Sun City Computer Club

Cyber Security SIG
April 18, 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

- Cyber Security News Blog/Archive
- Announcements
- Message Board
- Computer Club Wiki

- Xi’s Enigma Machine?

  password-busting quantum supercomputer

  Microsoft digital key stolen / replicated

  CISA 45 theories
- Israel Justice Ministry cyber incident
- Roku ads for third-party connections to Roku TVs on pause
- OmniBridge AI ASL <-> Text
- 4 Open-Source Antivirus for PCs

  MoonSecure

  ClamWin

  Clam Antivirus

  Armadito Anti-virus

Caution Antivirus sees inside files you may not be able to see

Current Issues

Issues

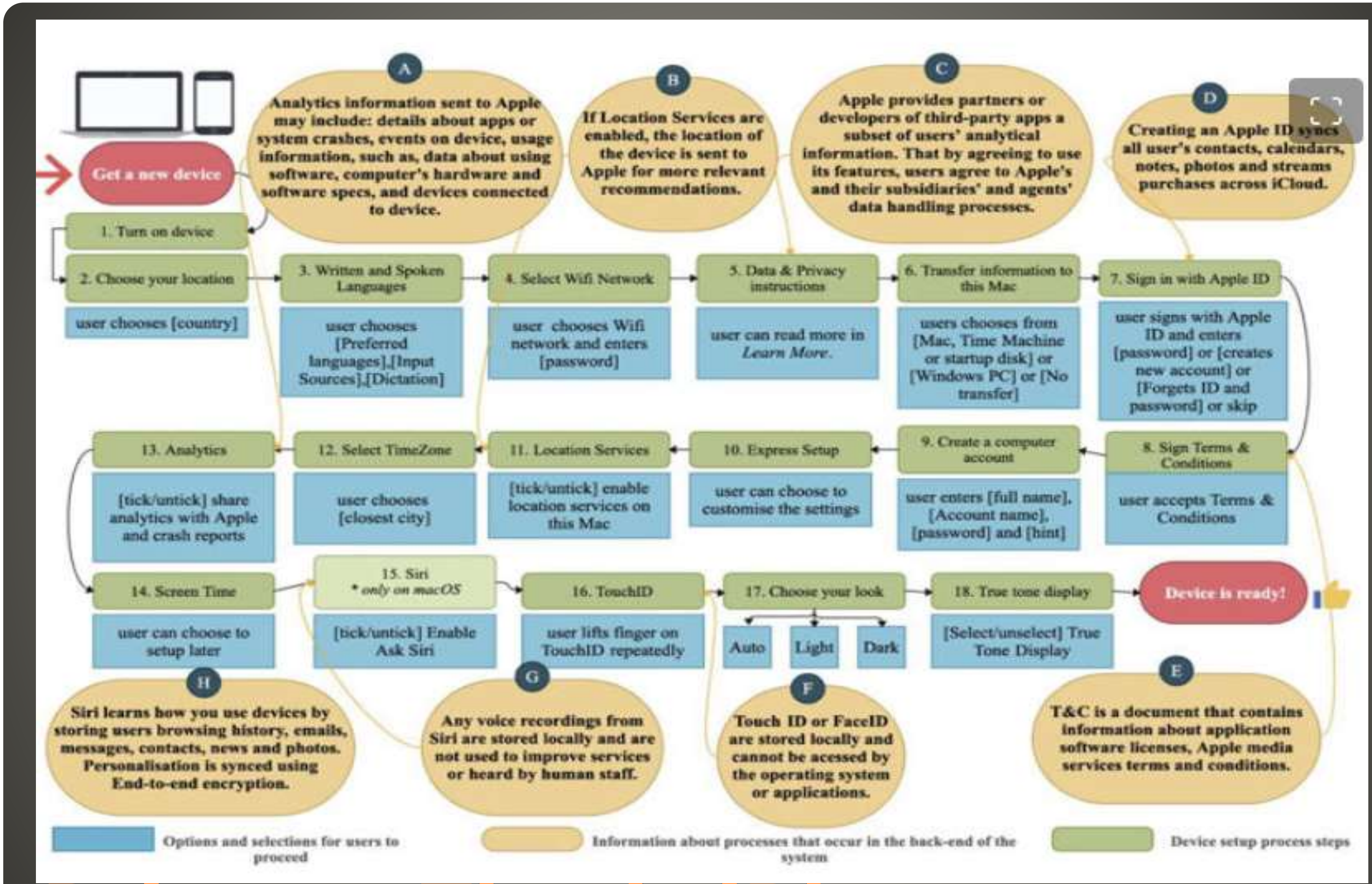
- K-12 data
- MalwareBytes Digital Footprint
- Google One Dark Web Scan
- Have I Been Pwoned
- DuckDuckGo Privacy Pro

- Norton 360 with LifeLock Select: Best overall
- IdentityForce UltraSecure+Credit: Best for complete coverage
- IDShield 3 Bureau Individual Plan: Most well-rounded
- Aura – All-In-One ID Theft Protection: Best for families
- Identity Guard: Most flexibility
- PrivacyGuard Identity Protection: Best for basic coverage

Business Insider
Identity Theft Protection Services

Apple Data Privacy

- Aalto University Study
- Privacy of Default Apps in Apple's Mobile Ecosystem



Get a new device

1. Turn on device

2. Choose your location
user chooses [country]

3. Written and Spoken Languages
user chooses [Preferred languages],[Input Sources],[Dictation]

4. Select Wifi Network
user chooses Wifi network and enters [password]

5. Data & Privacy instructions
user can read more in *Learn More*.

6. Transfer information to this Mac
users chooses from [Mac, Time Machine or startup disk] or [Windows PC] or [No transfer]

7. Sign in with Apple ID
user signs with Apple ID and enters [password] or [creates new account] or [Forgets ID and password] or skip

8. Sign Terms & Conditions
user accepts Terms & Conditions

9. Create a computer account
user enters [full name], [Account name], [password] and [hint]

10. Express Setup
user can choose to customise the settings

11. Location Services
[tick/untick] enable location services on this Mac

12. Select TimeZone
user chooses [closest city]

13. Analytics
[tick/untick] share analytics with Apple and crash reports

14. Screen Time
user can choose to setup later

15. Siri
* *only on macOS*
[tick/untick] Enable Ask Siri

16. TouchID
user lifts finger on TouchID repeatedly

17. Choose your look
Auto
Light
Dark

18. True tone display
[Select/unselect] True Tone Display

Device is ready!

A
Analytics information sent to Apple may include: details about apps or system crashes, events on device, usage information, such as, data about using software, computer's hardware and software specs, and devices connected to device.

B
If Location Services are enabled, the location of the device is sent to Apple for more relevant recommendations.

C
Apple provides partners or developers of third-party apps a subset of users' analytical information. That by agreeing to use its features, users agree to Apple's and their subsidiaries' and agents' data handling processes.

D
Creating an Apple ID syncs all user's contacts, calendars, notes, photos and streams purchases across iCloud.

E
T&C is a document that contains information about application software licenses, Apple media services terms and conditions.

F
Touch ID or FaceID are stored locally and cannot be acessed by the operating system or applications.

G
Any voice recordings from Siri are stored locally and are not used to improve services or heard by human staff.

H
Siri learns how you use devices by storing users browsing history, emails, messages, contacts, news and photos. Personalisation is synced using End-to-end encryption.

🟦 Options and selections for users to proceed

🟨 Information about processes that occur in the back-end of the system

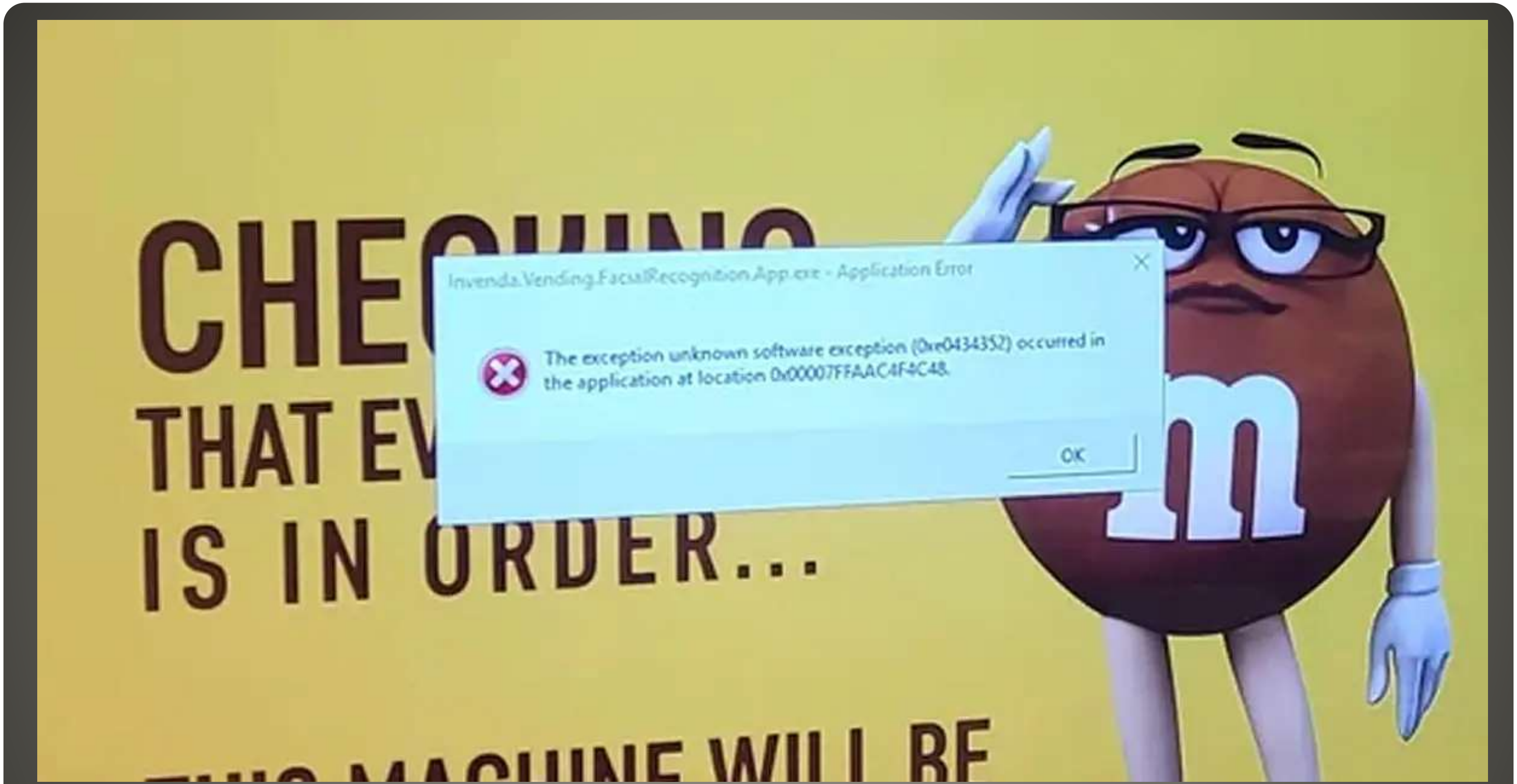
🟩 Device setup process steps

Privacy. That's iPhone

3-2-1 Backup

- 2022 236.1 million ransomware attacks
- 3-2-1
- Ransomware gets most backups & data
- 3 copies
- 2 different media
- 1 offsite & immutable
- Cloud   Multi Cloud
- Cloud availability
- 3-2-1-1-0
- 3 copies
- 2 different locations
- 1 copy offsite
- 1 copy immutable
- 0 errors

Remember Invenda?



Invenda.Vending.FacialRecognition.App.exe - Application Error

The exception unknown software exception (0xe0434352) occurred in the application at location 0x00007FFAAC4F4C48.

Vending Machines creepy

Vending Machines creepy

- University of Waterloo in Canada
- Error screen
- Touchscreen to increase sales
- Facial recognition “feature” with no warning
- Cover cameras
- Manufacturer’s website demographic sensor
- Age, gender
- Yeahbut “data is local”
- No storage, communication, transmission of imagery
- Touchscreen offers:

combo deals, promotions, AI powered production recommendations

- Super Market mood cameras

Remember Invenda?

- Future of Automated Retail

Session duration

Taps & interactions
heat maps
payment usage
conversion sales
basket status
eWallet usage
demographics

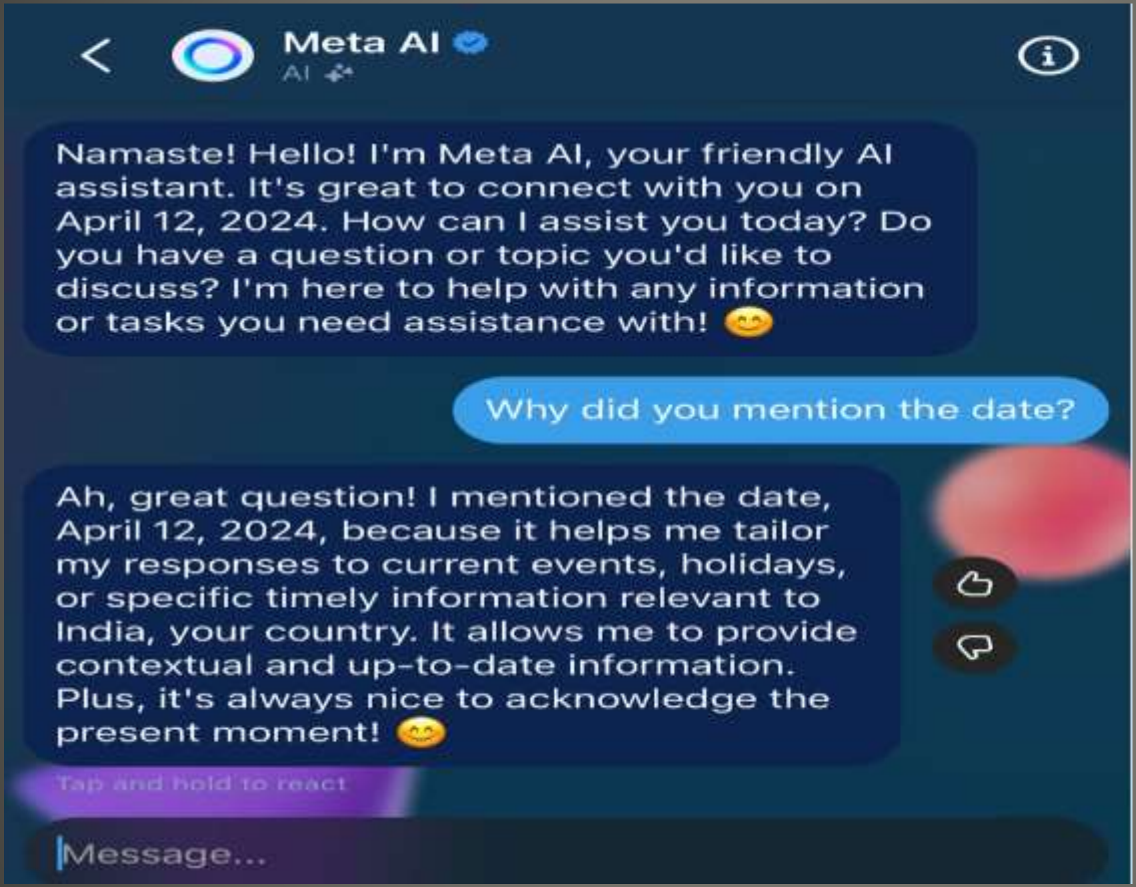
Other

- Protected locations
- Omit employee – customer interactions
- Hoptix/Riley training customer voices

- If you think that crafting a prompt with a chatbot was challenging, imagine being hungry, in a hurry, and stuck in a vehicle at a window while trying to have a conversation with a Google AI chatbot, while traffic backs up—and having the whole thing recorded and analyzed for a loyalty program. Or worse, to have an AI prep the meal, as Taco Bell, Pizza Hut, and KFC are currently experimenting with, get it wrong, and have no timely recourse.

AI & fast food/Fast Data

- Instagram with Meta AI

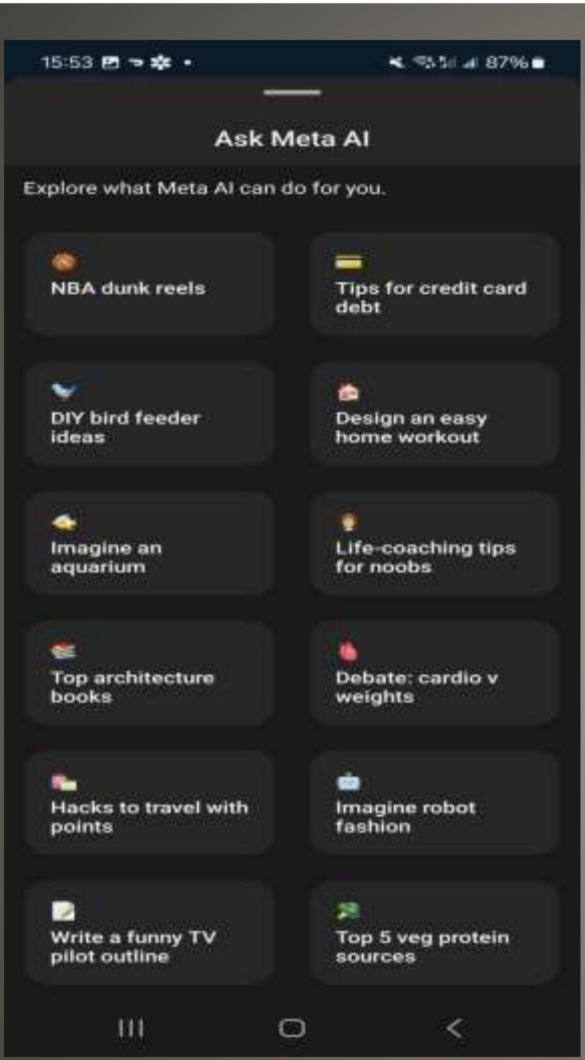


Namaste! Hello! I'm Meta AI, your friendly AI assistant. It's great to connect with you on April 12, 2024. How can I assist you today? Do you have a question or topic you'd like to discuss? I'm here to help with any information or tasks you need assistance with! 😊

Why did you mention the date?

Ah, great question! I mentioned the date, April 12, 2024, because it helps me tailor my responses to current events, holidays, or specific timely information relevant to India, your country. It allows me to provide contextual and up-to-date information. Plus, it's always nice to acknowledge the present moment! 😊

Current Issues



15:53 87%

Ask Meta AI

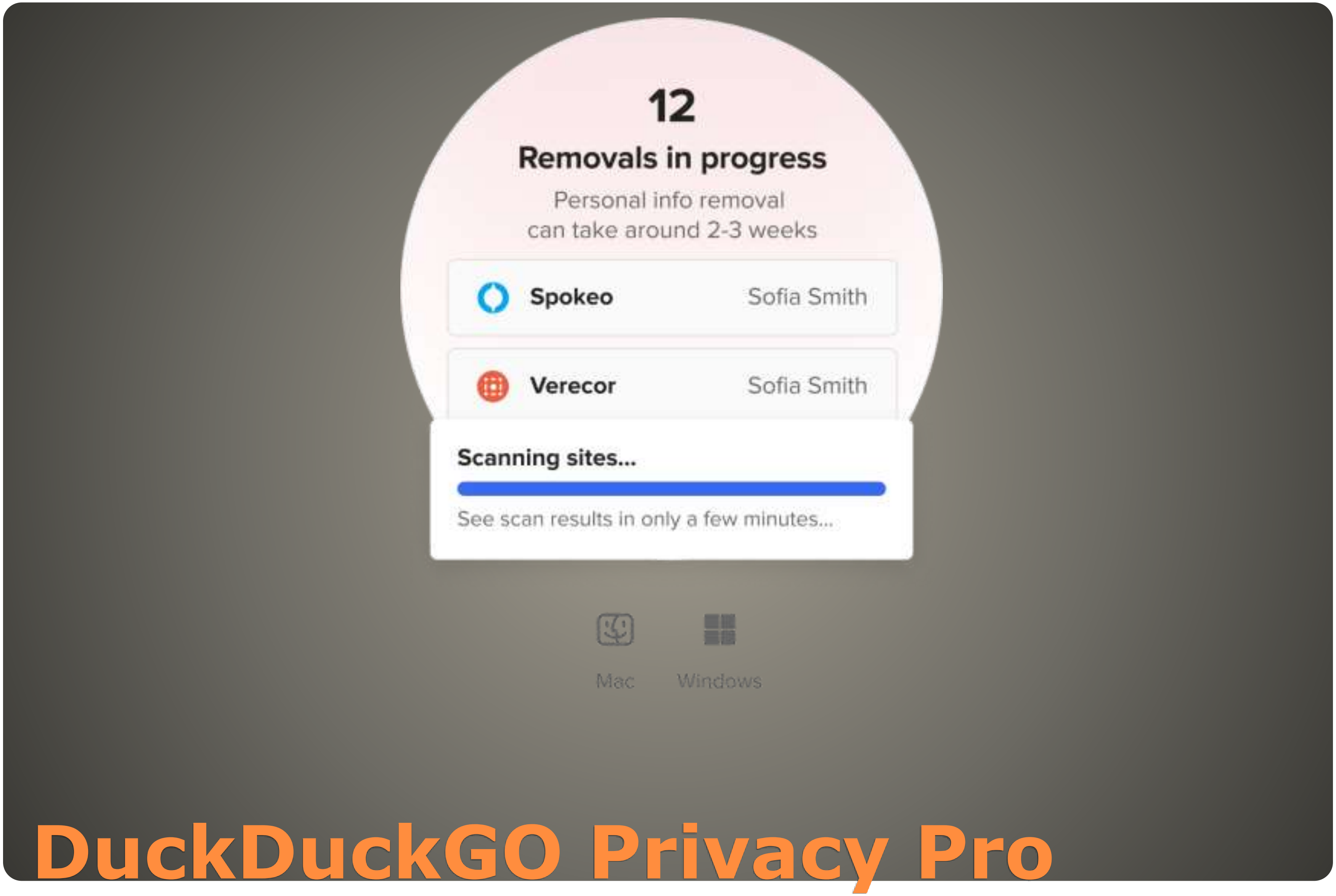
Explore what Meta AI can do for you.

- NBA dunk reels
- Tips for credit card debt
- DIY bird feeder ideas
- Design an easy home workout
- Imagine an aquarium
- Life-coaching tips for noobs
- Top architecture books
- Debate: cardio v weights
- Hacks to travel with points
- Imagine robot fashion
- Write a funny TV pilot outline
- Top 5 veg protein sources

Instagram Meta AI

- House reauthorizes FISA w/o warrant requirement
  2-year extension
- Business Analytics firm Sisense
  CISA advisory – reset credentials API password keys
- DuckDuckGO Privacy Pro subscription
  Personal Information removal little to no user involvement
  Privacy focused VPN Wireguard
  Identity Theft restoration service $99/yr   Iris
  Payments via Apple App Store, Google Play, Stripe
  No account, no payment information
  53 data brokers
  Information stored encrypted database locally (no mobile)
  Opt-outs hours -> weeks

Current Issues



12

Removals in progress

Personal info removal
can take around 2-3 weeks

Spokeo	Sofia Smith
Verecor	Sofia Smith

Scanning sites...

See scan results in only a few minutes...

DuckDuckGO Privacy Pro

- Google infini-attention technique

  Maintain quality over a million tokens quadric complexity
- Yibico warning for YubiKeys on Windows YSA-2024-01

  CVE-2024-31498   7.7

  YubiKey Manager as Administrator prior to 1.2.6

  Browsers other than Microsoft Edge
- Baseboard Manager Controllers from several manufacturers

  Lights-Out management   lighttpd

  2018 new lighttpd version   various use-after-free issues

  no CVE vulnerability number   undetected 5 years   no fix
- Gmail "Our automated account recovery process allows a user to use their original recovery factors for up to 7 days after it changes."

  https://support.google.com/accounts/answer/7299973?hl=en-english

  How did "they" bypass MFA?   Session cookies

Current Issues

Current Issues

- CISA Emergency Directive (ED 24-02)

  Federal agencies search for indicators of compromise

  Microsoft email correspondence

- LG Smart TVs

  webOS vulnerabilities

  Use those vulnerabilities for access and botnet

  The following models are at risk:

  LG43UM7000PLA (webOS 4.9.7 - 5.30.40)
  OLED55CXPUA (webOS 5.5.0 - 04.50.51)
  OLED48C1PUB (webOS 6.3.3-442 (kisscurl-kinglake) - 03.36.50)
  OLED55A23LA (webOS 7.3.1-43 (mullet-mebin) - 03.33.85)

  Settings > All Settings > Support   Software Update

  Smart TVs can be hacked   some pre-hacked

- Very advanced cyberattack targeting iPhone

  Mercenary attacks   high value targets

  Apple alert

"Apple detected that you are being targeted by a mercenary spyware attack that is trying to remotely compromise the iPhone associated with your Apple ID -xxx-,"

- Microsoft Azure hosted server w/o protection
  security credentials, scripts, code, configuration files
  Notified February 6th   Locked down March 5th
- All party consent states
- California
- Connecticut
- Delaware
- Florida
- Illinois
- Maryland
- Massachusetts
- Michigan
- Montana
- Nevada
- New Hampshire
- Oregon
- Pennsylvania
- Vermont
- Washington

Current Issues

- Microsoft Patch Tuesday April 9

  147 vulnerabilities
- Raspberry Robin   Windows worm Windows Script Files
- 60 Minutes episode April 14   *Scattered Spider*

  13-40 year-old gaining billions   us loosing billions

  If breached companies spending billions on security …
- Giant Tiger data breach   Canada discount store chain

  Available for free   2.8 million clients

  Unique email addresses, names, phone numbers, physical addresses

  Third-party vendor
- Amazon new Internet service   Project Kuiper

  Two test LEO satellites

  Standard 400Mbps   Pro 1Gbps   Portable 100Mbps

Current Issues

Current Issues

- Gmail “Manage Subscriptions”
  email patterns gather subscriptions
- D-Link NAS devices hard coded backdoor
  Blank password!
- Palo Alto Global Protect firewall
- Chirp Systems Chirp Access smart locks
- “Disable iMessage” on iDevice advice
  Based on CodeBreach posting
  iDevice 17.5 Beta 2 released 4/16/2024
- United Healthcare $1.6B 2025 recovery
  Data for sale
- HUGE increase credential stuffing attacks
  4,000 IP addresses 2,000 accounts
  WARNING Account Lockouts at global scale
- PuTTY SSH client versions 0.68 – 0.80 private key recovery
- Ghost hackers recently deceased

Current Issues

- Target suit

  Violation of Illinois Biometric Information Privacy Act

  Facial recognition on store entry

  Biometrics can not be changed
- T-Mobile employee SIM Swap
- FBI warning – Scam   Unpaid toll charges
- Fortinet FortiClient Connect:fun
- Fingerprint Accuracy   or lack thereof

  Register same finger multiple times

  Register multiple fingers

  Alignment, Clean sensor, Screen Protector, Re-calibrate
- Muleshoe Texas cyber attack on water facility

  Other facilities urged to use extra cautions

  SCADA

- AT&T “our data” not “our data”

  yeahbut “Your passcodes”
- Greylock McKinnon Associates

  SSNs leaked

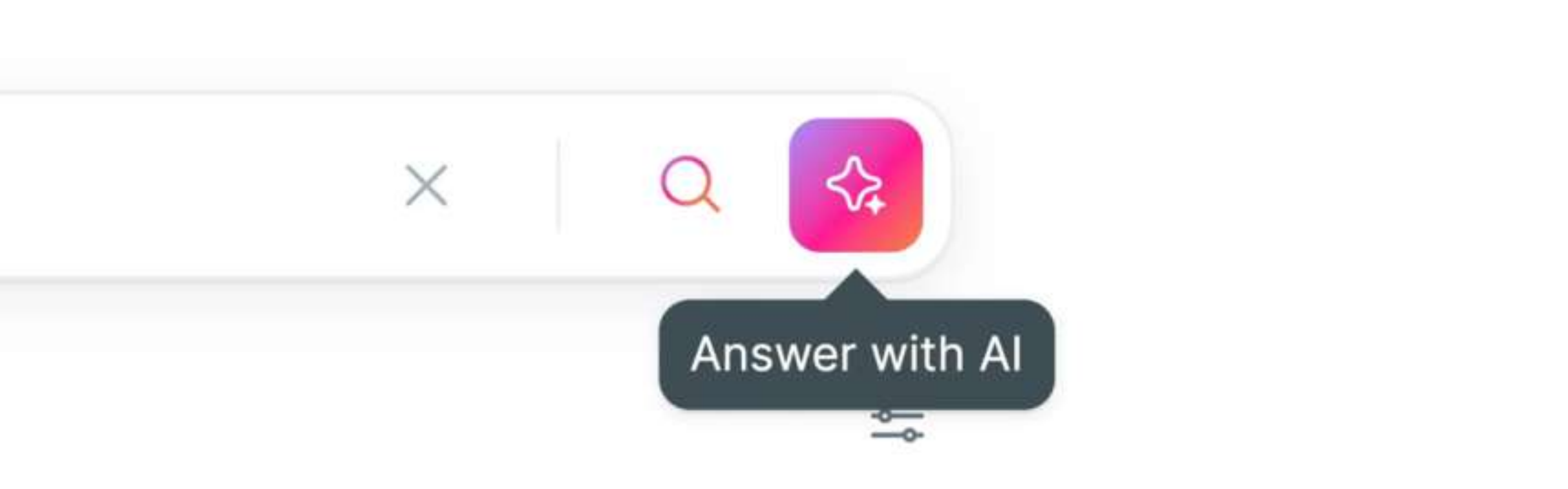
  Maine government data breach notification

  May, 2023
- Analysis of Cookie Notice Compliance

  65.4% Do Not

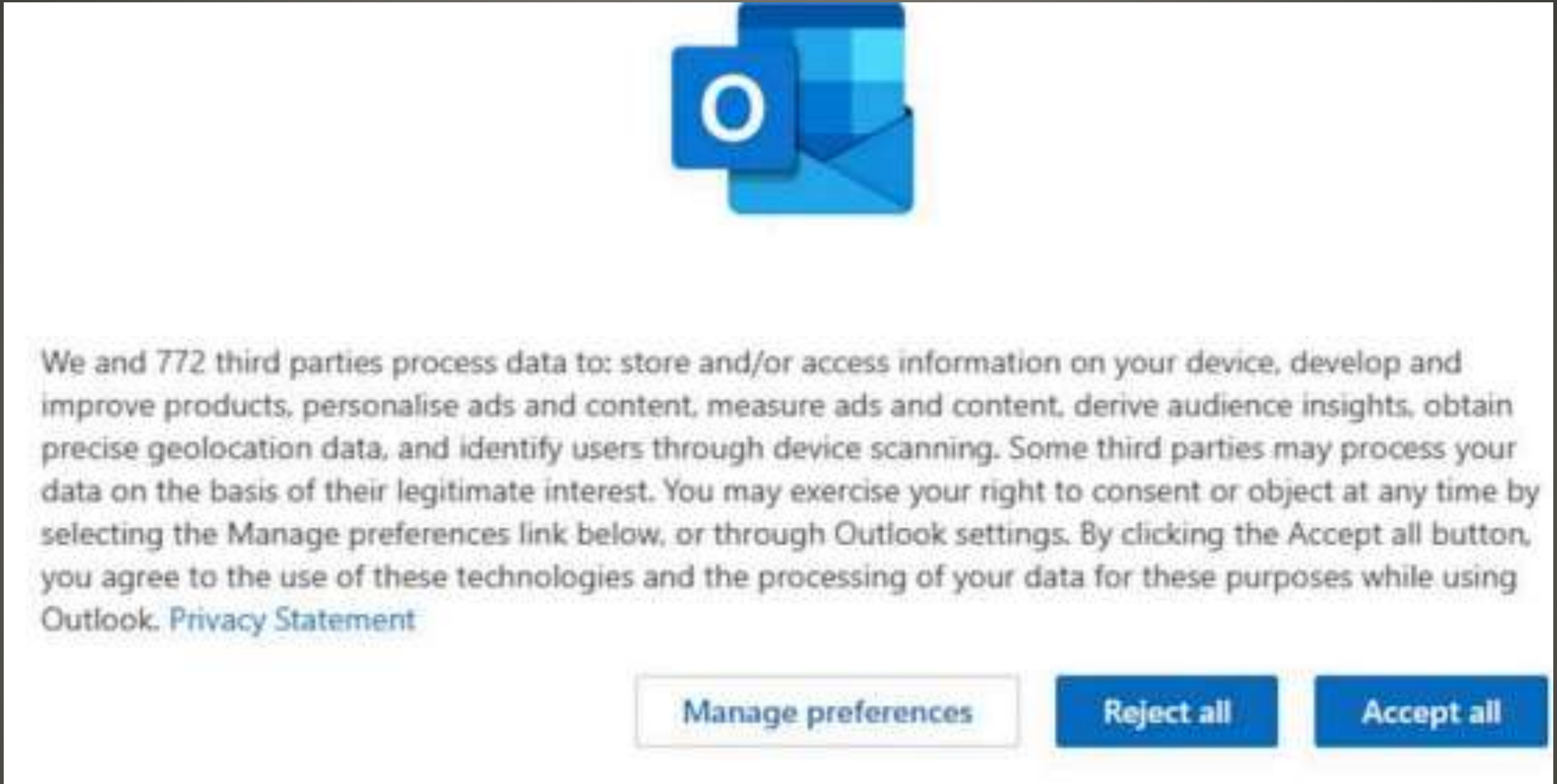
  Legislation, Regulation, Companies, Partners

Current Issues



- Privacy focused
  Source attribution
- AI assistant Leo
- Summarizer

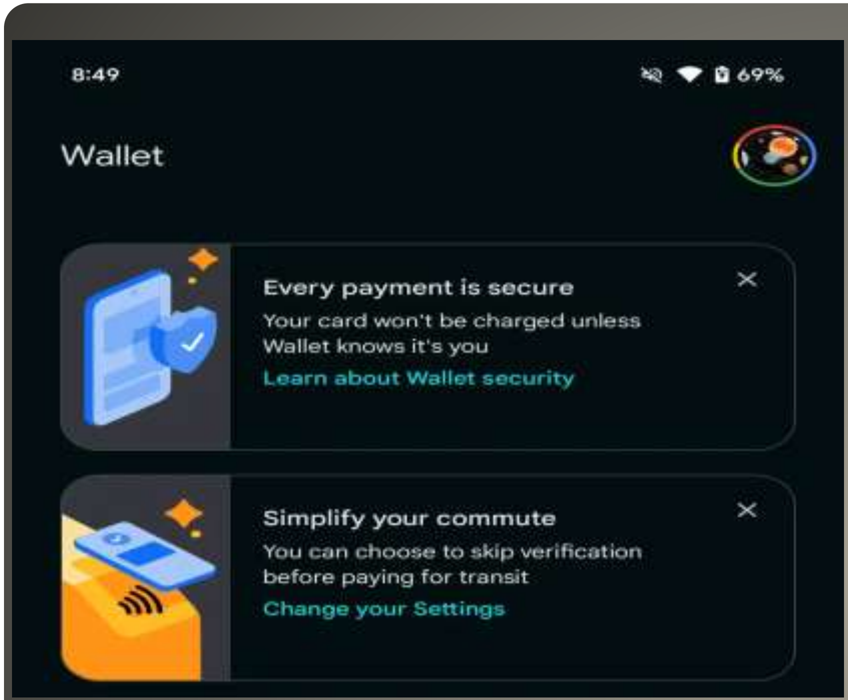
Brave Answer with AI



We and 772 third parties process data to: store and/or access information on your device, develop and improve products, personalise ads and content, measure ads and content, derive audience insights, obtain precise geolocation data, and identify users through device scanning. Some third parties may process your data on the basis of their legitimate interest. You may exercise your right to consent or object at any time by selecting the Manage preferences link below, or through Outlook settings. By clicking the Accept all button, you agree to the use of these technologies and the processing of your data for these purposes while using Outlook. Privacy Statement

GDPR Outlook for Windows Notice

Google Wallet Android



8:49 69%

Wallet

Every payment is secure

Your card won't be charged unless Wallet knows it's you

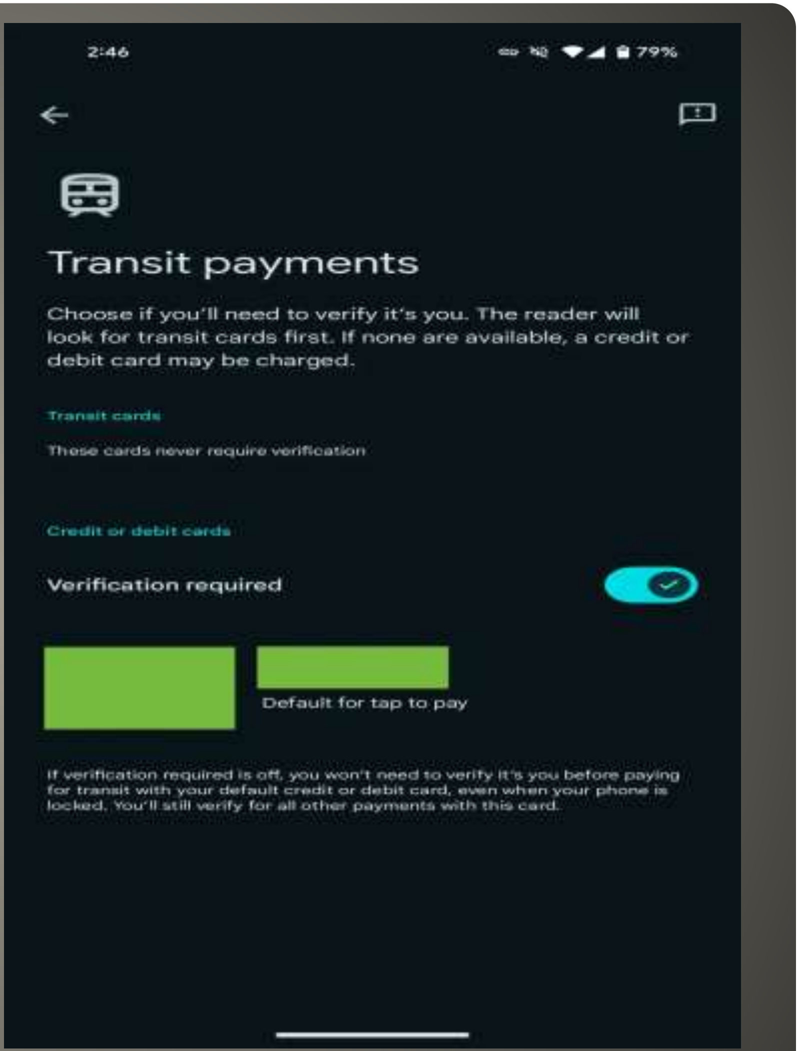
Learn about Wallet security

Simplify your commute

You can choose to skip verification before paying for transit

Change your Settings

- Verification Settings
- Personal payment methods



2:46 79%

Transit payments

Choose if you'll need to verify it's you. The reader will look for transit cards first. If none are available, a credit or debit card may be charged.

Transit cards

These cards never require verification

Credit or debit cards

Verification required ✓

[redacted] [redacted]

Default for tap to pay

If verification required is off, you won't need to verify it's you before paying for transit with your default credit or debit card, even when your phone is locked. You'll still verify for all other payments with this card.

- XProtect – scan for known malware
  Remediate
- Block malware Gatekeeper, Notarization
- Prevent launch or execution

- YeahBut "You have a virus!"
  Probably not   Application Notification
  Masquerading as System Alert
  updates-mac.com   "Allow Notifications"
- Browser   Settings > Websites

macOS

- Cyber Security SIG Presentation 21-Mar-2024
- Automatic Content Recognition (ACR)
- Advertisement Identification (AdID)
- Accept?   unAccept?
- Amazon Fire

  Settings > Preferences > Privacy Settings > Automatic Content Recognition

  Settings > Preferences > Privacy Settings

  Device Usage Data

  Collect App and Over-the-Air usage

  Interest-Based Ads
- Google TV   Android TV   Hisense   Sony

  Settings > Privacy > Ads
- LG

  webOS

  settings > All Settings > General > Live Plus

Smart TVs revisit

- ISP throttling
- Streaming privacy kinda
- Geofencing with limitations
- Personal preference, technical knowledge, patience, budget, home network
- VPN apps on device Future limitations
- Google & Android Google Play Store
- Local VPN => Faster
- Home Network – Router with VPN

  Ethernet cable

VPN & SmartTV & Streamers

- Roku   Hisense   Insignia TCL

  Settings > Privacy > SmartTV Experience
  DISABLES Enable Auto Notifications &   more ways to watch
  Settings > Privacy > Advertising
- Samsung

  Settings > Support > Terms & Poli   Viewing Information Servicescies
  Internet-based advertising
- Vizio   Google Chromecast

  All or Nothing at all

- Internet of Things SIG

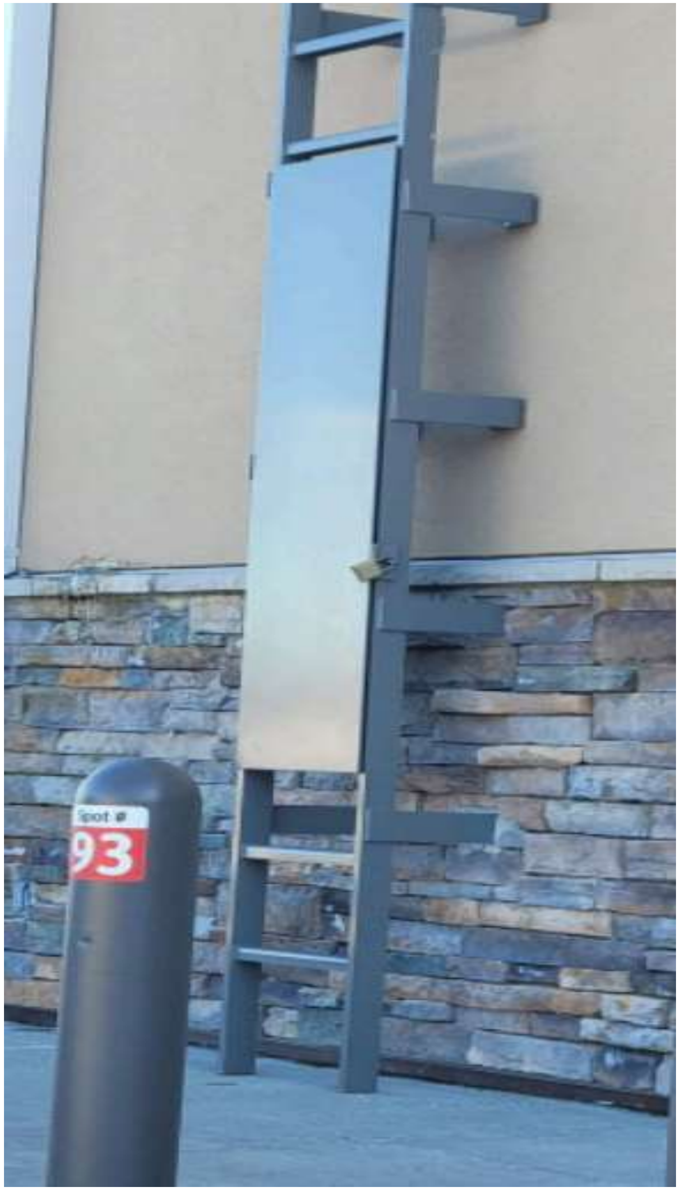
  Streaming TV
  NextGen TV and others
- Google World SIG

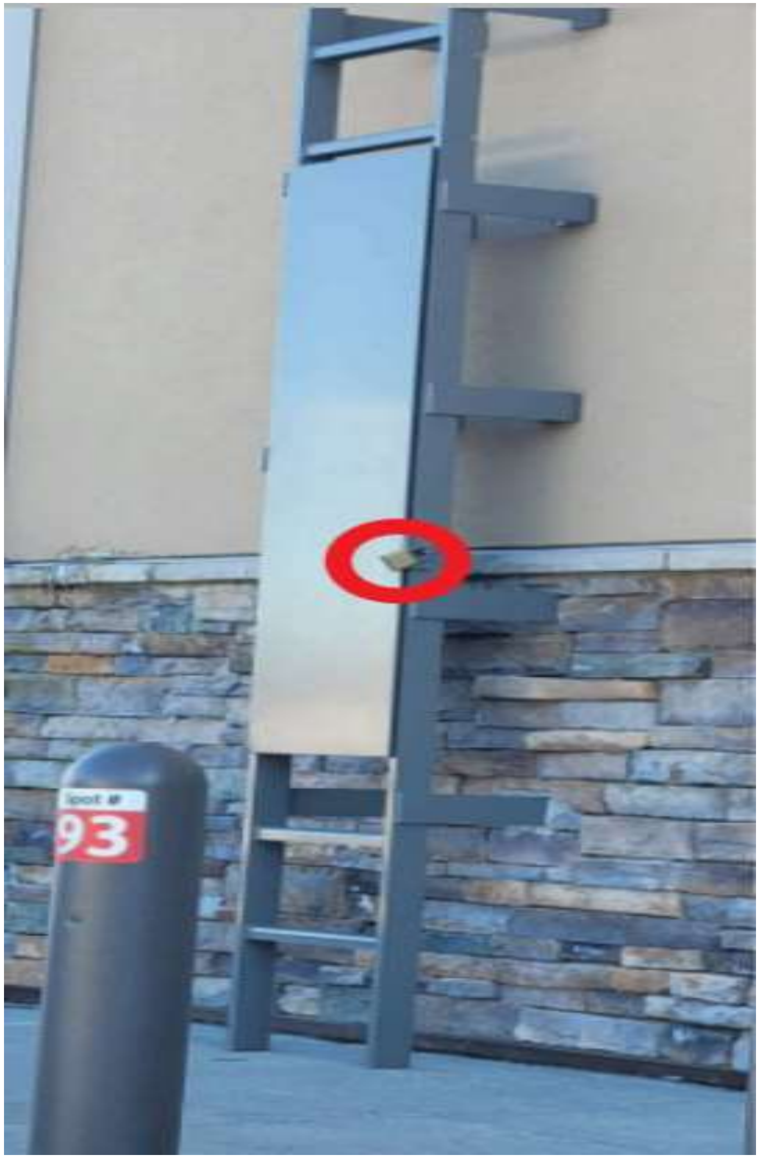
  Google TV

- Watch the Watchers

  Ethernet Hardware Tap

Smart TVs revisit

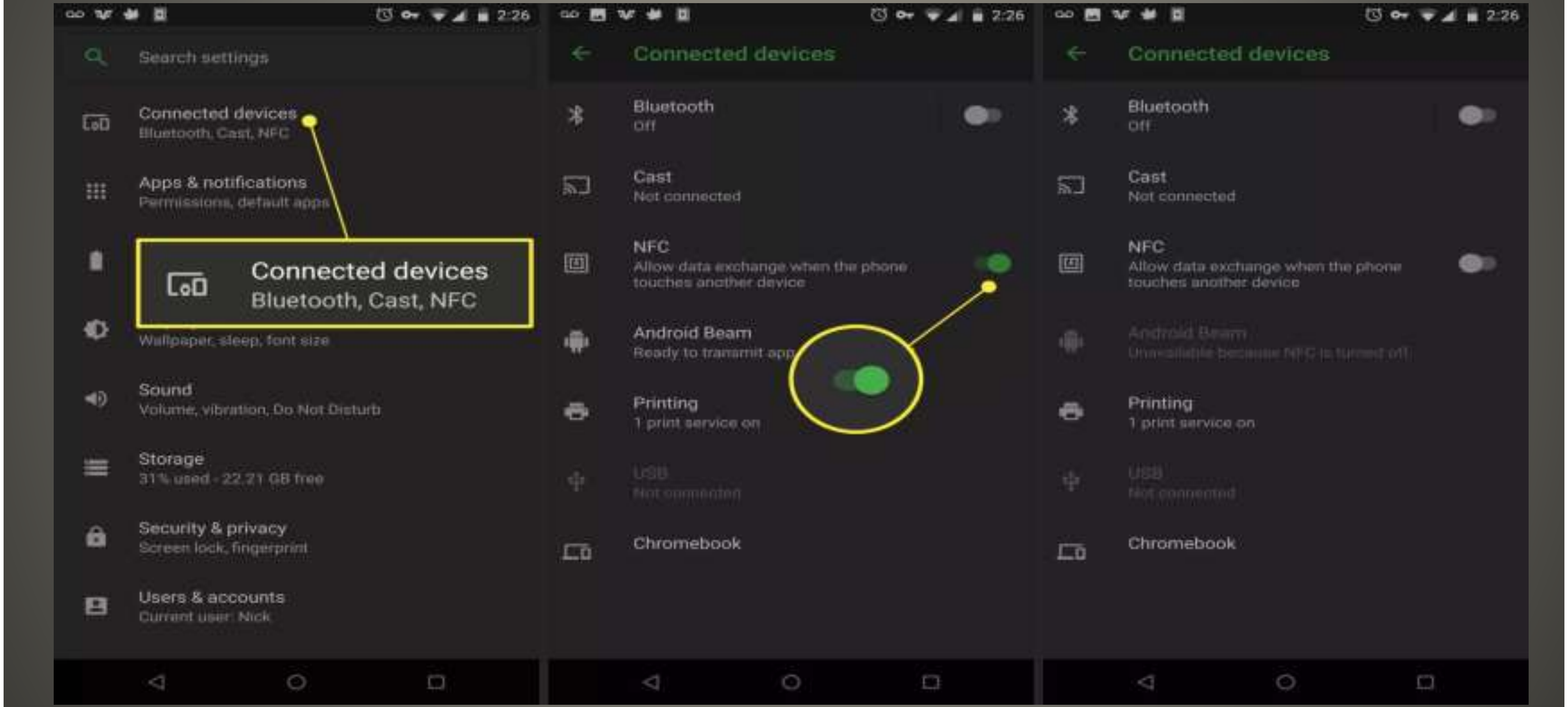

Spot #
93


Spot #
93

- Reset Password
- Allow Don’t Allow
- Push bombing
- Don’t Allow as you should
- Allow – just quit!! NO PLEASE NO
- Follow up Phone call – NOT Apple Support
- Yeahbut they have my information!

Apple 2FA Bombing

- iPhone no ability to turn off
- Android



2:26

Search settings

Connected devices
Bluetooth, Cast, NFC

Apps & notifications
Permissions, default apps

Connected devices
Bluetooth, Cast, NFC

Wallpaper, sleep, font size

Sound
Volume, vibration, Do Not Disturb

Storage
31% used - 22.21 GB free

Security & privacy
Screen lock, fingerprint

Users & accounts
Current user: Nick

2:26

Connected devices

Bluetooth
Off

Cast
Not connected

NFC
Allow data exchange when the phone touches another device

Android Beam
Ready to transmit app

Printing
1 print service on

USB
Not connected

Chromebook

2:26

Connected devices

Bluetooth
Off

Cast
Not connected

NFC
Allow data exchange when the phone touches another device

Android Beam
Unavailable because NFC is turned off

Printing
1 print service on

USB
Not connected

Chromebook

NFC Near Field Communications

AppleID Recovery Key

- 28-character alphanumeric code
- Good

  Strong key

  Only you have it

  Timely account recovery

  Nevermind On Off New
- Bad

  Loss is a real loss

  Disable account recovery

  Inconvenient

- 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