud storage
Access your files
Within browser confines
Bypass filesystem and OS protections
Ransomware vector

Upload Cautions

- Do it before **they** do
- Lock out of your access
- During MFA setup
- SMS, Authenticating tokens, Push notifications
- Session cookies
- Centralization Apple, Google, Microsoft
- Adding user, Adding device, Account Recovery
- Registration, identity proofing, authenticators establishment, authentication, recovery-identification, account termination
- Zero-Trust architecture

MFA

- It has happened to me before
- WAIT
- Stolen Device Protections

  Known Location

  Wait Time

Apple Accounts

- CAUTION: Many fake download sites
- Was iOS & macOS
- Now Windows
- The Browser Company
- Chromium engine
  - Swift programming language
  - Weekly Updates
  - .EXE Wants an account created

Arc Browser

- iPhone alarm problem
  “Attention Aware” feature?
- iOS “Ready for Repair” 17.5 beta
- Cuttlefish malware
  Monitor traffic for credentials
- Mysterious AI system detected
  Then removed gpt2-chatbot
  LMSYS.Org benchmarks AI
- Alarming surge in bank Account closures
  Suspicious activity
  Anti money laundering software

Current Issues

- Cutting the Cord

  Alternatives to deliver video/audio content

  https://vimeo.com/749640628

- Cyber Security SIG 21-Mar-2024

  Automatic Content Recognition (ACR)

  Advertisement Identification

- Roku account breach
- Roku advertisement change

Streaming TV 101

- 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