Sun City Computer Club

Cyber Security SIG

September 1, 2022

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

- Ever want to be a presenter??

Presenter???


1-800-614-1051
Wifi Network: BMS_Guest
Wifi Password: 1122334455
1 626min
RELAY
720-59.94p
AVCHD PM
ICONS
A 4660K
MA4.03ft
Z19.3mm

RANT

- Several residents have financial life ruined
- For years
- Cyber is important Cyber is not easy
- No quick means to an end
- “Over my head” Tone it down
- Agree for Windows and Mac Not cyber
- Life Liberty Pursuit of happiness
- Awareness, Preparedness, Understanding
- Any learning activity

- Not another member

- New Seminar

Computer Club Web Site Navigation – Update

- Coupon $30+ Million
- Evacuation notice send in error

Ventura Co., Los Angeles, Eastern North Pacific Ocean, Port Conception to Guadalupe


bitcoin
ATM

Bitcoin ATMs

- Hackers exploit vulnerability
- Steal digital currencies at exploited ATMs
- Several digital currencies on ATMs
- Hackers create a rogue Administrator

iOS 12

- Update released by Apple 31-August-2022
- Older iPhones & iPads
- Same serious vulnerability released 8/17/2022
- Update iOS 12.5.6
- Older devices in closet or used as IoT controller?

- My iPhone iOS 10.3.4

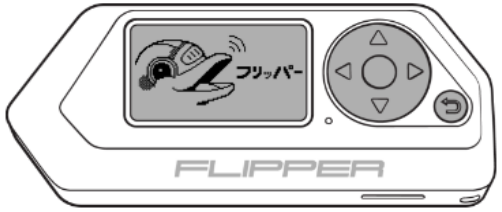
- ChromeOS 1.4.0.5112.110

Updates

Amazon Smart Shelf

Current Issues

- Shlayer North Korea SHARPEXT
  Detected at Black Hat
- Apple stops signing iOS 15.6
  Can't then downgrade after 15.6.1
- LastPass hacked
  Source code & technical information
- Starlink V2 direct to mobile phones
  Eliminate dead zones For receiving?
- Japan government current requirement
  CD-ROM or floppy disks
- OptFi blockchain crypto platform
  Developer entered wrong command
  $661,000 accidently & permanently gone
- T-Mobile Network Pass program



Flipper Zero Documentation

Need help using your Flipper Zero?
Discover usage guides, developer documentation, schematics, configs and more.

Basics
How to Update Firmware, Control your device, Setup the SD card, edit Settings and recover in case of failures.

Sub GHz
Radio systems under 1GHz frequency range. Manipulating digital wireless remotes and their radio protocols.

RFID 125 kHz
Low frequency proximity cards. Reading, writing and emulating 125 kHz RFID tags.

NFC
High frequency 13,56 MHz smart cards. Reading, attacking, writing and emulating NFC cards.

Infrared
Infrared signals used in TVs, audio systems, air conditioners and more. Reading and emulating infrared remotes.

GPIO & Modules
General Purpouse I/O pins for connecting hardware modules. Physical wired connection via UART, SPI, I2C.

iButton
Dallas touch memory keys (1-Wire). Reading, writing and emulating iButton electronic keys requiring physical contact.

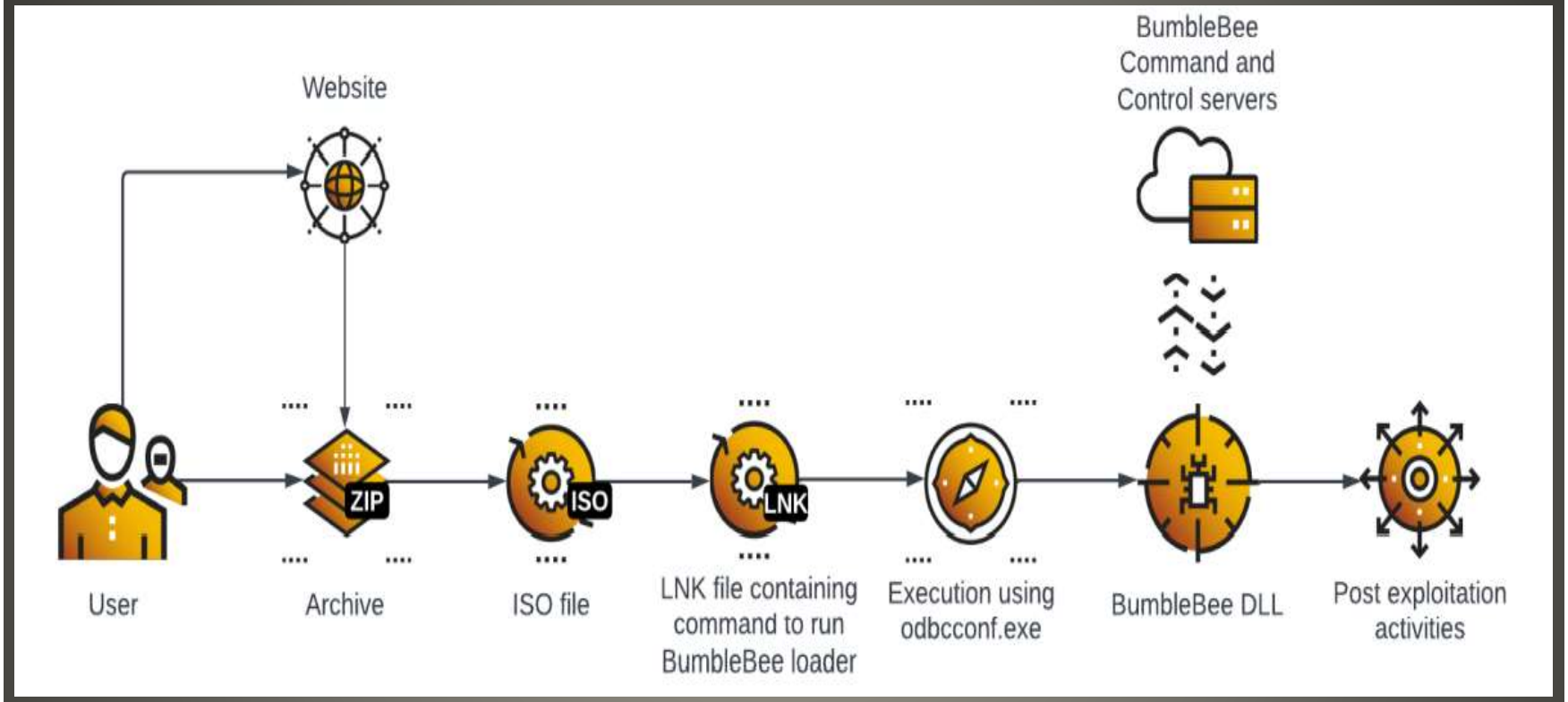
Bad USB
Emulating PC keyboard to inject keystrokes via USB Rubber Ducky's scriptable payloads language.

Mobile apps
Flipper Android/iOS mobile apps provide extended control of the device: updating firmware, sharing keys and more.

Development
Software and Hardware development. System API's documentation, code examples, debugging, PCB schematics.

Current Issues

- Samsung firmware updates for old smartphones
  500 million+
- Increasing mortgage wire transfer fraud
  Account takeover
  Knowledge of real estate transfer
- Desktop translate apps Crypto mining
- Apple Child Sexual Abuse Material (CDAM)
  Client side
  Server-side Apple, Google, Microsoft
- 45 million HTTPS requests per second
  24-hour requests to Wikipedia 10 seconds
  5256 source Ips 132 countries
  Tor exit nodes as C&C



Bumblebee Loader

- Montenegro ransomware attack
- Several days old
- Other nation states responding

- Programming Language
  Cross platform
  Resistant to reverse engineering and analysis
  Current threats not marked by VirusTotal
  Space images from James Webb telescope

Golang

Invoice updated

Billing Department of PayPal updated your invoice

Amount due: $600.00 USD

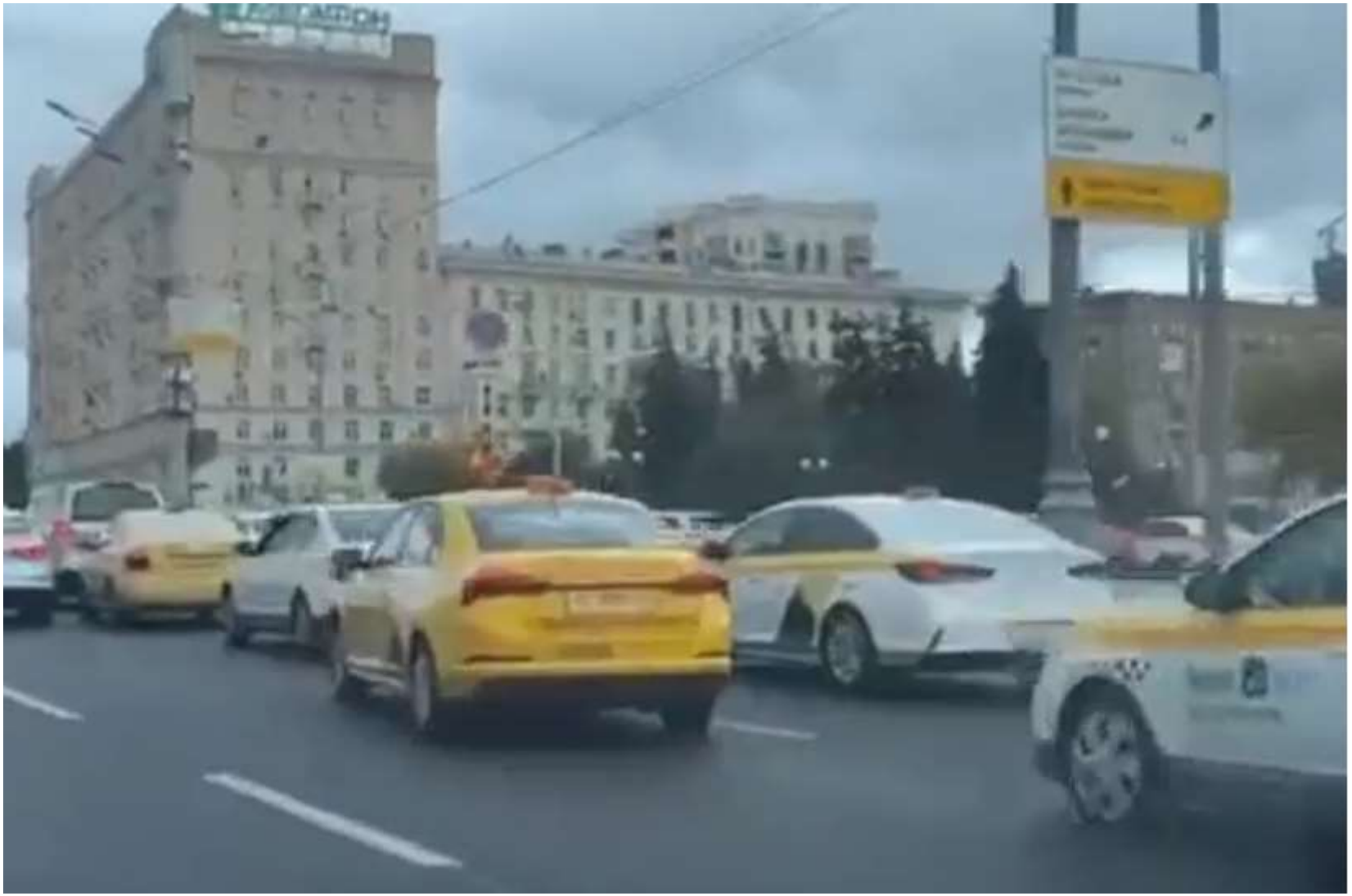
View and Pay Invoice

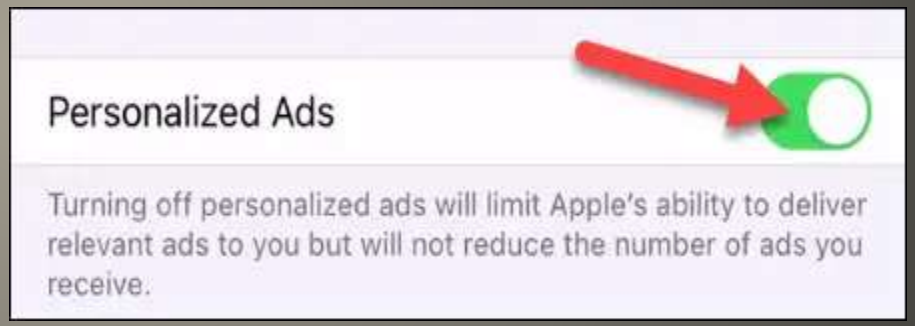
Seller note to customer

There is evidence that your PayPal account has been accessed unlawfully. $600. 00 has been debited to your account for the Walmart eGift Card purchase. This transaction will appear in the automatically deducted amount on PayPal activity after 24 hours. If you suspect you did not make this transaction, immediately contact us at the toll-free number +1 (888) 865-0443 or visit the PayPal Support Center area for assistance. Our Service Hours: (06:00 a. m. to 06:00 p. m. Pacific Time, Monday through Friday)

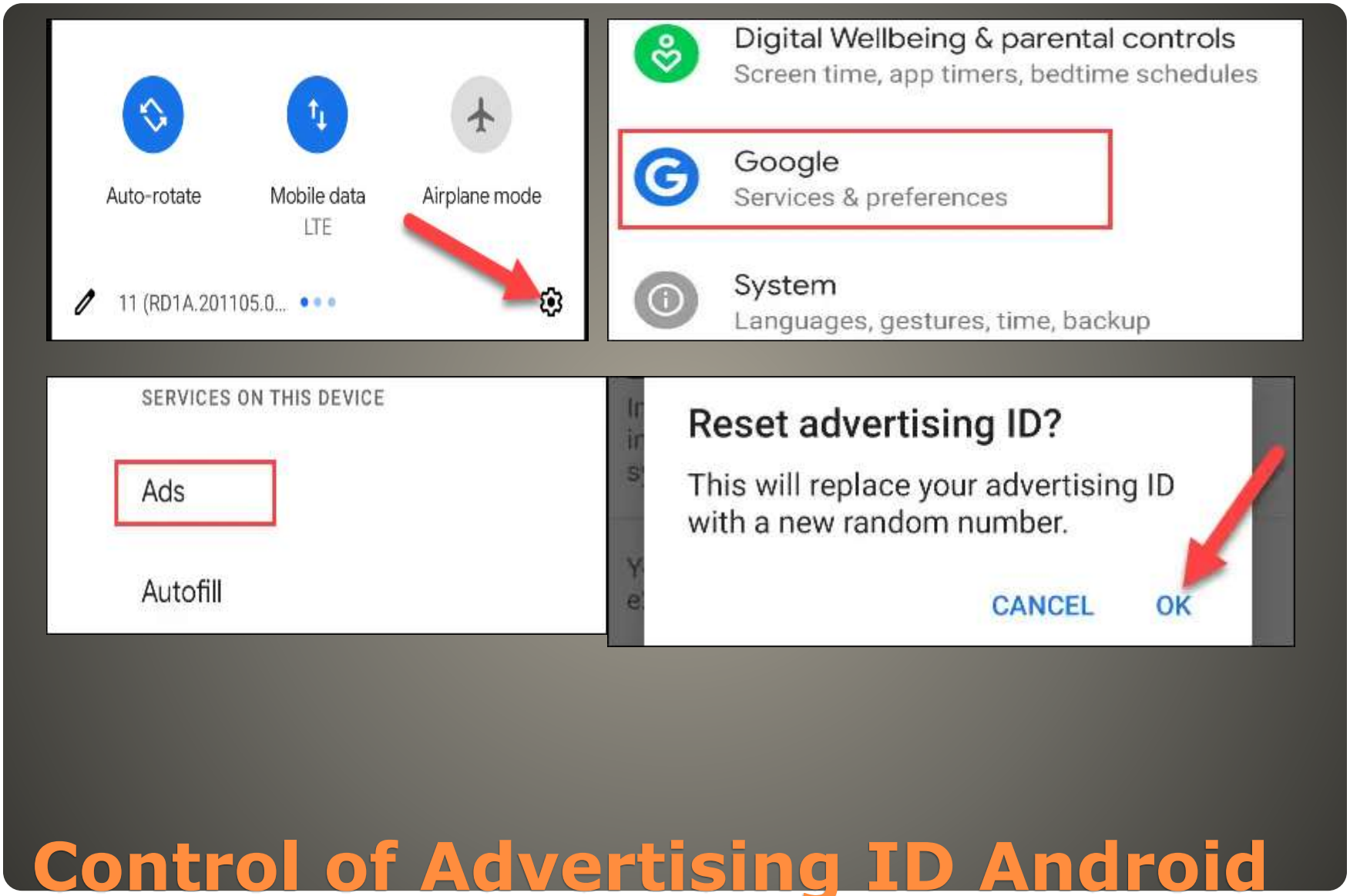
Current Issues

- Chrome 0-day
- Apple High priority updates
  iOS, iPadOS, macOS
- Bumblebee Loader
- Google Chrome version 105
- FTC suing Kochava for location data sales
  Mobile data:
  Mobile Advertising ID, device type, timestamps, Lat Long, IP address
- YandexTaxi hack
- AGT Deep Fake

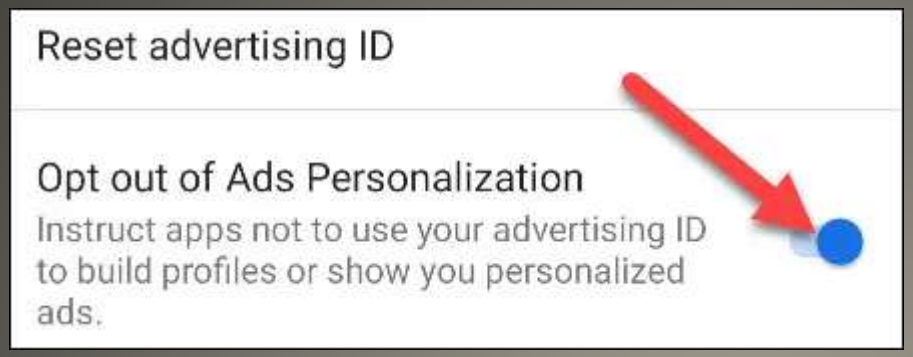


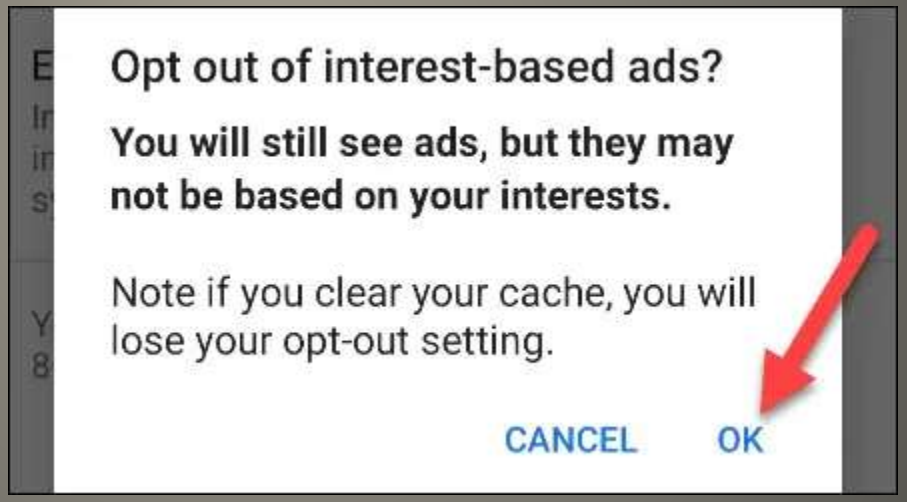


Control of Mobile Advertising ID iOS



Control of Advertising ID Android



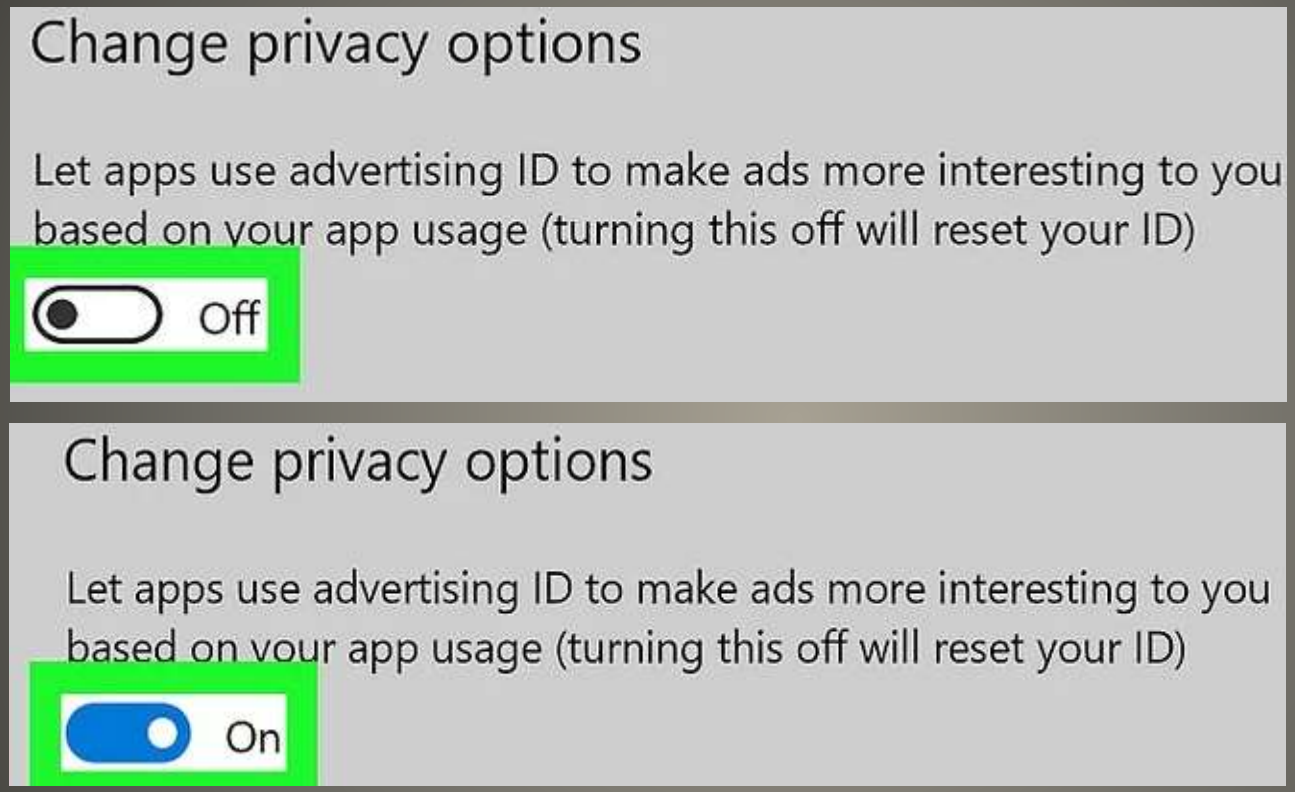


Control of Advertising ID Android

- System Preferences > Security & Privacy

Control of Advertising ID macOS

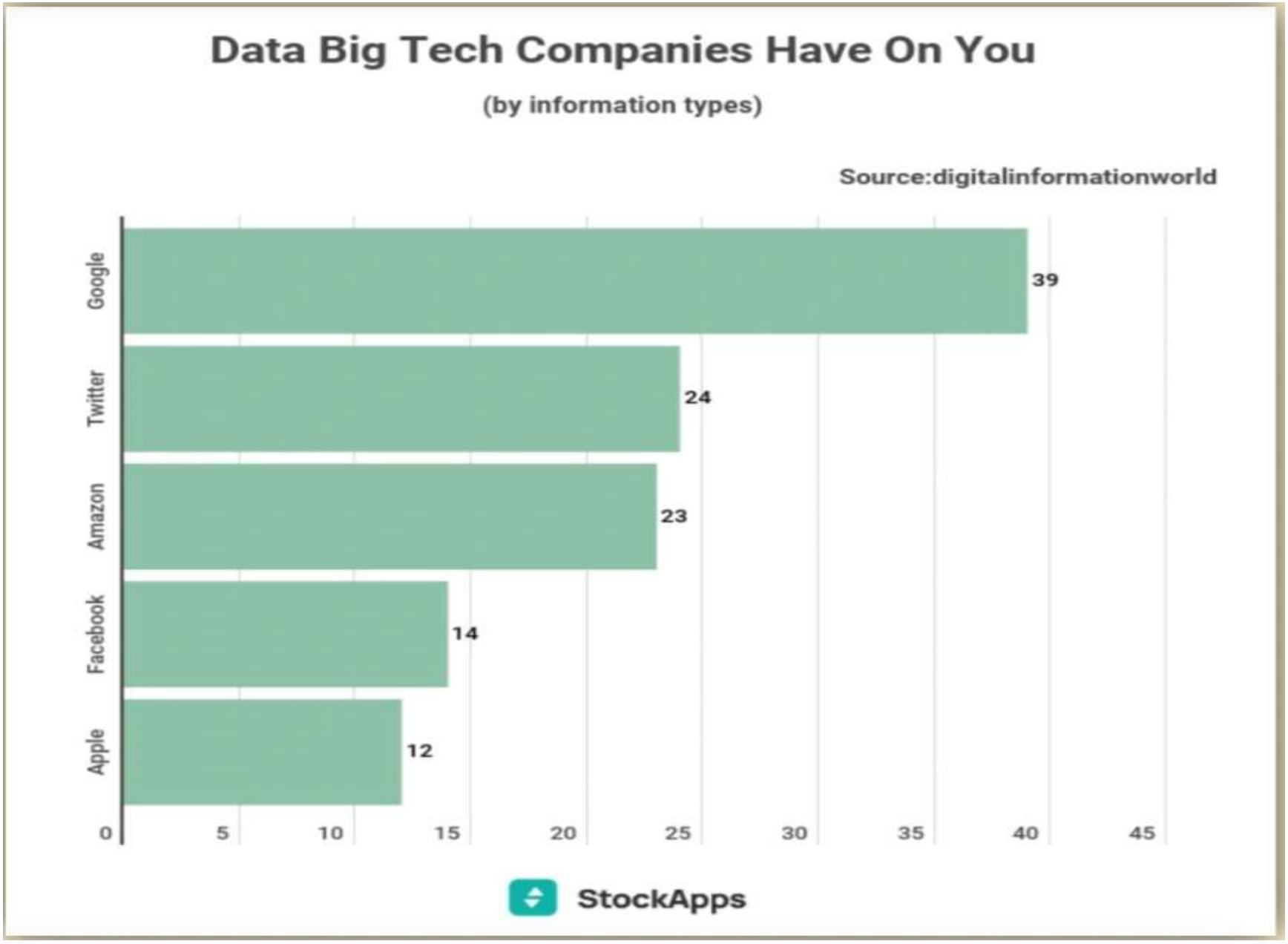
- Settings > Privacy > General



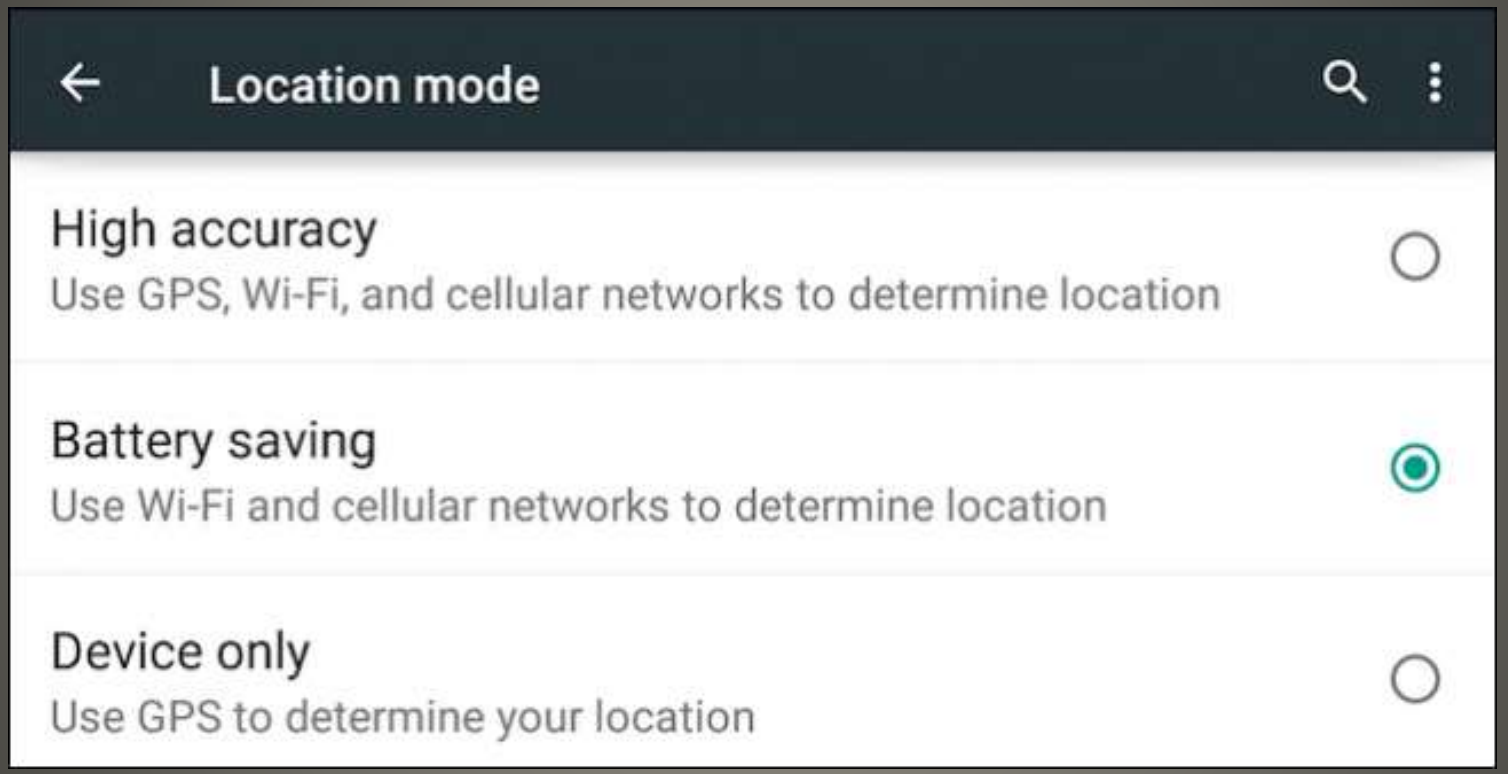
Control of Advertising ID Windows

- One click
- Thousands of employees
- Many thousands of contractors, service providers, customers
- Many millions of clicks
- One click

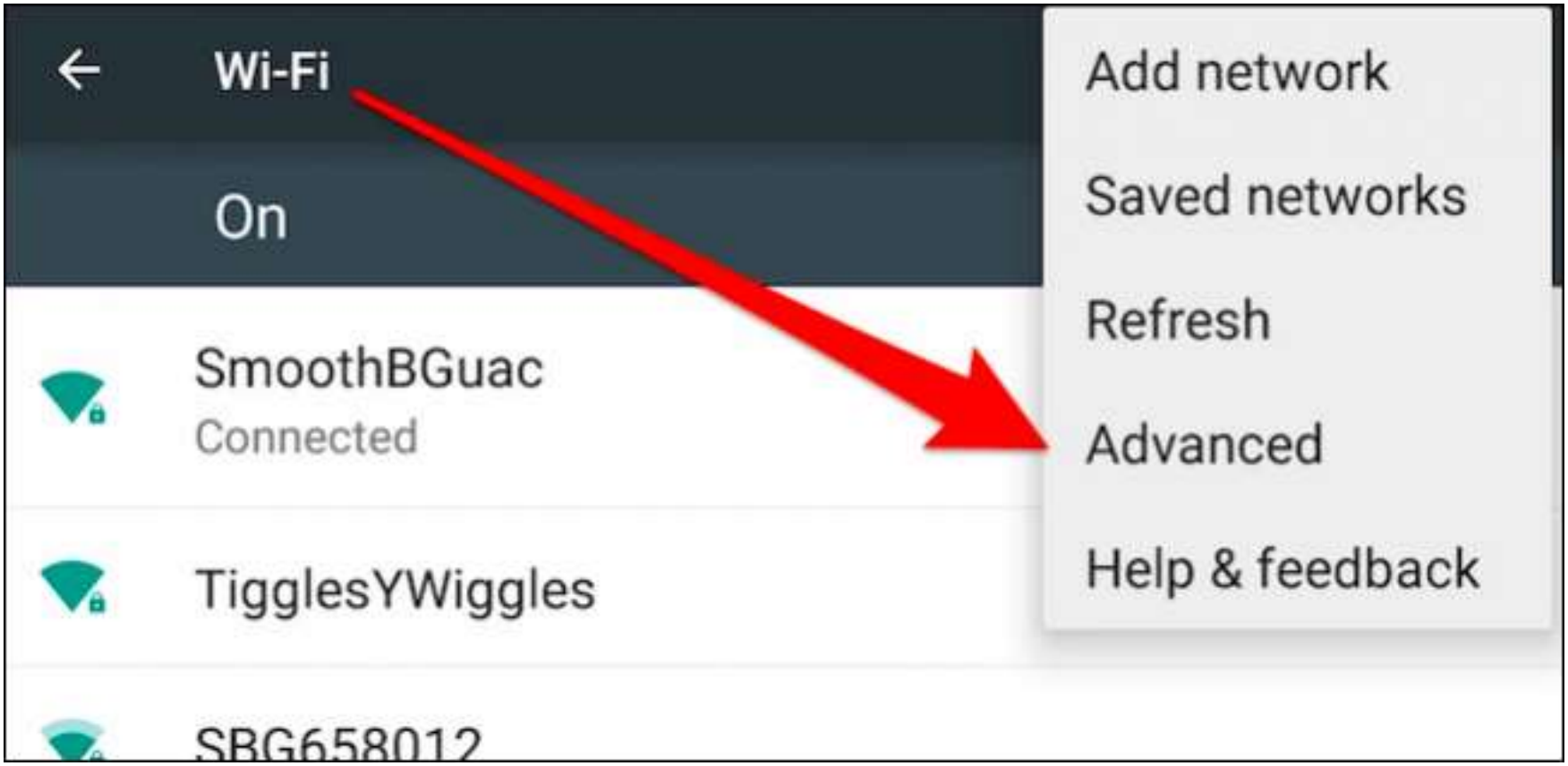
Enterprise & malware

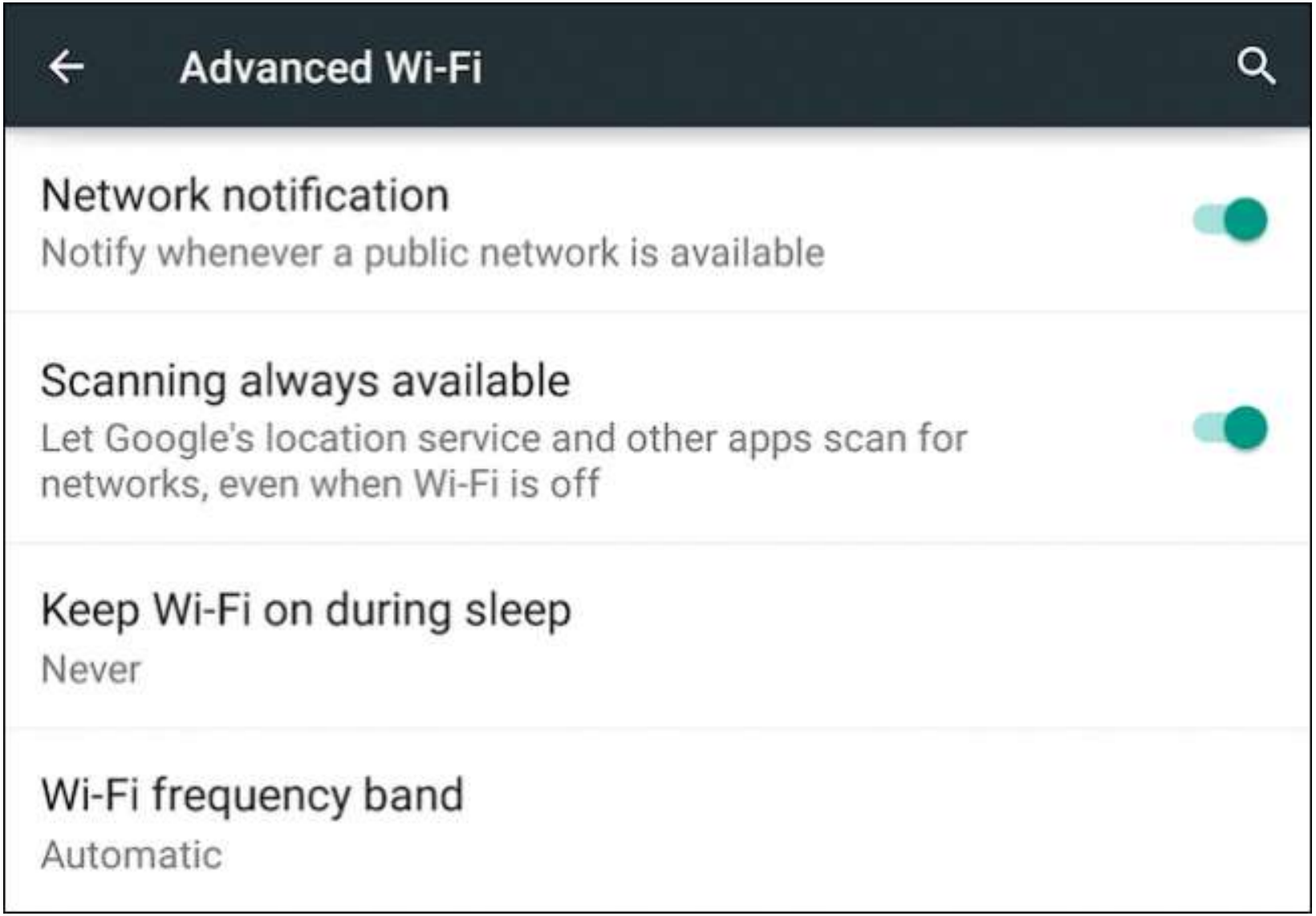

Data Big Tech Companies Have On You
(by information types)
Source:digitalinformationworld
Google
Twitter
Amazon
Facebook
Apple
39
24
23
14
12
0
5
10
15
20
25
30
35
40
45
StockApps

- **Scanning always available**



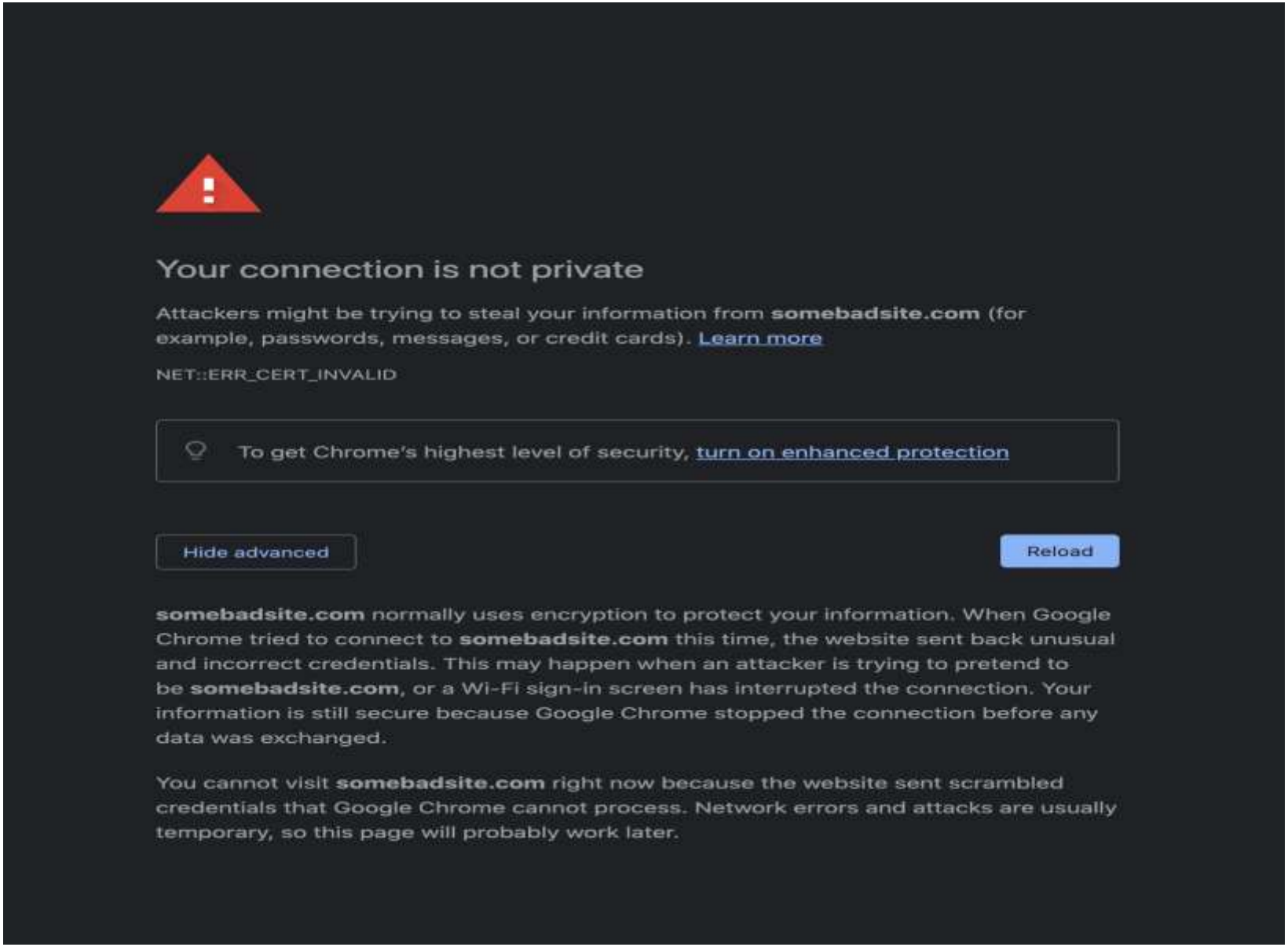
Android WiFi


Wi-Fi
On
SmoothBGuac
Connected
TigglesYWiggles
SBG658012
Add network
Saved networks
Refresh
Advanced
Help & feedback


Advanced Wi-Fi
Network notification
Notify whenever a public network is available
Scanning always available
Let Google's location service and other apps scan for networks, even when Wi-Fi is off
Keep Wi-Fi on during sleep
Never
Wi-Fi frequency band
Automatic

Secure Cloud Services

- NerdLocker
- Tresorit
- Sync.com
- Nextcloud
- Mega
- Best Privacy-First Cloud Storage Services


Your connection is not private
Attackers might be trying to steal your information from somebadsite.com (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_INVALID
To get Chrome's highest level of security, turn on enhanced protection
Hide advanced
Reload
somebadsite.com normally uses encryption to protect your information. When Google Chrome tried to connect to somebadsite.com this time, the website sent back unusual and incorrect credentials. This may happen when an attacker is trying to pretend to be somebadsite.com, or a Wi-Fi sign-in screen has interrupted the connection. Your information is still secure because Google Chrome stopped the connection before any data was exchanged.
You cannot visit somebadsite.com right now because the website sent scrambled credentials that Google Chrome cannot process. Network errors and attacks are usually temporary, so this page will probably work later.

thisisunsafe - bad idea?

As you can see, these are just warnings. Some browsers will let you go through after clicking on the `Accept and Continue` button. In some situations Chrome doesn't even present you with a `Continue` button. For those circumstances though, there is a bypass available. You can just type in `thisisunsafe` anywhere on the window and the browser will let you visit the page.

The bypass adds an exception for that particular domain to chrome's internal memory. You can remove the exception by clicking on the padlock icon and **Re-enable Warnings** link. Same is true with Firefox albeit with slight change in the UI etc.

MAIL STORE®

Products Customers Support Blog Company

Overview Changelog

MailStore Home

MailStore Home lets you archive your private emails from almost any source and search through them quickly. Keep your emails safe and retrievable for years.

Download MailStore Home (Free)

Version 22.2.1 | Changelog | For Windows 7, 8.1 and 10

Email Security Made in Germany

You are here: Home ▶ Products ▶ Free Email Archiving Software for Home Users

Free Email Archiving Software for Home Users

Emails are a valuable source of information for home users, too. A large amount of data and important files are saved in the form of emails. With MailStore Home, you can backup all emails in a secure and central archive, even if they are distributed across different computers, programs or mailboxes. You can do this either on your PC or on a USB drive as a "portable" option.

An additional advantage: you can still reply to or forward archived emails by opening them with a single mouse-click in your standard email program. In addition, the archive allows you to search quickly and easily through all your email communications.

MailStore Home Support

Please visit our customer support community and feel free to ask questions or read the MailStore Home Help.

Support Community

Benefits

A Central Archive for All Emails

- Internet mailboxes such as Gmail or Yahoo! Mail
- Any POP3 and IMAP mailboxes
- Microsoft Outlook 2003, 2007, 2010, 2013, 2016 and 2019
- Windows Mail and Windows Live Mail
- Microsoft Exchange Server 2003[1], 2007[1], 2010, 2013, 2016 and 2019 mailboxes
- Microsoft 365[2] (Exchange Online)
- Mozilla Thunderbird and SeaMonkey
- PST, EML and other files

All Emails Securely Stored in the Archive

Emails can be lost due to incomplete data backups, corrupted PST files, or other technical problems. With MailStore Home, you can keep all your emails safely in the archive, where they are easily retrievable.

Not a One-Way Street

All archived emails can be restored from the archive at any time using the handy export feature. This allows MailStore Home also to be used for migrating emails.

Fast Search

MailStore Home has a powerful full-text search feature that can search through large amounts of data and any type of file attachment.

One-Click Restore

Emails can be restored from the archive or simply opened in an email client (e.g. Outlook) with a single mouse-click.

Safe Even for Large Amounts of Data

MailStore Home can manage large amounts of data effortlessly. Now both your past and future emails are safely stored.

Mobile Email Archive

MailStore Home is also available as a "portable" option and can be launched directly from a USB hard drive on any PC without prior installation. If you prefer to use a USB flash drive instead, be sure to use a high-quality device.

- https://www.mailstore.com/en/products/mailstore-home/

hackerone

[redacted] rewarded you with a bounty of **$75,000** for [redacted]. If you're as excited as we are, go ahead and tweet about it!

Beyond the bounty amount, do not disclose any weakness information without the express permission of the bounty program operator.

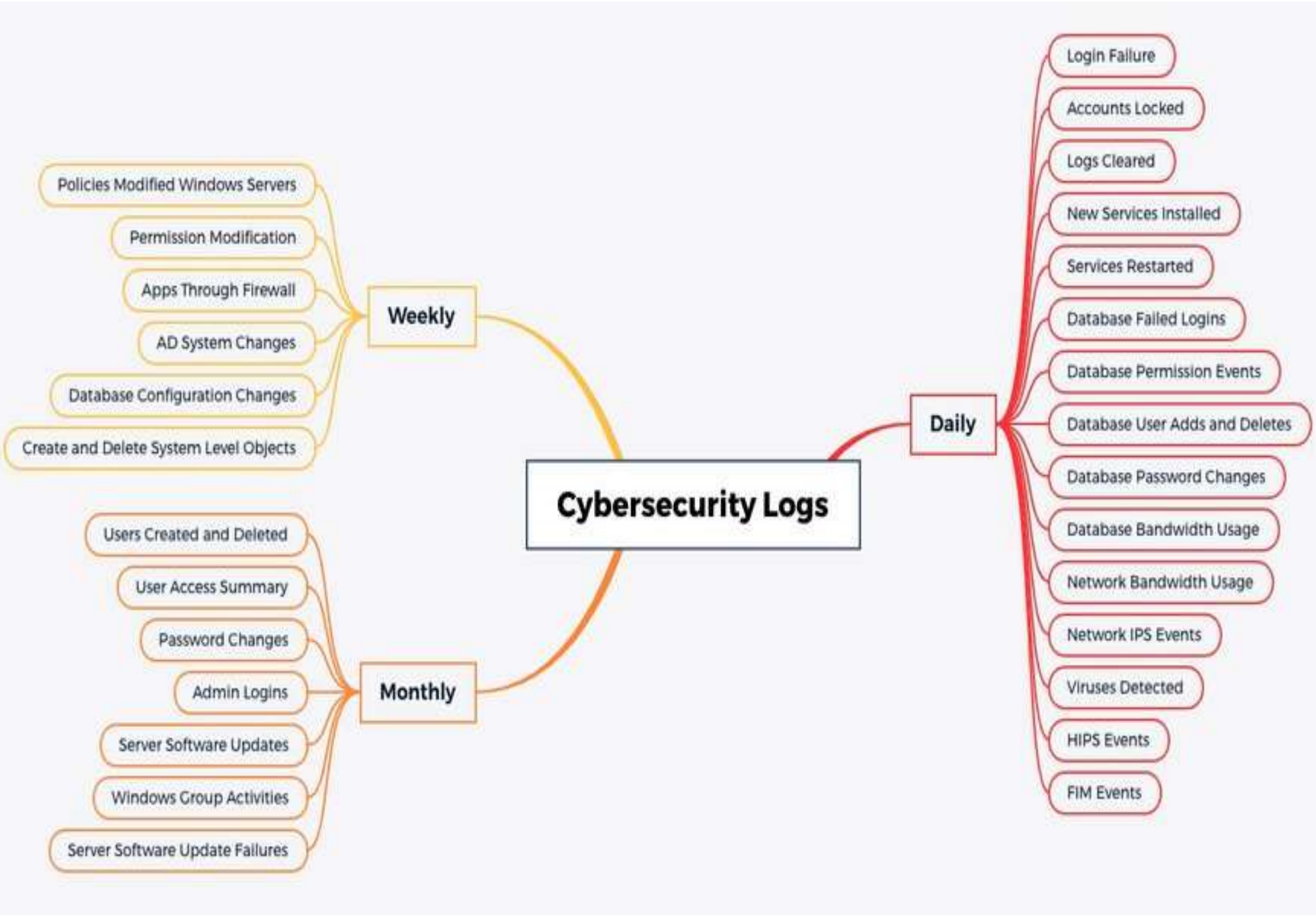
Congrats @meals!! Have a great weekend :)

What's next?
Before we can begin the payment process, United States tax law requires that we collect some information from you. Please click the link below to


Saved to this PC

Here are 21 cybersecurity search engines:

1. Shodan—Search for devices connected to the internet.
2. Wigle—Database of wireless networks, with statistics.
3. Grep App—Search across a half million git repos.
4. Binary Edge—Scans the internet for threat intelligence.
5. ONYPHE—Collects cyber-threat intelligence data.
6. GreyNoise—Search for devices connected to the internet.
7. Censys—Assessing attack surface for internet connected devices.
8. Hunter—Search for email addresses belonging to a website.
9. Fofa—Search for various threat intelligence.
10. ZoomEye—Gather information about targets.
11. LeakIX—Search publicly indexed information.
12. IntelligenceX—Search Tor, I2P, data leaks, domains, and emails.
13. Netlas—Search and monitor internet connected assets.
14. URL Scan—Free service to scan and analyse websites.
15. PublicWWW—Marketing and affiliate marketing research.
16. FullHunt—Search and discovery attack surfaces.
17. CRT sh—Search for certs that have been logged by CT.
18. Vulners—Search vulnerabilities in a large database.
19 Pulsedive—Search for threat intelligence.
20. Packet Storm Security—Browse latest vulnerabilities and exploits.
21. GrayHatWarefare—Search public S3 buckets.


Cybersecurity Logs
Daily
Login Failure
Accounts Locked
Logs Cleared
New Services Installed
Services Restarted
Database Failed Logins
Database Permission Events
Database User Adds and Deletes
Database Password Changes
Database Bandwidth Usage
Network Bandwidth Usage
Network IPS Events
Viruses Detected
HIPS Events
FIM Events
Weekly
Policies Modified Windows Servers
Permission Modification
Apps Through Firewall
AD System Changes
Database Configuration Changes
Create and Delete System Level Objects
Monthly
Users Created and Deleted
User Access Summary
Password Changes
Admin Logins
Server Software Updates
Windows Group Activities
Server Software Update Failures

Apple macOS security protections

- Windows Defender
- macOS
  - Xprotect
  - Gatekeeper
  - app notarization
  - System Integrity Protection
  - Signed system volume
  - Access controls for software and hardware
  - Malware Removal Tool
- Updates last 6 months
- Xprotect scan varies
- DubRobber scan every hour or two
- Older mac versions
  - El Capitan, Mojave,

- System Information > Software > Installations
  Gatekeeper Compatibility Data
  MRT Configuration Data
  MRTConfigData
  XProtectPayloads
  XProtectPlistConfigData

macOS Security Protections

XProtectPlistConfigData	2133	Apple	10/20/20, 8:47 AM
XProtectPlistConfigData	2134	Apple	11/2/20, 10:32 AM
XProtectPlistConfigData	2134	Apple	11/2/20, 10:32 AM
XProtectPlistConfigData	2135	Apple	11/13/20, 9:20 AM
XProtectPlistConfigData	2136	Apple	12/5/20, 4:21 PM
XProtectPlistConfigData	2137	Apple	12/21/20, 11:28 AM
XProtectPlistConfigData	2138	Apple	1/26/21, 10:04 AM
XProtectPlistConfigData	2139	Apple	2/8/21, 11:32 AM
XProtectPlistConfigData	2140	Apple	2/25/21, 5:27 PM
XProtectPlistConfigData	2141	Apple	3/8/21, 11:31 PM
XProtectPlistConfigData	2141	Apple	3/8/21, 11:31 PM
XProtectPlistConfigData	2142	Apple	3/19/21, 2:27 PM
XProtectPlistConfigData	2143	Apple	4/12/21, 1:00 PM
XProtectPlistConfigData	2144	Apple	4/18/21, 4:25 PM
XProtectPlistConfigData	2145	Apple	5/2/21, 4:02 PM
XProtectPlistConfigData	2146	Apple	5/14/21, 4:54 PM
XProtectPlistConfigData	2146	Apple	5/14/21, 4:54 PM
XProtectPlistConfigData	2147	Apple	5/31/21, 1:47 PM
XProtectPlistConfigData	2148	Apple	6/12/21, 11:19 AM
XProtectPlistConfigData	2149	Apple	6/28/21, 2:26 PM
XProtectPlistConfigData	2150	Apple	8/23/21, 1:26 PM
XProtectPlistConfigData	2151	Apple	9/24/21, 1:59 PM
XProtectPlistConfigData	2151	Apple	9/24/21, 1:59 PM
XProtectPlistConfigData	2153	Apple	12/20/21, 12:53 PM
XProtectPlistConfigData	2154	Apple	1/28/22, 11:46 AM
XProtectPlistConfigData	2155	Apple	2/4/22, 2:01 PM
XProtectPlistConfigData	2157	Apple	3/7/22, 11:27 AM
XProtectPlistConfigData	2158	Apple	3/18/22, 10:47 AM
XProtectPlistConfigData	2159	Apple	5/12/22, 11:21 PM
XProtectPlistConfigData	2160	Apple	6/10/22, 8:42 AM
XProtectPlistConfigData	2161	Apple	6/30/22, 5:35 PM
XProtectPlistConfigData	2162	Apple	8/21/22, 1:46 PM

Apple Mail Privacy Protection

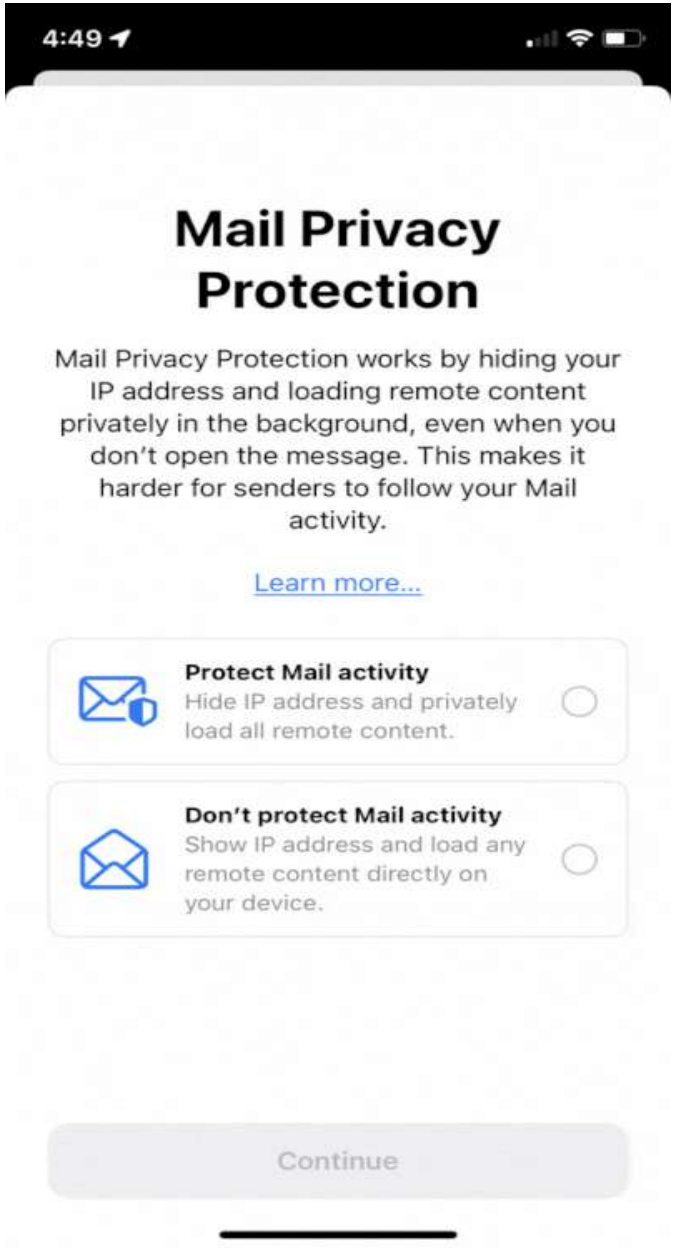
- Enhancements
- Monterey 12.5.1 iOS 15
- Anti-tracking controls
- Eavesdropping alerts
- Hides IP address
- Prevents sender from knowing you have opened
- Alert on microphone access
- iOS 15

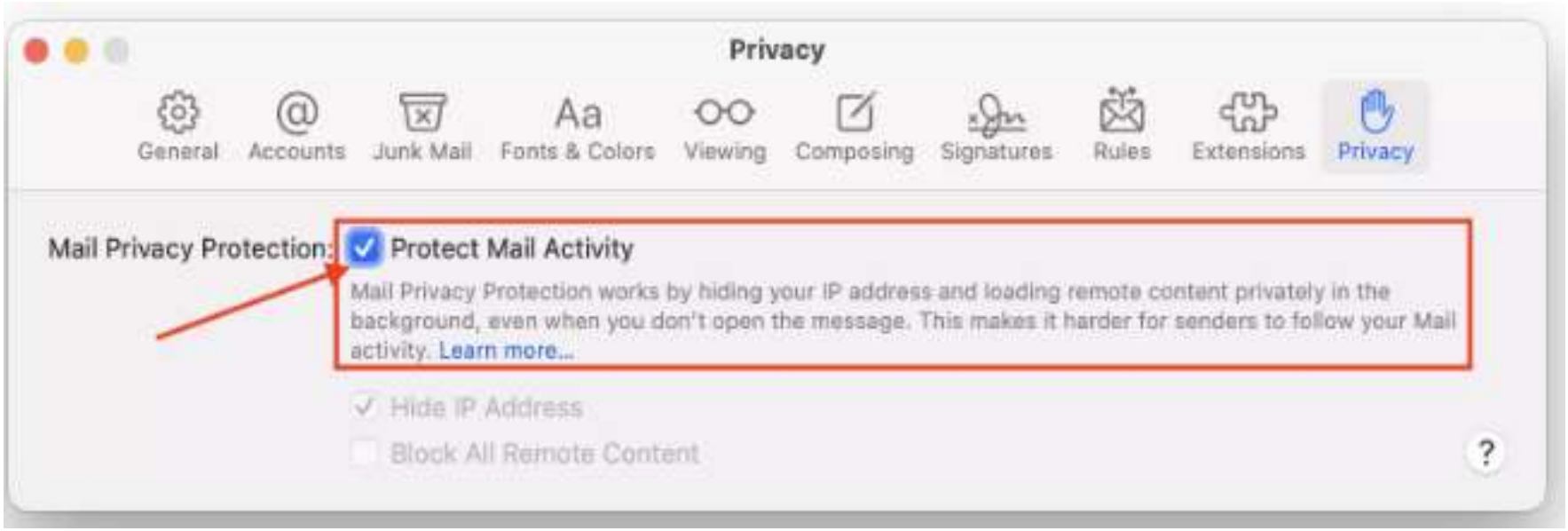
  Settings > Mail > Privacy Protection

  Protect Mail Activity
- macOS Monterey

  Settings > Mail > Preferences > Privacy

  Protect Mail Activity


4:49
Mail Privacy Protection
Mail Privacy Protection works by hiding your IP address and loading remote content privately in the background, even when you don't open the message. This makes it harder for senders to follow your Mail activity.
Learn more...
Protect Mail activity
Hide IP address and privately load all remote content.
Don't protect Mail activity
Show IP address and load any remote content directly on your device.
Continue


Privacy
General
Accounts
Junk Mail
Fonts & Colors
Viewing
Composing
Signatures
Rules
Extensions
Privacy
Mail Privacy Protection:
Protect Mail Activity
Mail Privacy Protection works by hiding your IP address and loading remote content privately in the background, even when you don't open the message. This makes it harder for senders to follow your Mail activity. Learn more...
Hide IP Address
Block All Remote Content
?

Class Action Suit

- Multiple restaurant chains
- Usage of AI enabled voice ordering systems
- Collection and use of voice print
- Violation of state Biometric Information Privacy Act

Identify your perimeter

Less is more! The fewer connected devices and entry points you have, the safer your network is.

Update software and devices regularly

Regular updates make you less vulnerable to attack. Only download updates from the manufacturer and enable auto-updates when possible.

Secure your Wi-Fi network

Routers often have default credentials that people don't know about. Disable the "remote configuration" option in your router and change both your Wi-Fi password and your router password.

Watch out for insecure websites

Always use HTTPS for sensitive communications. Don't ignore browser warnings and always remember to check the website address carefully for misspellings and oddly-placed letters or numbers. When in doubt, manually enter the URL in your browser.

Back up your files

Backups save your information if your device breaks or is taken over by an attacker. Back up files to a removable device that can be locked away safely, such as a CD or flash drive.

Don't download carelessly

Files can contain malware, and websites aren't always what they appear to be. Always verify sender identity before downloading files and remember: If it comes from an oddly-spelled email or is hosted on a site that makes your browser generate a warning, stay away!

Encrypt devices to deter thieves

Encryption renders files unreadable without the correct key. Some devices offer the option to encrypt individual files or the entire device. Consider which solution suits your needs best.

Practice password safety

Choose long passwords containing uncommon words. Use unique passwords for sensitive accounts and a password manager to help you remember them.

Always use antivirus software

Antivirus needs updates, too! Set it to auto-update.

Keep yourself informed

New cybersecurity bugs and attacks pop up every week. Staying informed about the latest threats will help you be safe!

- Ever want to be a presenter??

Presenter???

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

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

- Questions, suggestions, comments?

SCCCCyber@gmail.com