Sun City Computer Club

Cyber Security SIG

October 7, 2021

Questions, Comments, Suggestions welcomed at any time

Even Now

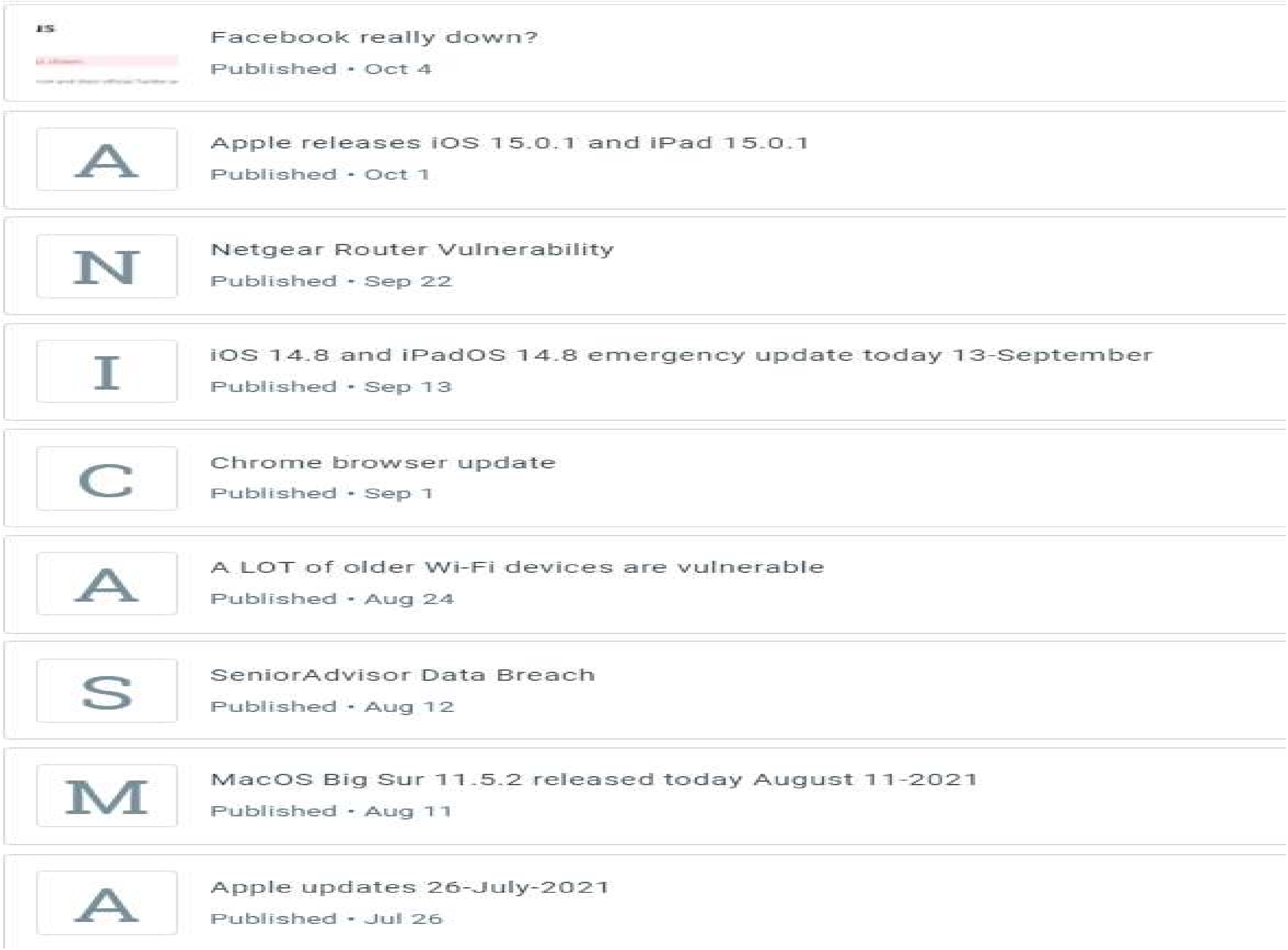
- Audio recording of this session as MP4 file
- Audio recording available at link shown above

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???



Facebook really down?

Published • Oct 4

Apple releases iOS 15.0.1 and iPad 15.0.1

Published • Oct 1

Netgear Router Vulnerability

Published • Sep 22

iOS 14.8 and iPadOS 14.8 emergency update today 13-September

Published • Sep 13

Chrome browser update

Published • Sep 1

A LOT of older Wi-Fi devices are vulnerable

Published • Aug 24

SeniorAdvisor Data Breach

Published • Aug 12

MacOS Big Sur 11.5.2 released today August 11-2021

Published • Aug 11

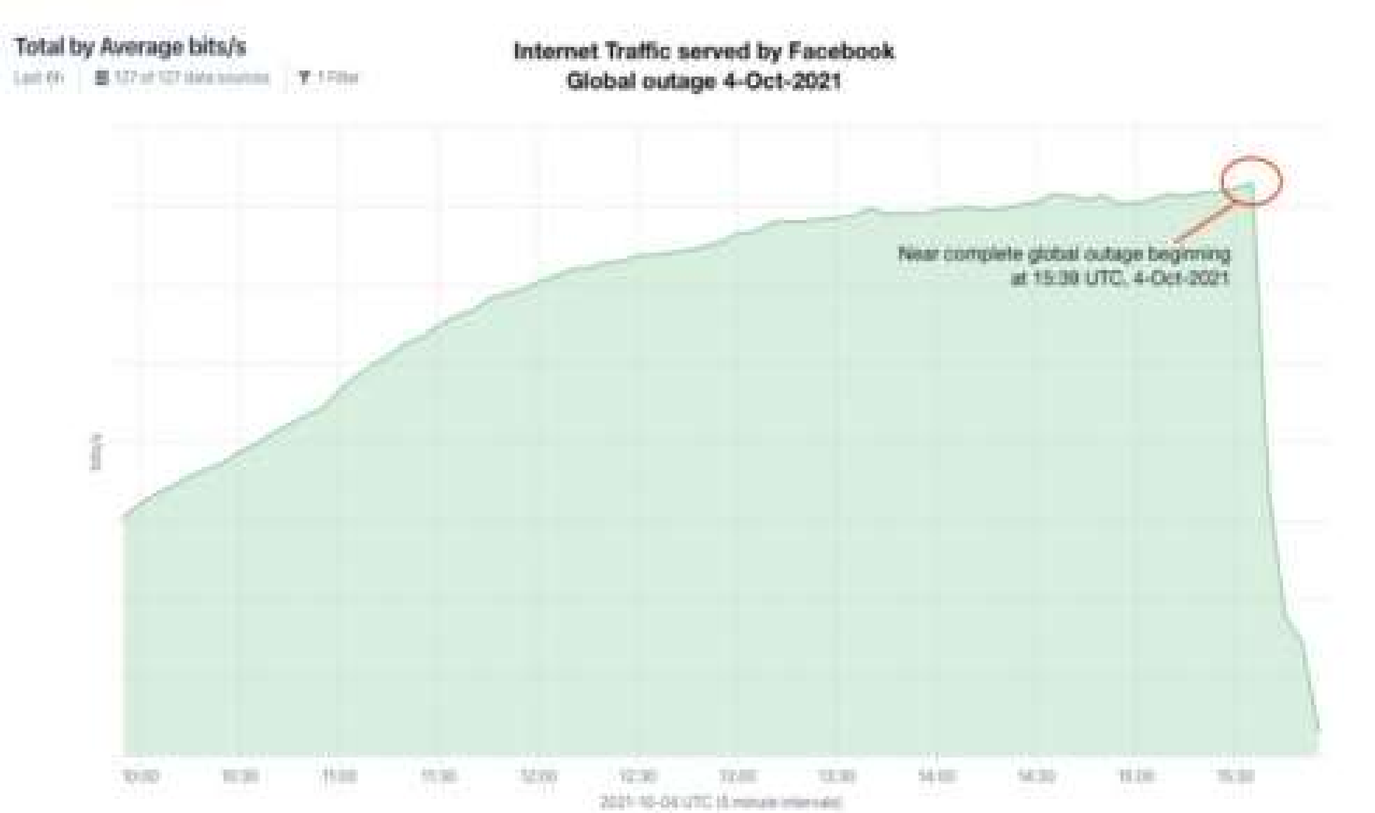
Apple updates 26-July-2021

Published • Jul 26

- Facebook, Instagram, WhatsApp, Oculus VR, …
  78 companies cost not disclosed
  October 4, 2021 10:39 Central time
  Facebook locked their keys in the car
  Border Gate Protocol BGP
  Unauthenticated unencrypted older
  Router peers update each other
  routing tables peer or admins
  Autonomous System number AS32934

Advertising routes

Facebook


Total by Average bits/s
Last 6h
127 of 127 data sources
1 Filter
Internet Traffic served by Facebook
Global outage 4-Oct-2021
Near complete global outage beginning
at 15:39 UTC, 4-Oct-2021
bits/s
10:00
10:30
11:00
11:30
12:00
12:30
13:00
13:30
14:00
14:30
15:00
15:30
2021-10-04 UTC (5 minute intervals)

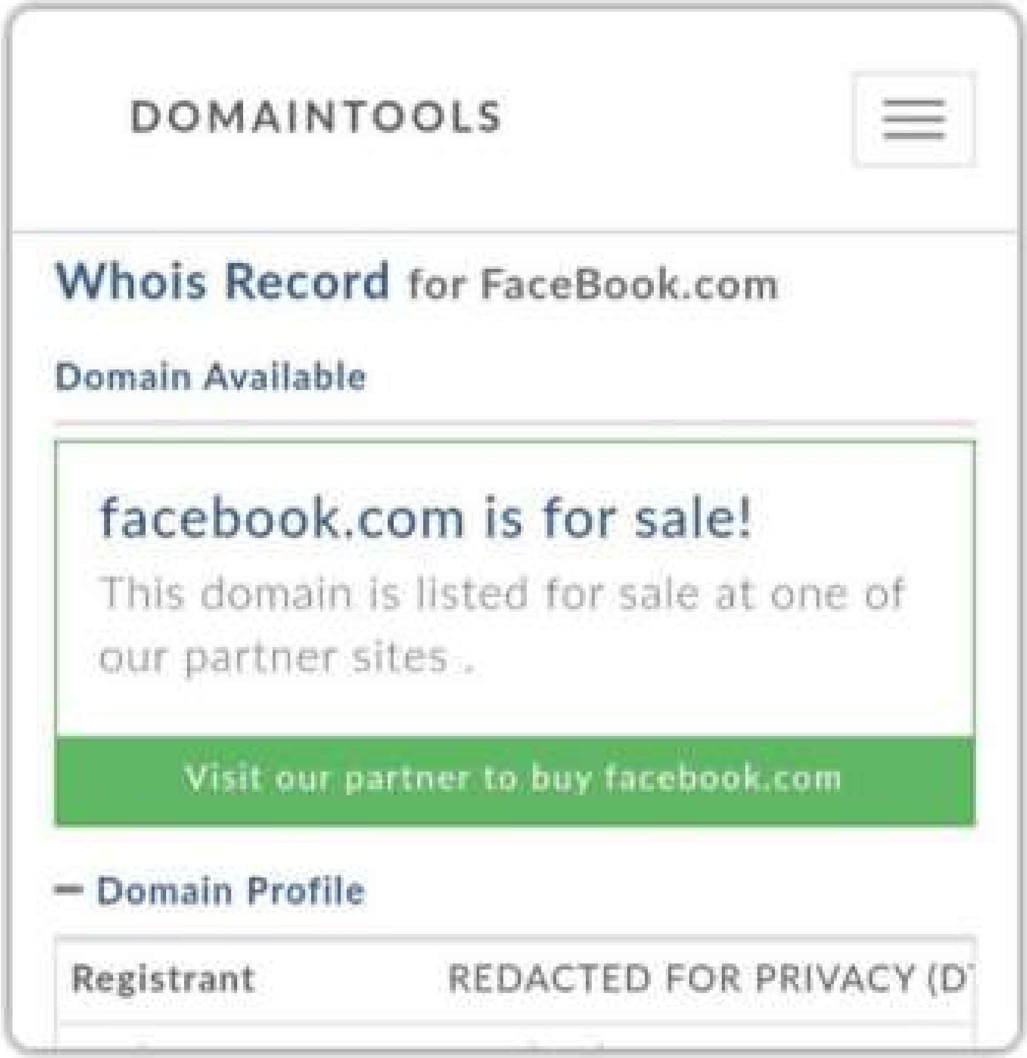
Facebook

- Sharp drop
- DNS caches information

  TTL 5 minutes   Expire 7 days

  Instagram DNS hosted at Amazon
- BGP error
- Update “went wrong”
- Employees locked out logically & physically
- Facebook their own DNS registrar

Facebook



DOMAINTOOLS

Whois Record for FaceBook.com

Domain Available

facebook.com is for sale!

This domain is listed for sale at one of our partner sites .

— Domain Profile

Registrant	REDACTED FOR PRIVACY (D

Log in with Facebook

BGP

- Mistakes happen often

  Japan

- Intentional route disturbance

Current Issues

- Consumer Reports Antivirus products
  Paid subscription
  Added Data Privacy score
  30 products
  MacOS and Windows
  Price vs value
  FBI 800 thousand reports 2020 up 69%
- High severity flaw Netgear routers
  Review firmware often
- Browser Updates

Current Issues

- Ransomware & cyber warfare

  30 countries cyber currency

  Colonial pipeline

  JBS foods

  Kaseya IT platform

  law enforcement and encryption

  AI

  Afghanistan HIIDE

- Syniverse – critical part of global telecom

  AT&T, Verizon, Vodafone, China Mobile, etc.

  200 clients & millions of users for years

- FCC news rules SIM swapping

  porting current phone number to another carrier

  PIN vital link

  carrier's support staff

  "other" means

  SHAKEN/STIR - June 30, 2021
- GriftHorse – Android trojan 139 apps

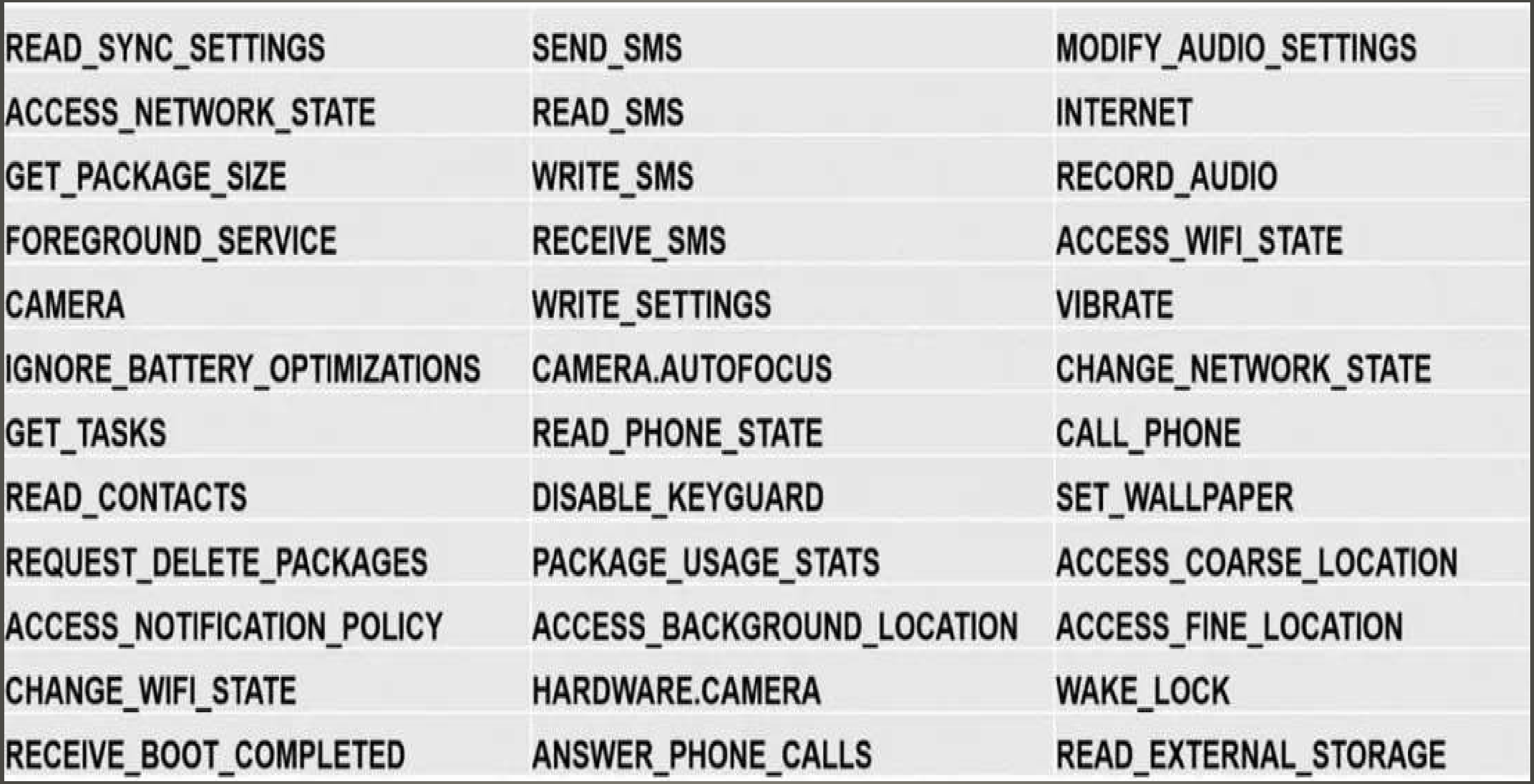
  18 million downloads

  Little amounts from large number of victims
- TangleBot Android malware – Adobe Flash update

  really – Adobe Flash? Game over COMPLETE control
- Bluetooth connected flip-flops – test cheating

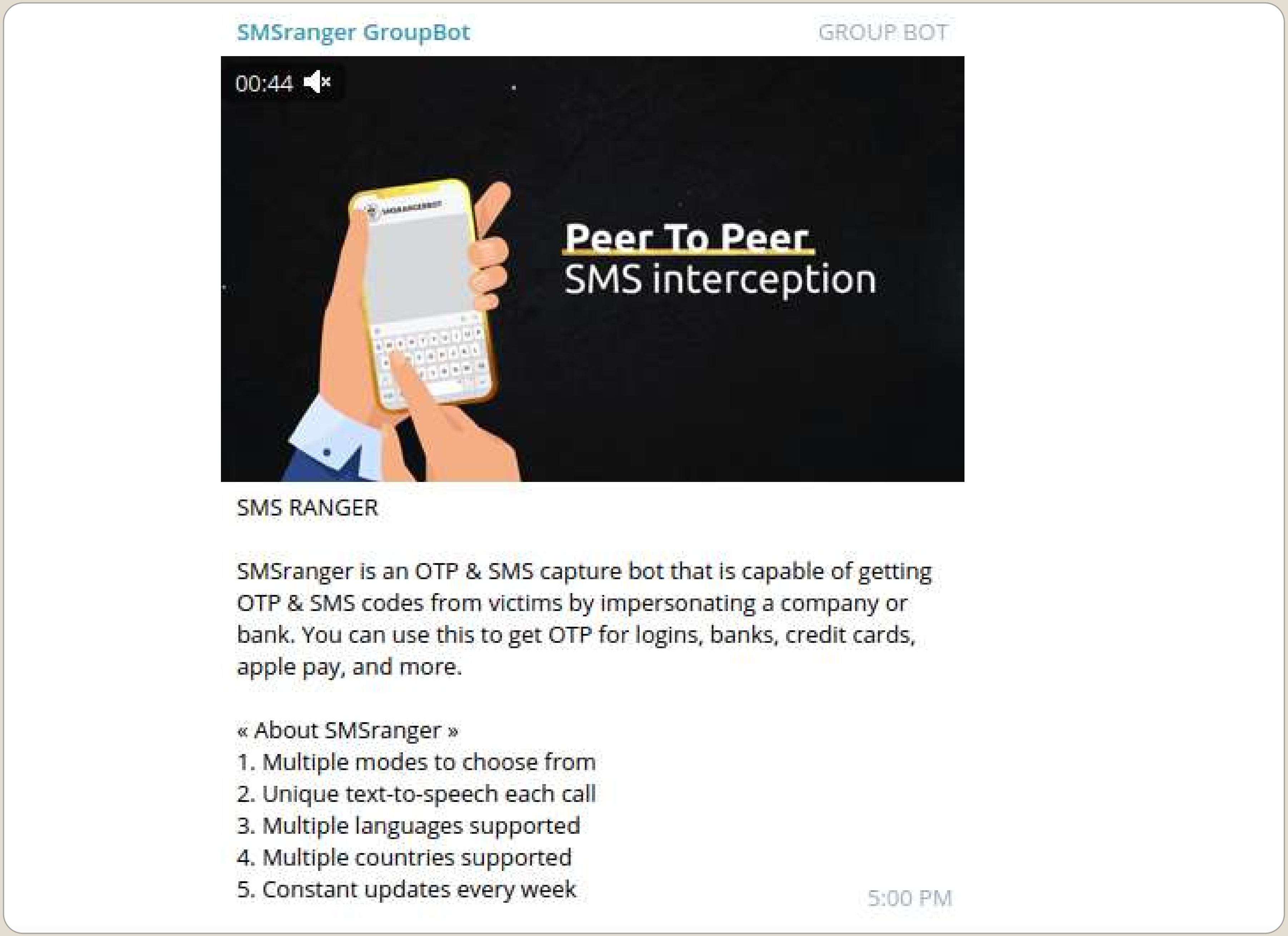
Current Issues

- Multiple obfuscation layers



READ_SYNC_SETTINGS	SEND_SMS	MODIFY_AUDIO_SETTINGS
ACCESS_NETWORK_STATE	READ_SMS	INTERNET
GET_PACKAGE_SIZE	WRITE_SMS	RECORD_AUDIO
FOREGROUND_SERVICE	RECEIVE_SMS	ACCESS_WIFI_STATE
CAMERA	WRITE_SETTINGS	VIBRATE
IGNORE_BATTERY_OPTIMIZATIONS	CAMERA.AUTOFOCUS	CHANGE_NETWORK_STATE
GET_TASKS	READ_PHONE_STATE	CALL_PHONE
READ_CONTACTS	DISABLE_KEYGUARD	SET_WALLPAPER
REQUEST_DELETE_PACKAGES	PACKAGE_USAGE_STATS	ACCESS_COARSE_LOCATION
ACCESS_NOTIFICATION_POLICY	ACCESS_BACKGROUND_LOCATION	ACCESS_FINE_LOCATION
CHANGE_WIFI_STATE	HARDWARE.CAMERA	WAKE_LOCK
RECEIVE_BOOT_COMPLETED	ANSWER_PHONE_CALLS	READ_EXTERNAL_STORAGE

TangleBot



SMSranger GroupBot GROUP BOT

SMS RANGER

SMSranger is an OTP & SMS capture bot that is capable of getting OTP & SMS codes from victims by impersonating a company or bank. You can use this to get OTP for logins, banks, credit cards, apple pay, and more.

« About SMSranger »
1. Multiple modes to choose from
2. Unique text-to-speech each call
3. Multiple languages supported
4. Multiple countries supported
5. Constant updates every week

5:00 PM

Current Issues

- Apple Pay & Visa
  smartphone payment apps
  fingerprint, PIN, face ID
  then Apple Pay – *Express Transit/Travel*
  transport-ticketing barrier
  Locked iPhone Visa card
  Any amount without user authorization
  Contactless limit bypassed
  Visa proposed countermeasures
  bypassed with NFC paired Android devices

Apple

- iOS 15 iPadOS 15 released 9/21/2021
- iOS 15.0.1 01/1/2021
- iOS 14.8 iPadOS 14.8 WatchOS - security
- Updates Big Sur and Catalina – security
- Safari update 15.0 16612
  (17612) for Monterey
  iOS 15 feature catch-up
  and new design
  do and undo via Preferences

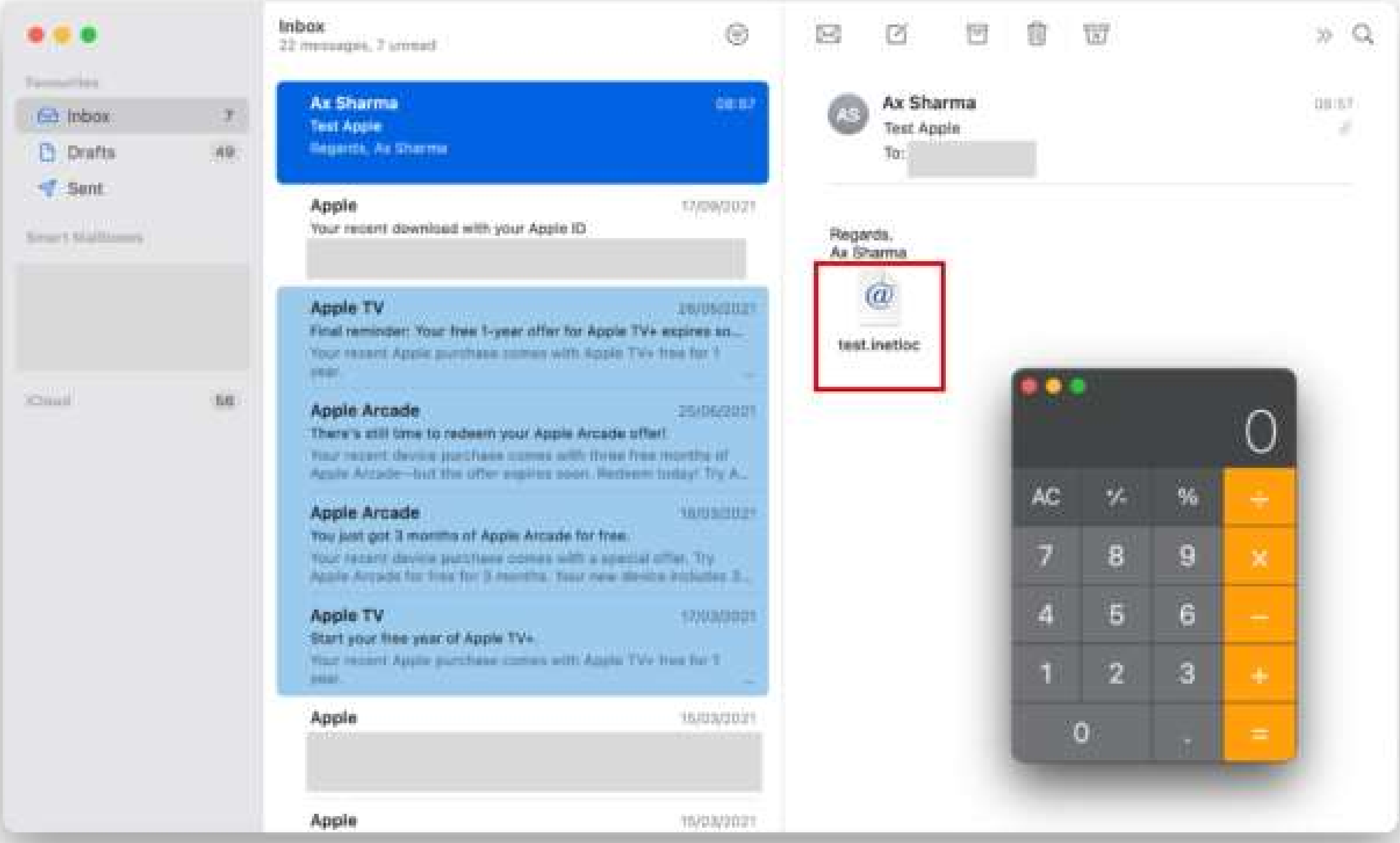
- Shortcut files
- Inetloc file extension
- Trigger without warning
- Usually used for http links
- http protocol has file as a method
- File:// in browser opens a file

  helpful <-> harmful

MacOS vulnerability

Proof of Concept

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PrepertyList-1.0.dtd">
<plist version="1.0">
 <dict>
   <key>URL</key>

<string>File:////////////////////////System/Applications/Calculator.
app</string>
  </dict>
</plist>
```



Inbox
22 messages, 7 unread

Ax Sharma 08:57
Test Apple
Regards, Ax Sharma

Apple 17/09/2021
Your recent download with your Apple ID
[redacted]

Apple TV 26/05/2021
Final reminder: Your free 1-year offer for Apple TV+ expires so...
Your recent Apple purchase comes with Apple TV+ free for 1 year.

Apple Arcade 25/06/2021
There's still time to redeem your Apple Arcade offer!
Your recent device purchase comes with three free months of Apple Arcade—but the offer expires soon. Redeem today! Try A...

Apple Arcade 16/03/2021
You just got 3 months of Apple Arcade for free.
Your recent device purchase comes with a special offer. Try Apple Arcade for free for 3 months. Your new device includes 3...

Apple TV 17/03/2021
Start your free year of Apple TV+
Your recent Apple purchase comes with Apple TV+ free for 1 year.

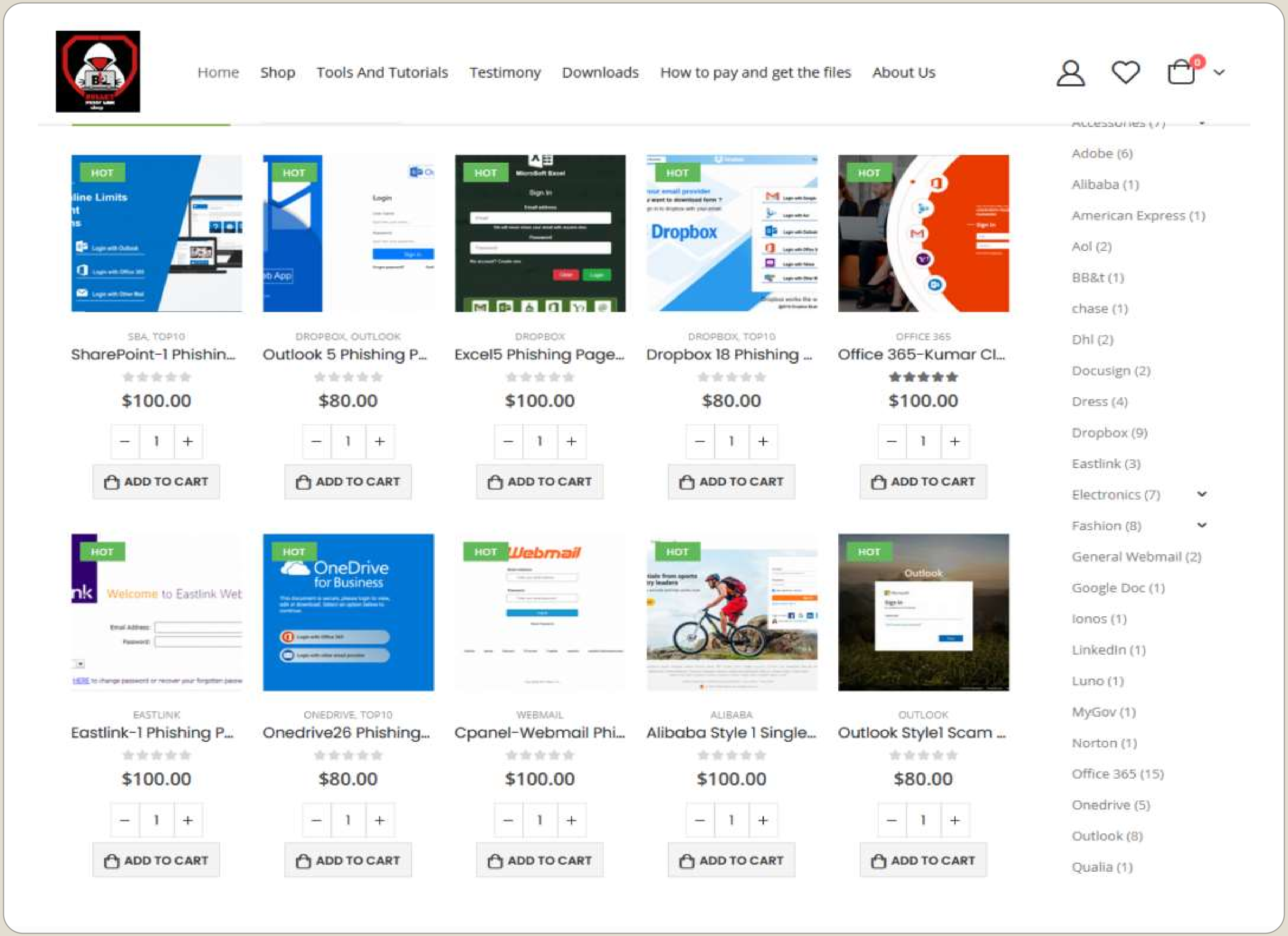
Apple 15/03/2021
[redacted]

Apple 15/03/2021

AS
Ax Sharma 08:57
Test Apple
To: [redacted]

Regards,
Ax Sharma

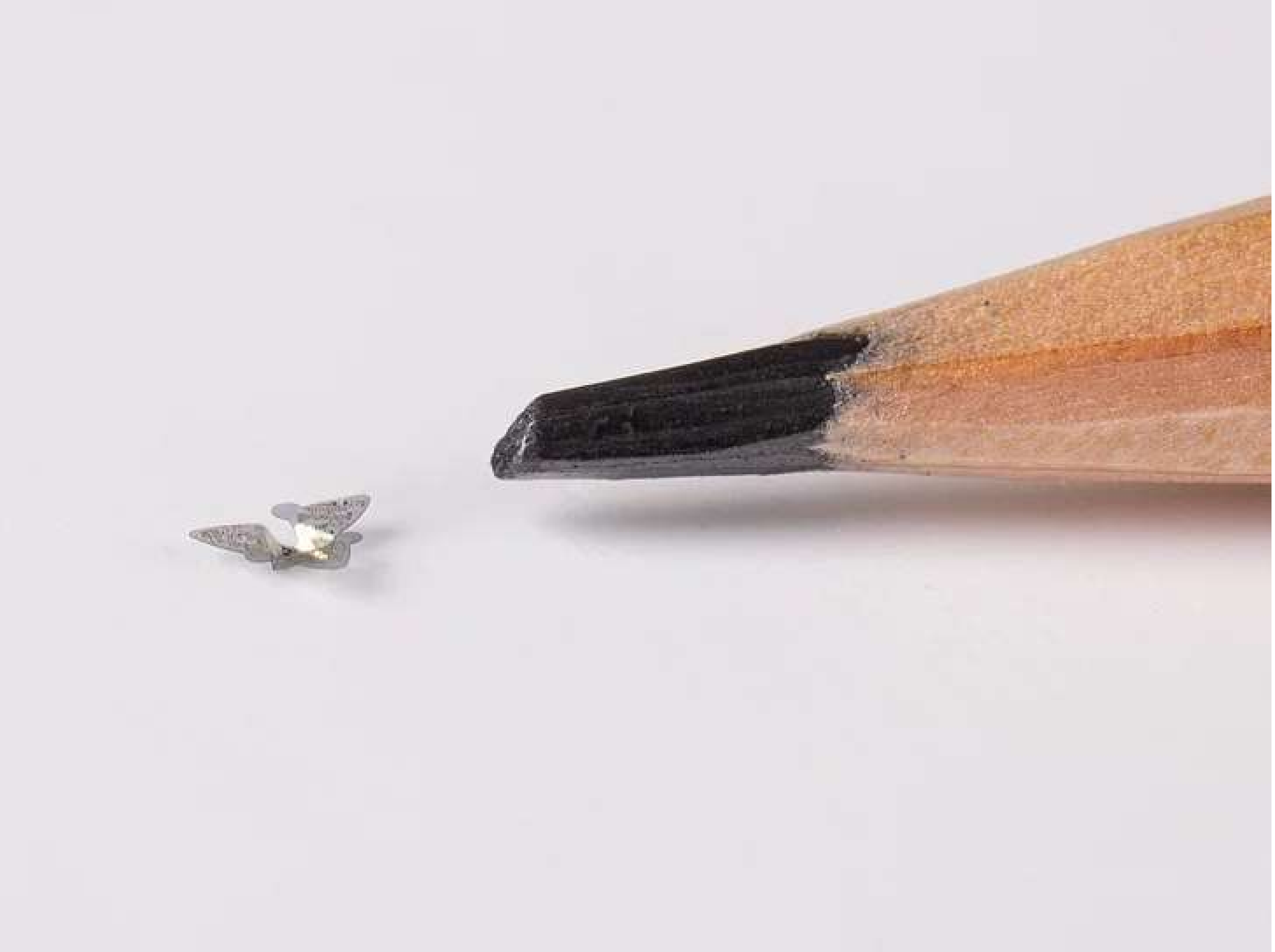
test.inetloc

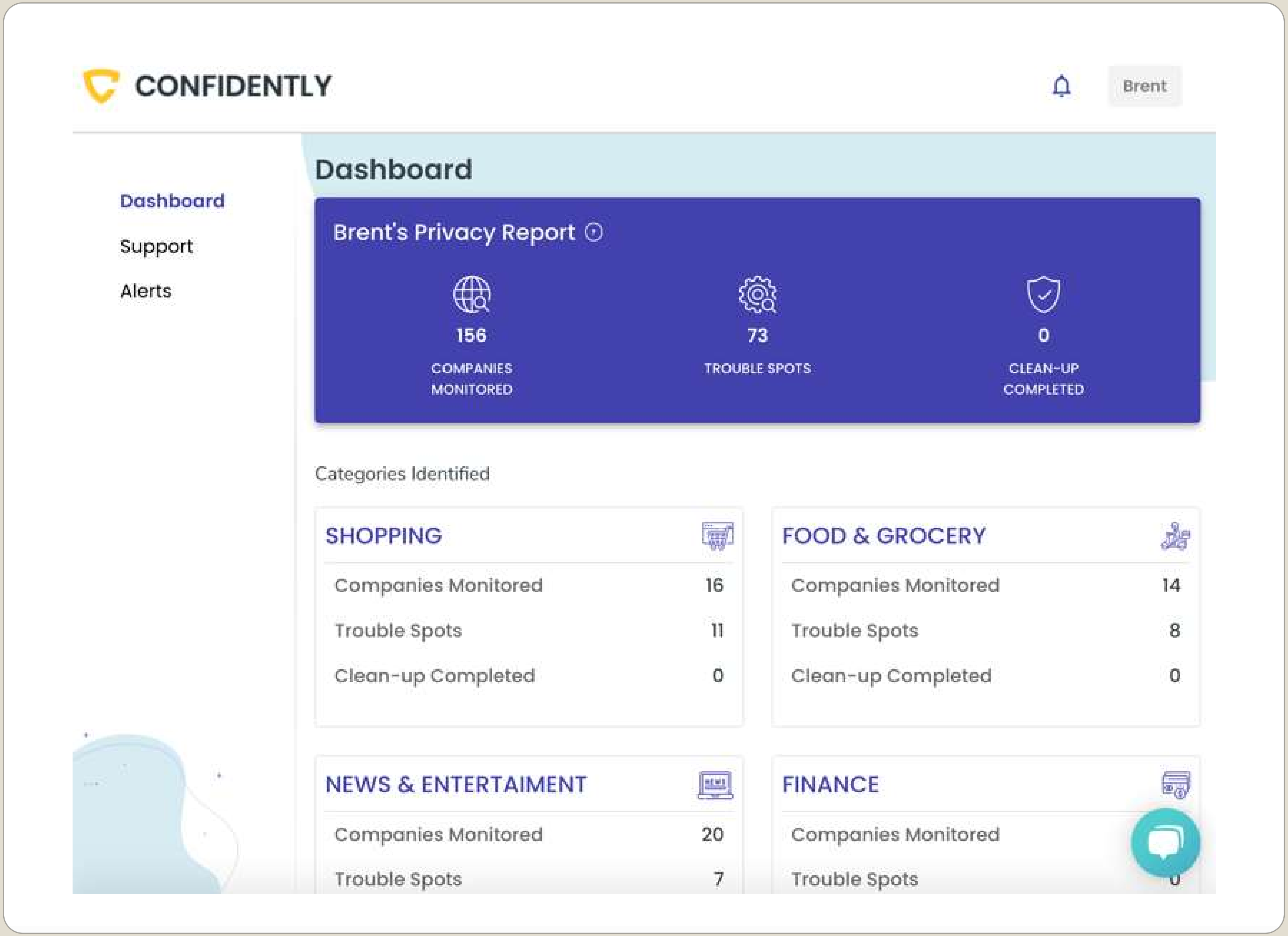


Home Shop Tools And Tutorials Testimony Downloads How to pay and get the files About Us

Category	Product	Price
SBA, TOP10	SharePoint-1 Phishin...	$100.00
DROPBOX, OUTLOOK	Outlook 5 Phishing P...	$80.00
DROPBOX	Excel5 Phishing Page...	$100.00
DROPBOX, TOP10	Dropbox 18 Phishing ...	$80.00
OFFICE 365	Office 365-Kumar Cl...	$100.00
EASTLINK	Eastlink-1 Phishing P...	$100.00
ONEDRIVE, TOP10	Onedrive26 Phishing...	$80.00
WEBMAIL	Cpanel-Webmail Phi...	$100.00
ALIBABA	Alibaba Style 1 Single...	$100.00
OUTLOOK	Outlook Style1 Scam ...	$80.00

- Accessories (7)
- Adobe (6)
- Alibaba (1)
- American Express (1)
- Aol (2)
- BB&t (1)
- chase (1)
- Dhl (2)
- Docusign (2)
- Dress (4)
- Dropbox (9)
- Eastlink (3)
- Electronics (7)
- Fashion (8)
- General Webmail (2)
- Google Doc (1)
- Ionos (1)
- LinkedIn (1)
- Luno (1)
- MyGov (1)
- Norton (1)
- Office 365 (15)
- Onedrive (5)
- Outlook (8)
- Qualia (1)





Dashboard

Brent's Privacy Report

156 COMPANIES MONITORED

73 TROUBLE SPOTS

0 CLEAN-UP COMPLETED

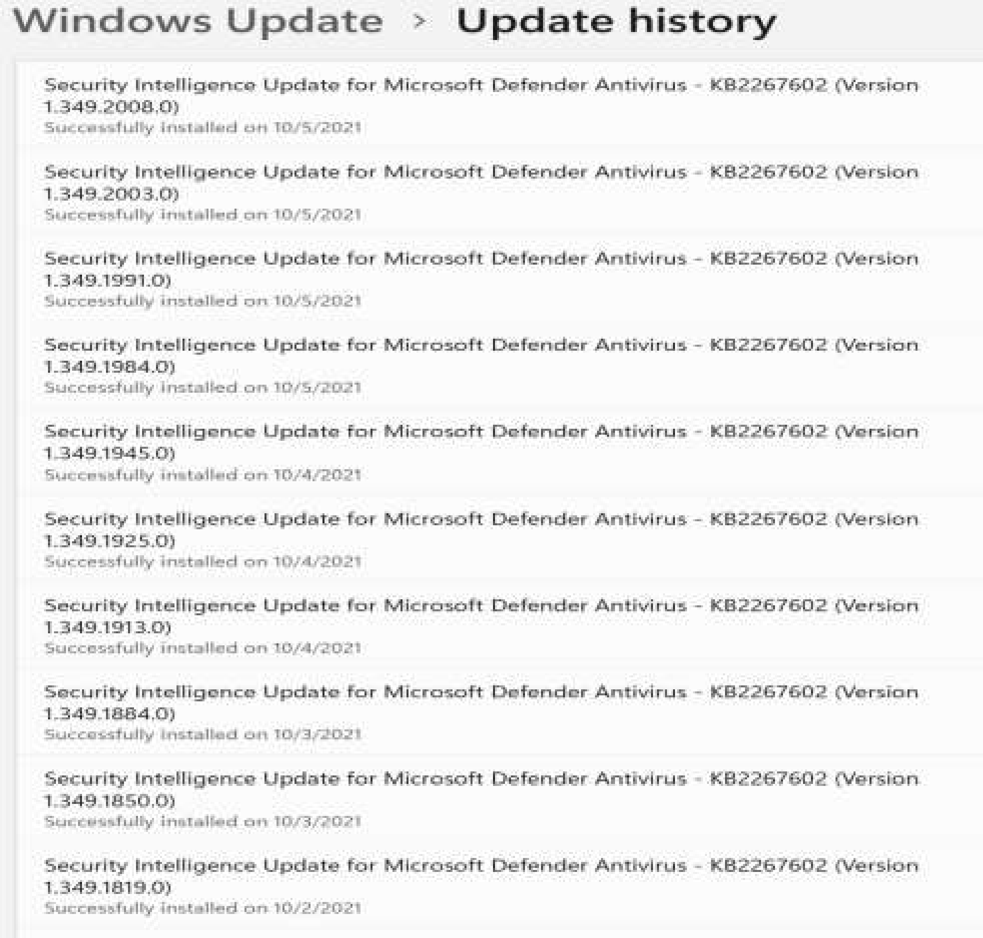
Categories Identified

SHOPPING	
Companies Monitored	16
Trouble Spots	11
Clean-up Completed	0

FOOD & GROCERY	
Companies Monitored	14
Trouble Spots	8
Clean-up Completed	0

NEWS & ENTERTAIMENT	
Companies Monitored	20
Trouble Spots	7

FINANCE	
Companies Monitored	
Trouble Spots	0



Windows Update > Update history

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.349.2008.0)
Successfully installed on 10/5/2021

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.349.2003.0)
Successfully installed on 10/5/2021

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.349.1991.0)
Successfully installed on 10/5/2021

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.349.1984.0)
Successfully installed on 10/5/2021

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.349.1945.0)
Successfully installed on 10/4/2021

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.349.1925.0)
Successfully installed on 10/4/2021

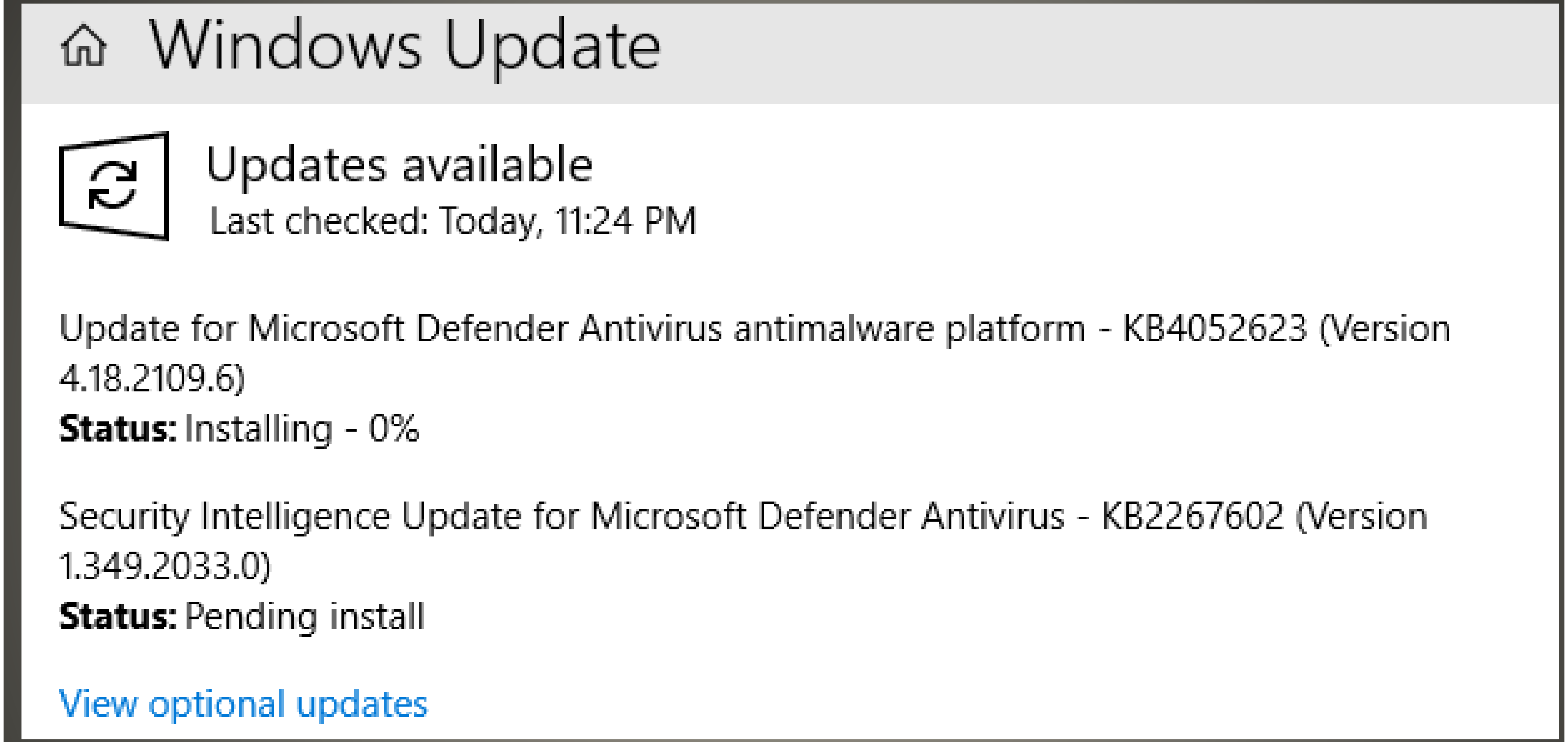
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.349.1913.0)
Successfully installed on 10/4/2021

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.349.1884.0)
Successfully installed on 10/3/2021

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.349.1850.0)
Successfully installed on 10/3/2021

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.349.1819.0)
Successfully installed on 10/2/2021

Windows Defender signature updates



Updates available

Last checked: Today, 11:24 PM

Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2109.6)

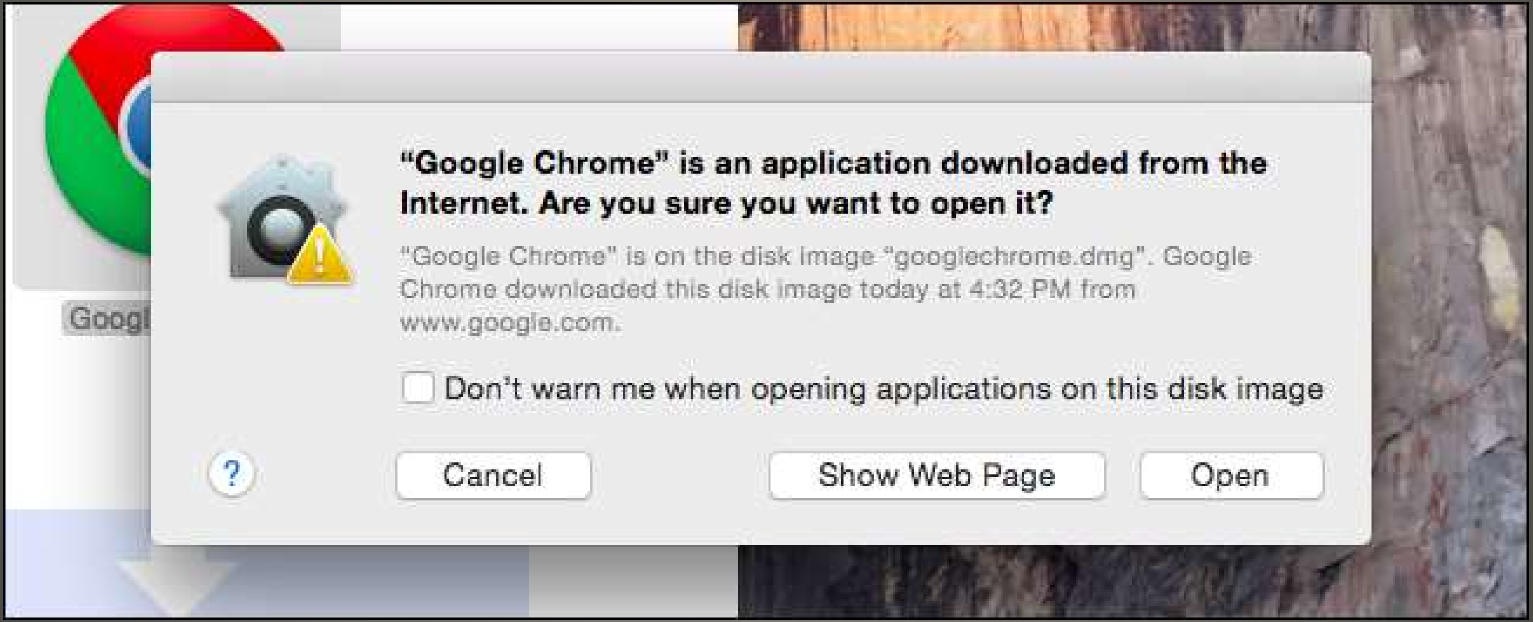
Status: Installing - 0%

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.349.2033.0)

Status: Pending install

macOS protections

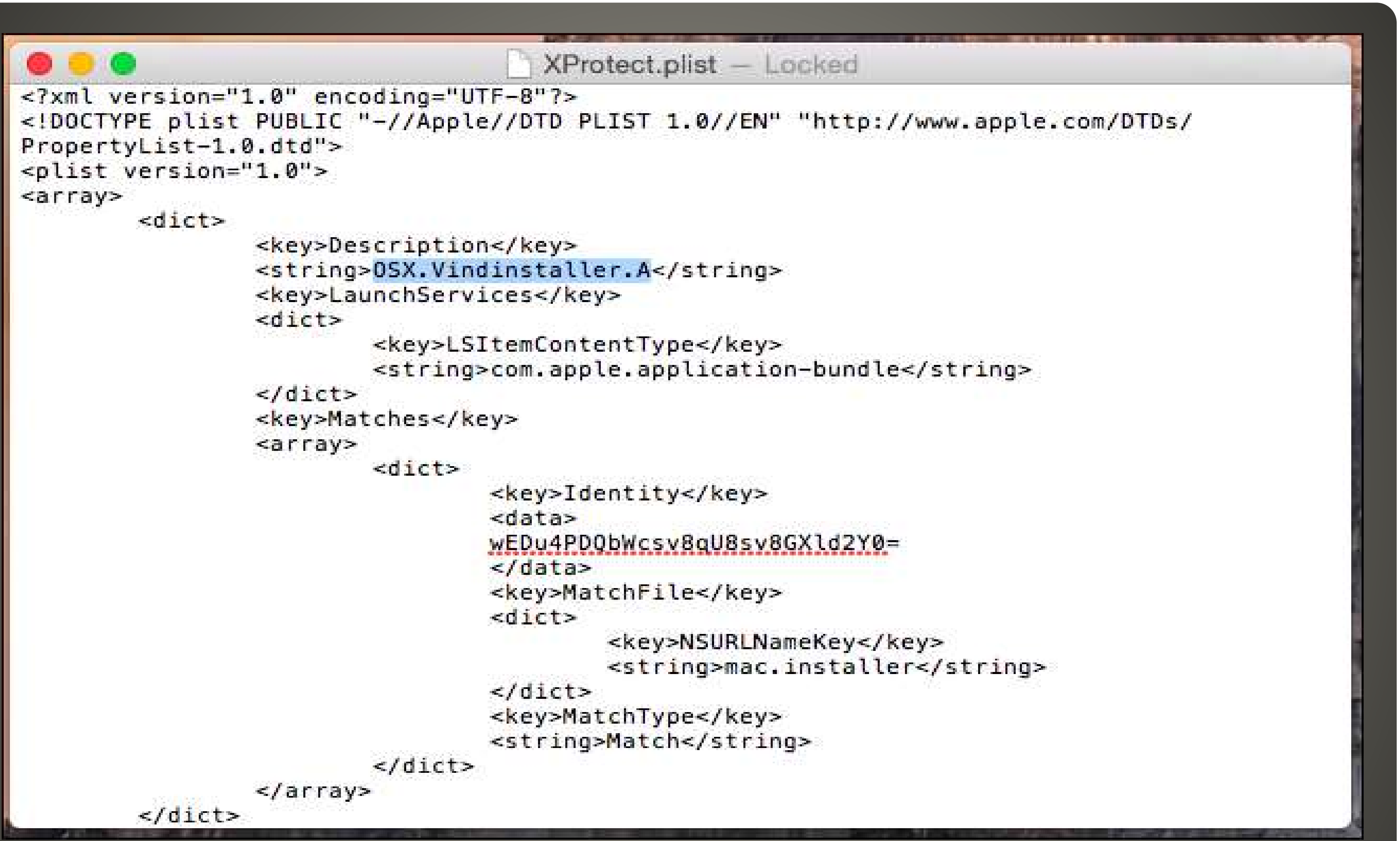
- Similar to Windows Defender
- XProtect
- File Quarantine aware applications



"Google Chrome" is an application downloaded from the Internet. Are you sure you want to open it?

"Google Chrome" is on the disk image "googlechrome.dmg". Google Chrome downloaded this disk image today at 4:32 PM from www.google.com.

☐ Don't warn me when opening applications on this disk image



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
<array>
        <dict>
                <key>Description</key>
                <string>OSX.Vindinstaller.A</string>
                <key>LaunchServices</key>
                <dict>
                        <key>LSItemContentType</key>
                        <string>com.apple.application-bundle</string>
                </dict>
                <key>Matches</key>
                <array>
                        <dict>
                                <key>Identity</key>
                                <data>
                                wEDu4PDQbWcsv8qU8sv8GXld2Y0=
                                </data>
                                <key>MatchFile</key>
                                <dict>
                                        <key>NSURLNameKey</key>
                                        <string>mac.installer</string>
                                </dict>
                                <key>MatchType</key>
                                <string>Match</string>
                        </dict>
                </array>
        </dict>
```

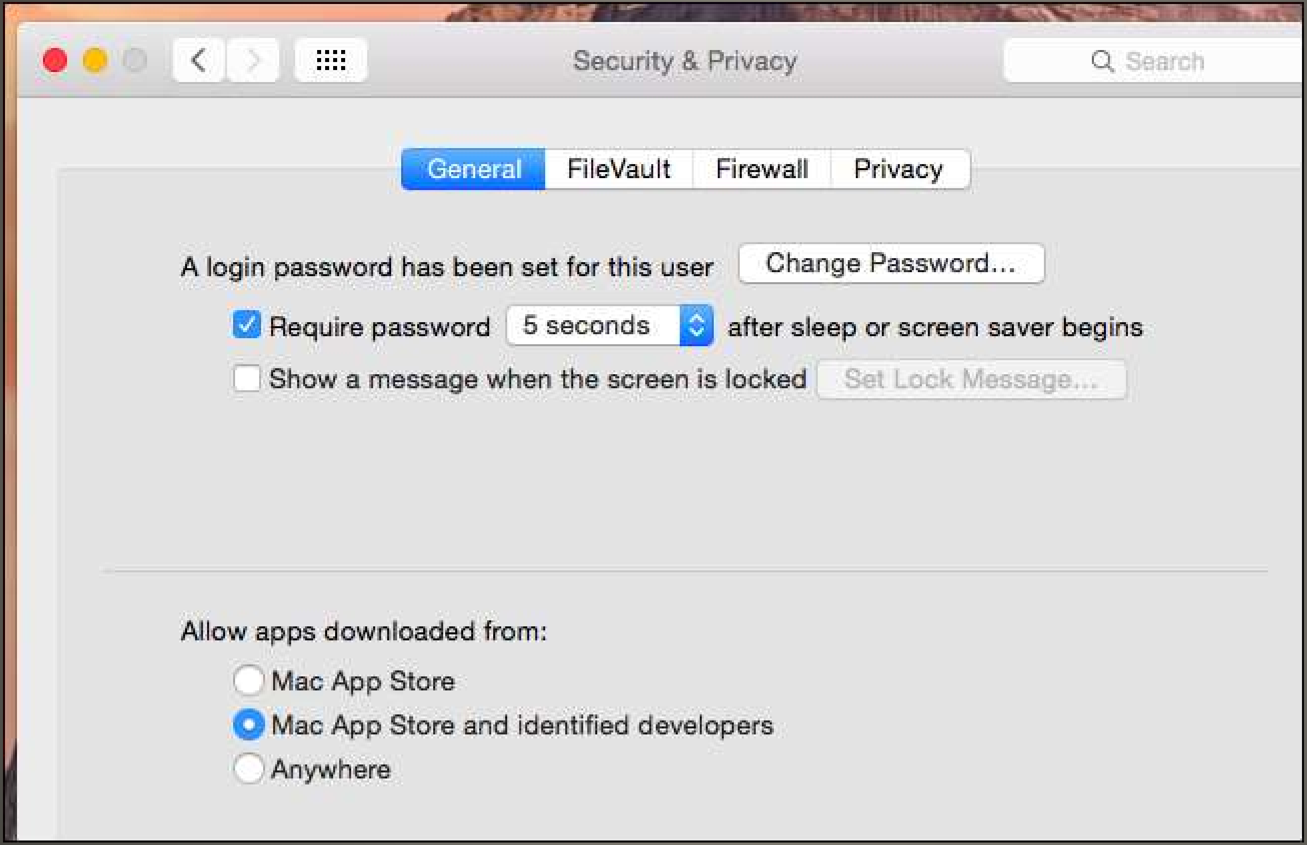
macOS file protections

- Short & fairly static list
- Not immune to rename or hash manipulations
- Interface between WEB and Mac

Windows SmartScreen

Xprotect

- Gatekeeper



A login password has been set for this user

☑ Require password 5 seconds after sleep or screen saver begins

□ Show a message when the screen is locked

Allow apps downloaded from:

○ Mac App Store

● Mac App Store and identified developers

○ Anywhere

macOS Protections

- Notarization

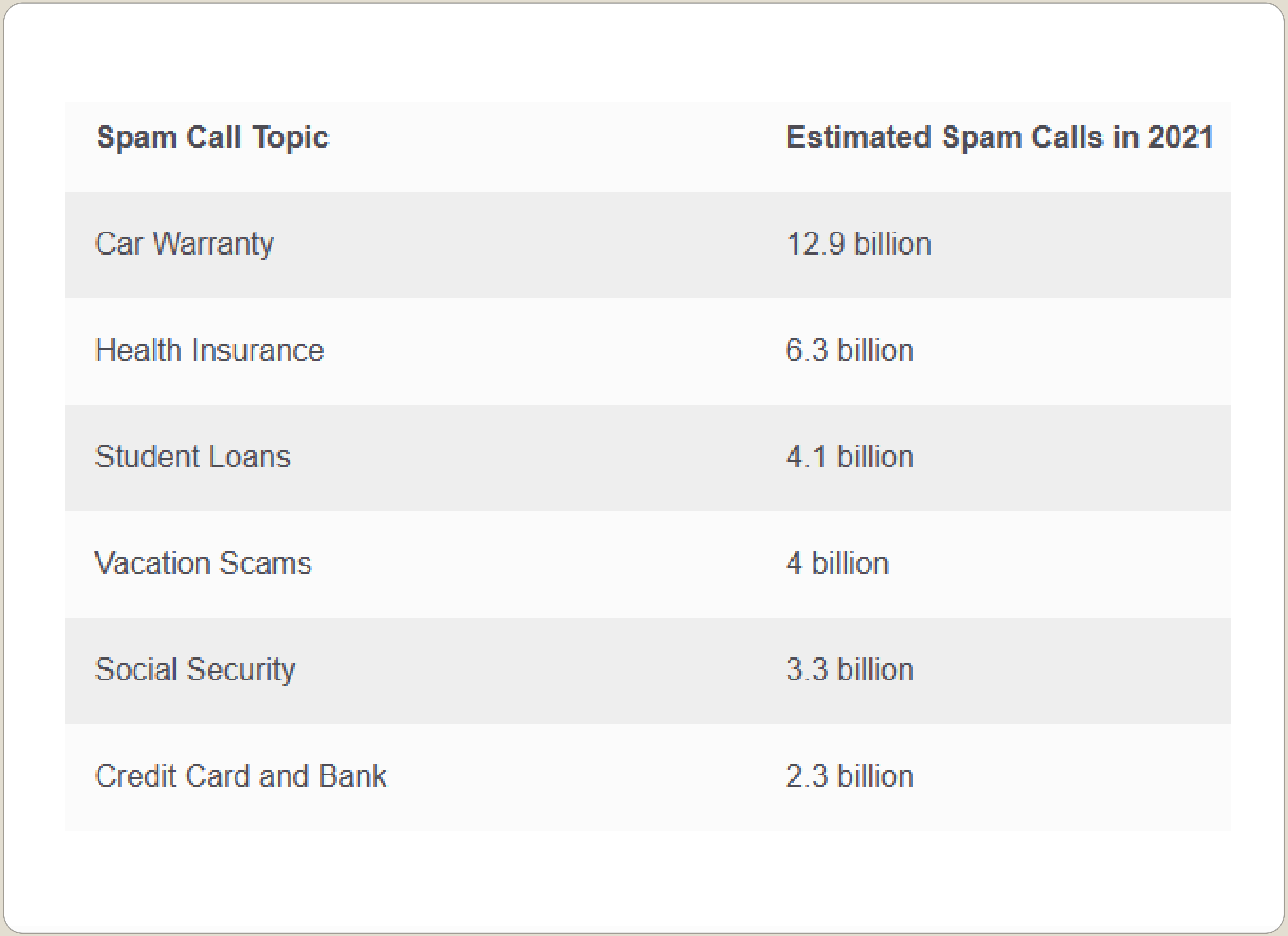
  Developers apply for from Apple

  Notarization can and is revoked

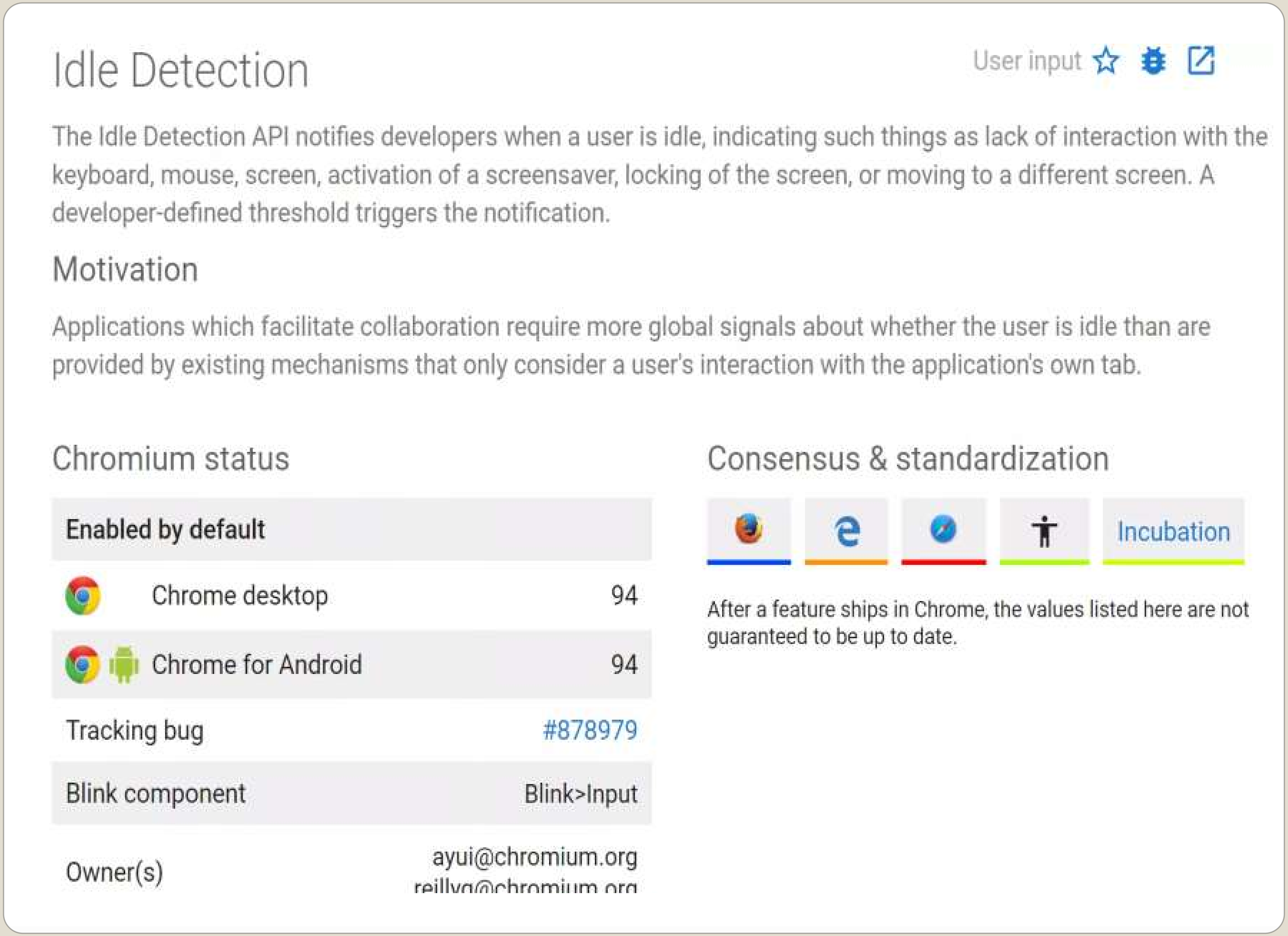
  More current than Xprotect
- Malware Removal Tool (MRT)

  Restart & Login

macOS protections



Spam Call Topic	Estimated Spam Calls in 2021
Car Warranty	12.9 billion
Health Insurance	6.3 billion
Student Loans	4.1 billion
Vacation Scams	4 billion
Social Security	3.3 billion
Credit Card and Bank	2.3 billion



Idle Detection

The Idle Detection API notifies developers when a user is idle, indicating such things as lack of interaction with the keyboard, mouse, screen, activation of a screensaver, locking of the screen, or moving to a different screen. A developer-defined threshold triggers the notification.

Motivation

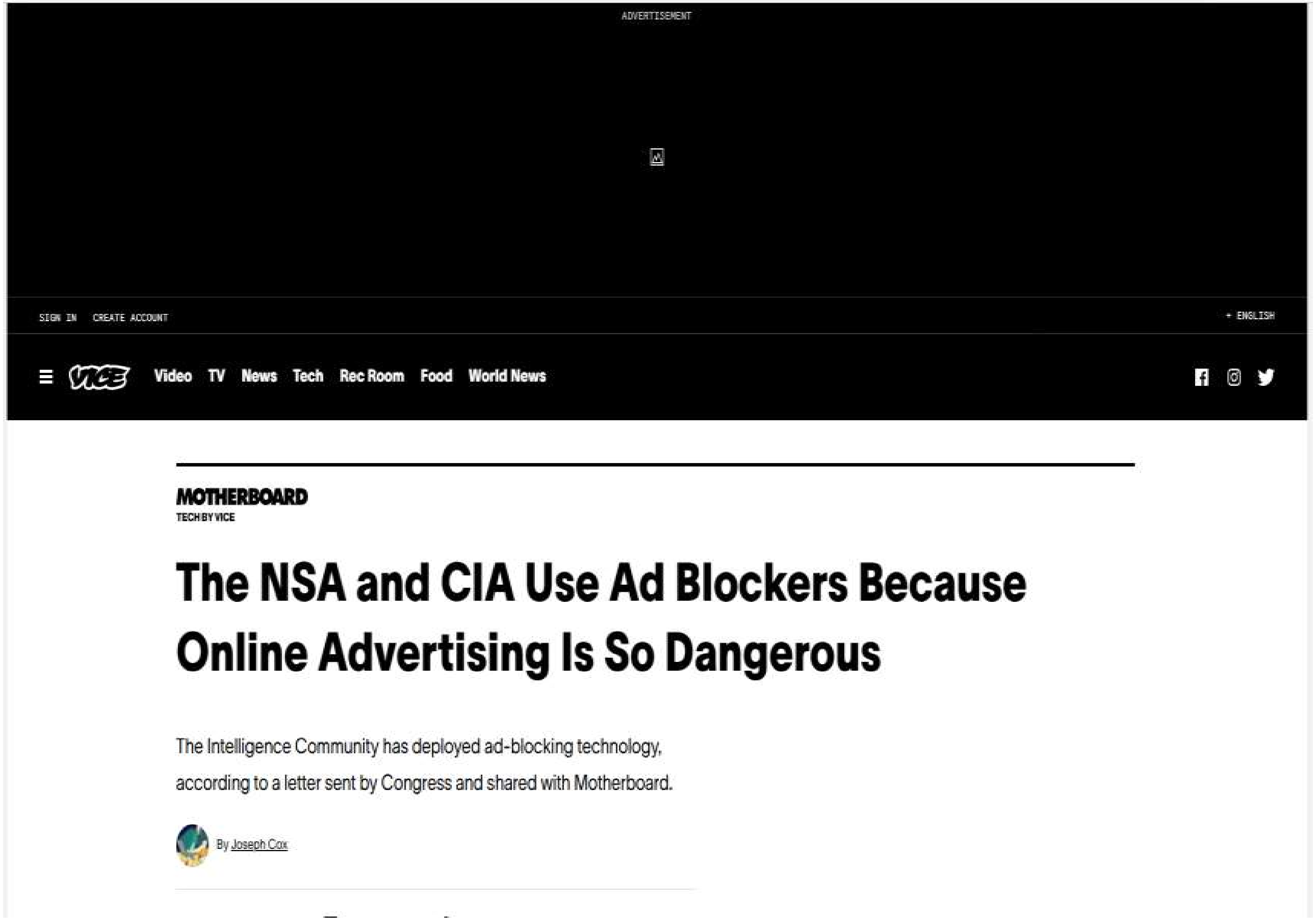
Applications which facilitate collaboration require more global signals about whether the user is idle than are provided by existing mechanisms that only consider a user's interaction with the application's own tab.

Chromium status

Enabled by default	
Chrome desktop	94
Chrome for Android	94
Tracking bug	#878979
Blink component	Blink>Input
Owner(s)	ayui@chromium.org reillyg@chromium.org

Consensus & standardization

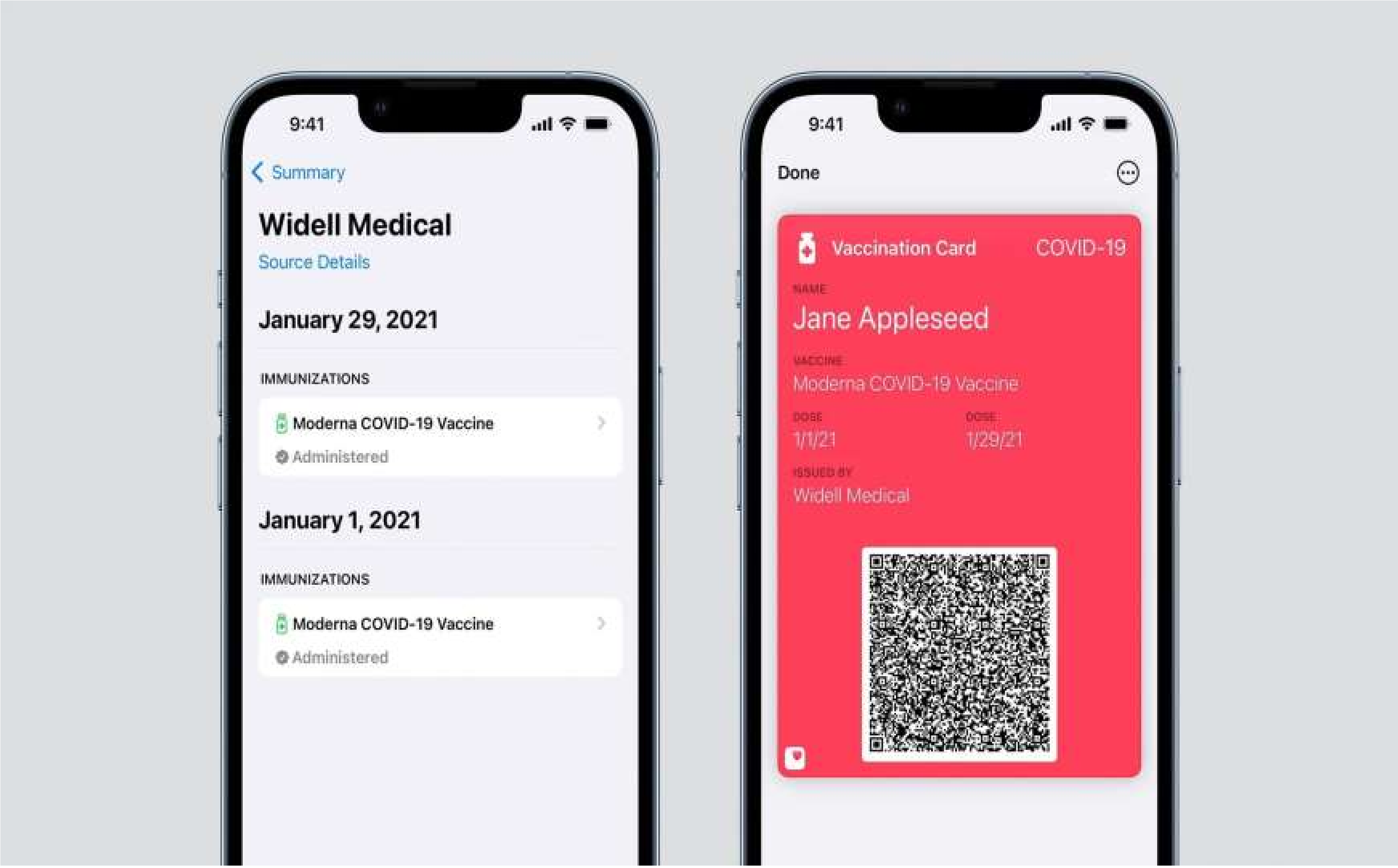
After a feature ships in Chrome, the values listed here are not guaranteed to be up to date.



The NSA and CIA Use Ad Blockers Because Online Advertising Is So Dangerous

The Intelligence Community has deployed ad-blocking technology, according to a letter sent by Congress and shared with Motherboard.

By Joseph Cox



Widell Medical

January 29, 2021

IMMUNIZATIONS

Moderna COVID-19 Vaccine

Administered

January 1, 2021

IMMUNIZATIONS

Moderna COVID-19 Vaccine

Administered

Vaccination Card COVID-19

NAME
Jane Appleseed

VACCINE
Moderna COVID-19 Vaccine

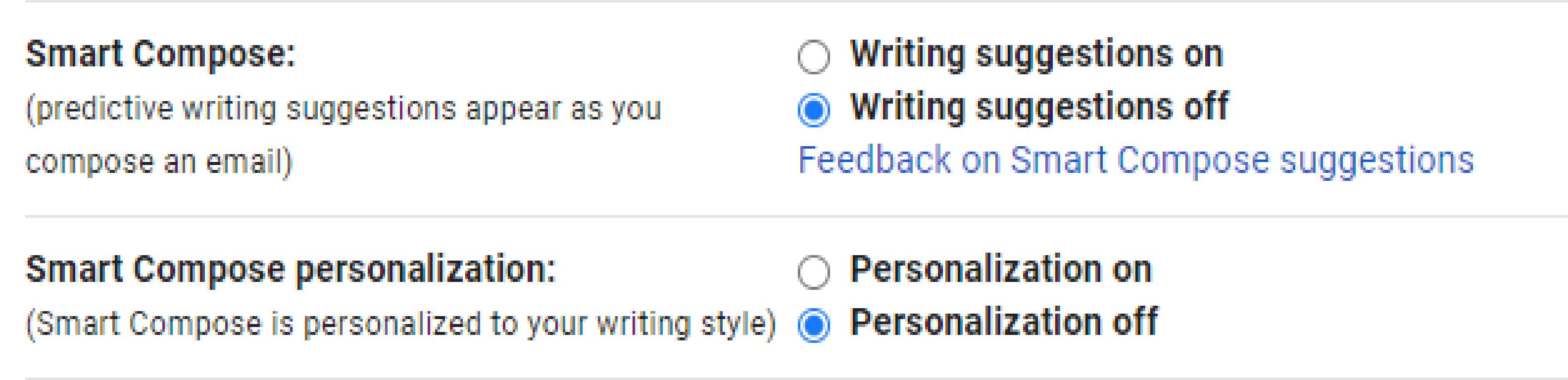
DOSE	DOSE
1/1/21	1/29/21

ISSUED BY
Widell Medical

- October Cyber Security Awareness month

Current issues

- Gmail “Smart Compose”
  as you type
  psycho analysis
  yeahbut



Smart Compose:
(predictive writing suggestions appear as you compose an email)

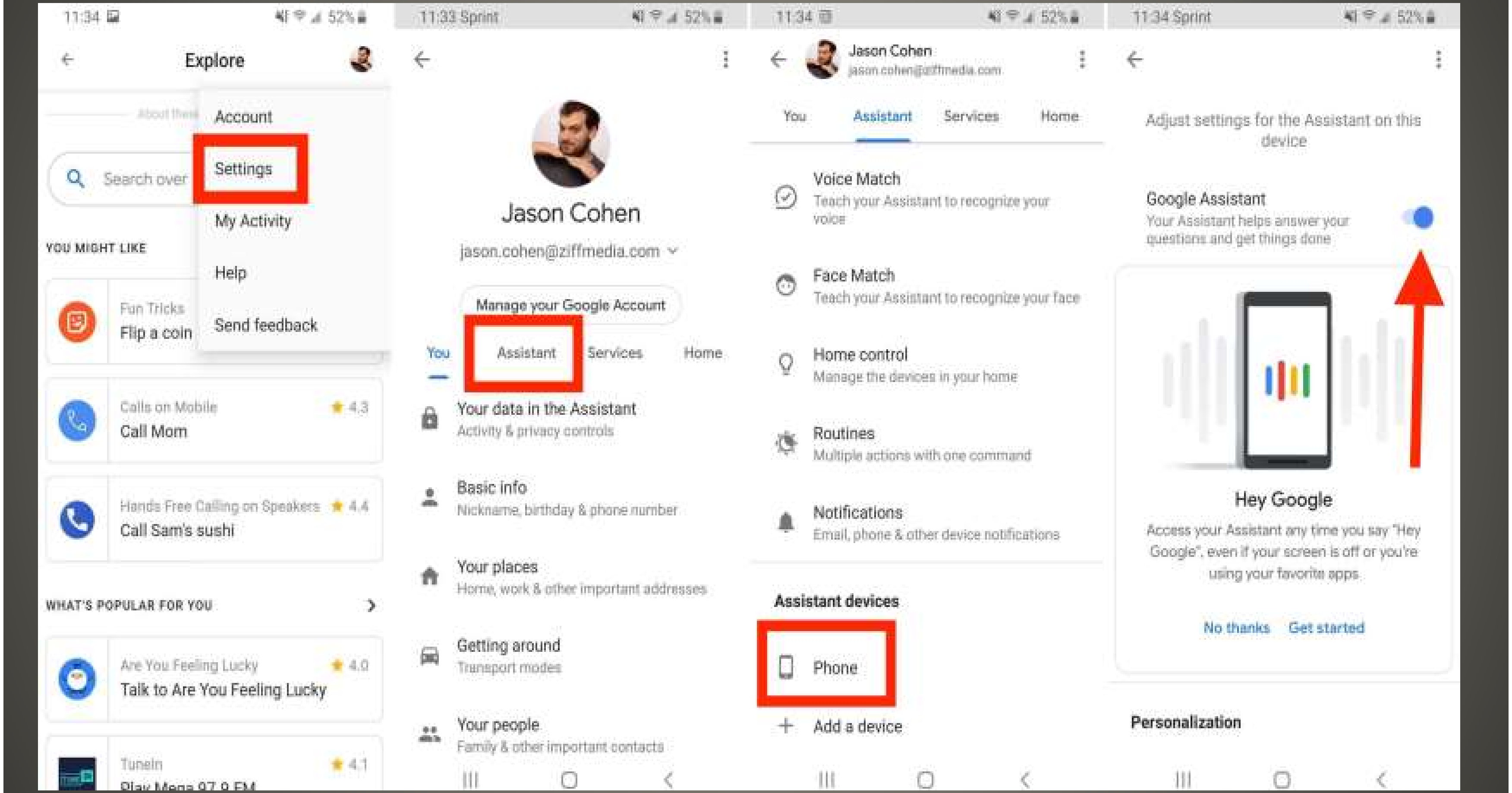
○ **Writing suggestions on**
● **Writing suggestions off**
Feedback on Smart Compose suggestions

Smart Compose personalization:
(Smart Compose is personalized to your writing style)

○ **Personalization on**
● **Personalization off**

Google

- Android


11:34
52%
Explore
About these
Account
Settings
My Activity
Help
Send feedback
Search over
YOU MIGHT LIKE
Fun Tricks
Flip a coin
Calls on Mobile
Call Mom
4.3
Hands Free Calling on Speakers
Call Sam's sushi
4.4
WHAT'S POPULAR FOR YOU
Are You Feeling Lucky
Talk to Are You Feeling Lucky
4.0
TuneIn
Play Mega 97.9 FM
4.1
11:33 Sprint
52%
Jason Cohen
jason.cohen@ziffmedia.com
Manage your Google Account
You
Assistant
Services
Home
Your data in the Assistant
Activity & privacy controls
Basic info
Nickname, birthday & phone number
Your places
Home, work & other important addresses
Getting around
Transport modes
Your people
Family & other important contacts
11:34
52%
Jason Cohen
jason.cohen@ziffmedia.com
You
Assistant
Services
Home
Voice Match
Teach your Assistant to recognize your voice
Face Match
Teach your Assistant to recognize your face
Home control
Manage the devices in your home
Routines
Multiple actions with one command
Notifications
Email, phone & other device notifications
Assistant devices
Phone
Add a device
11:34 Sprint
52%
Adjust settings for the Assistant on this device
Google Assistant
Your Assistant helps answer your questions and get things done
Hey Google
Access your Assistant any time you say "Hey Google", even if your screen is off or you're using your favorite apps
No thanks
Get started
Personalization

Google Assistant

- Apple

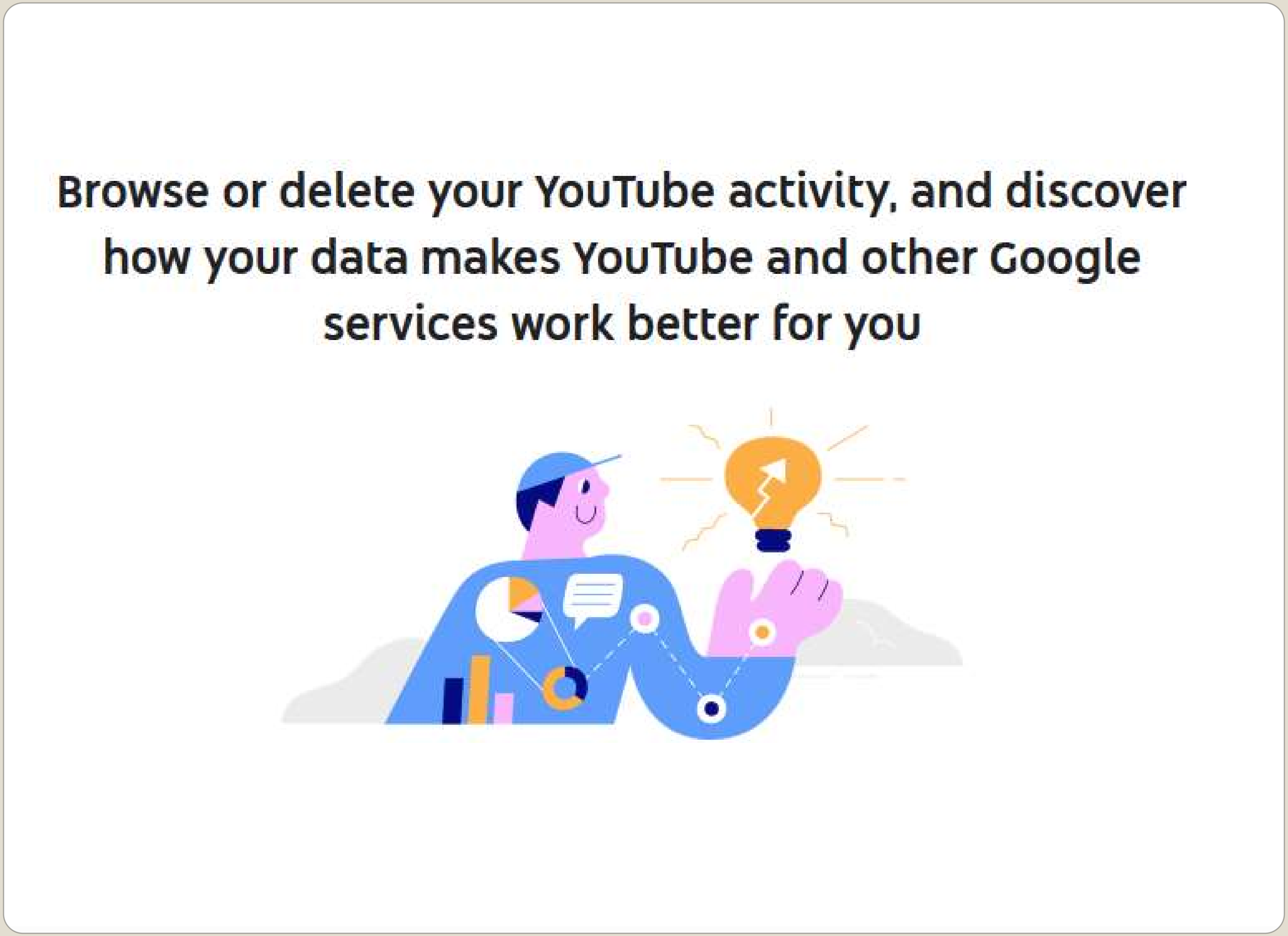
  Settings -> Privacy -> Microphone

  Disable Google Assistant

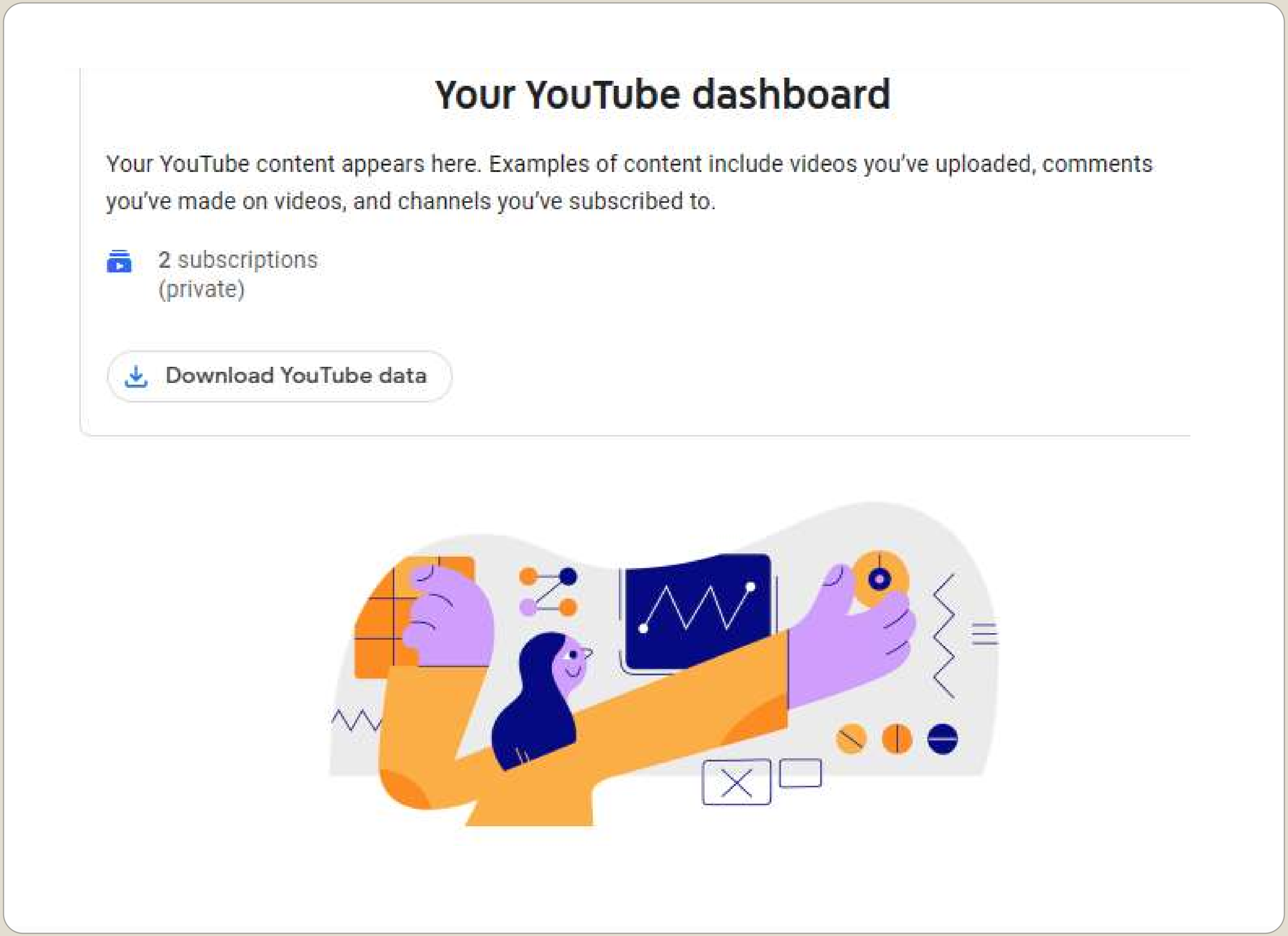
Google Assistant

- Don’t use account – tracking/history
  yeahbut
  account cookies

Google - YouTube



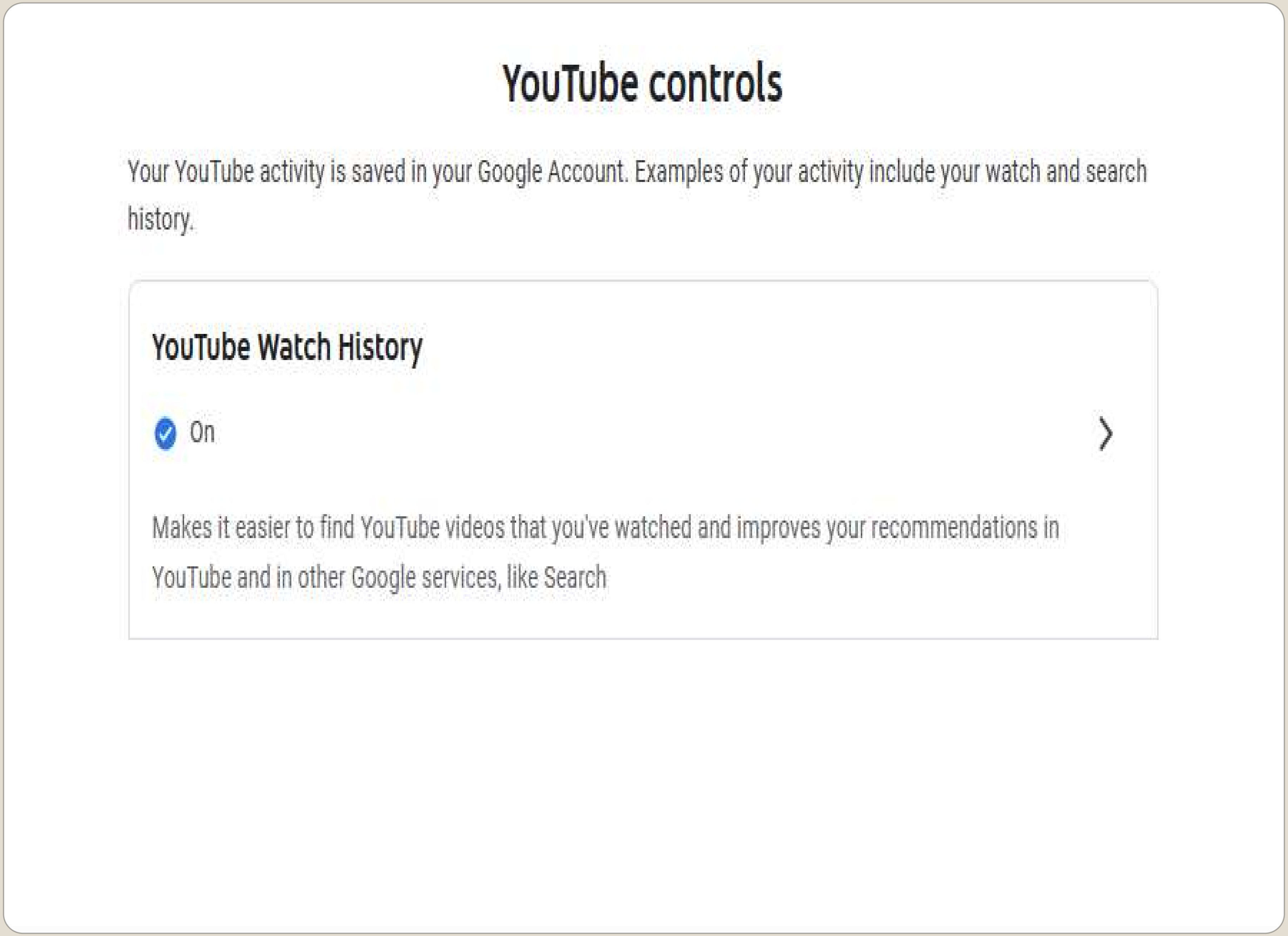
Browse or delete your YouTube activity, and discover how your data makes YouTube and other Google services work better for you



Your YouTube dashboard

Your YouTube content appears here. Examples of content include videos you've uploaded, comments you've made on videos, and channels you've subscribed to.

2 subscriptions
(private)



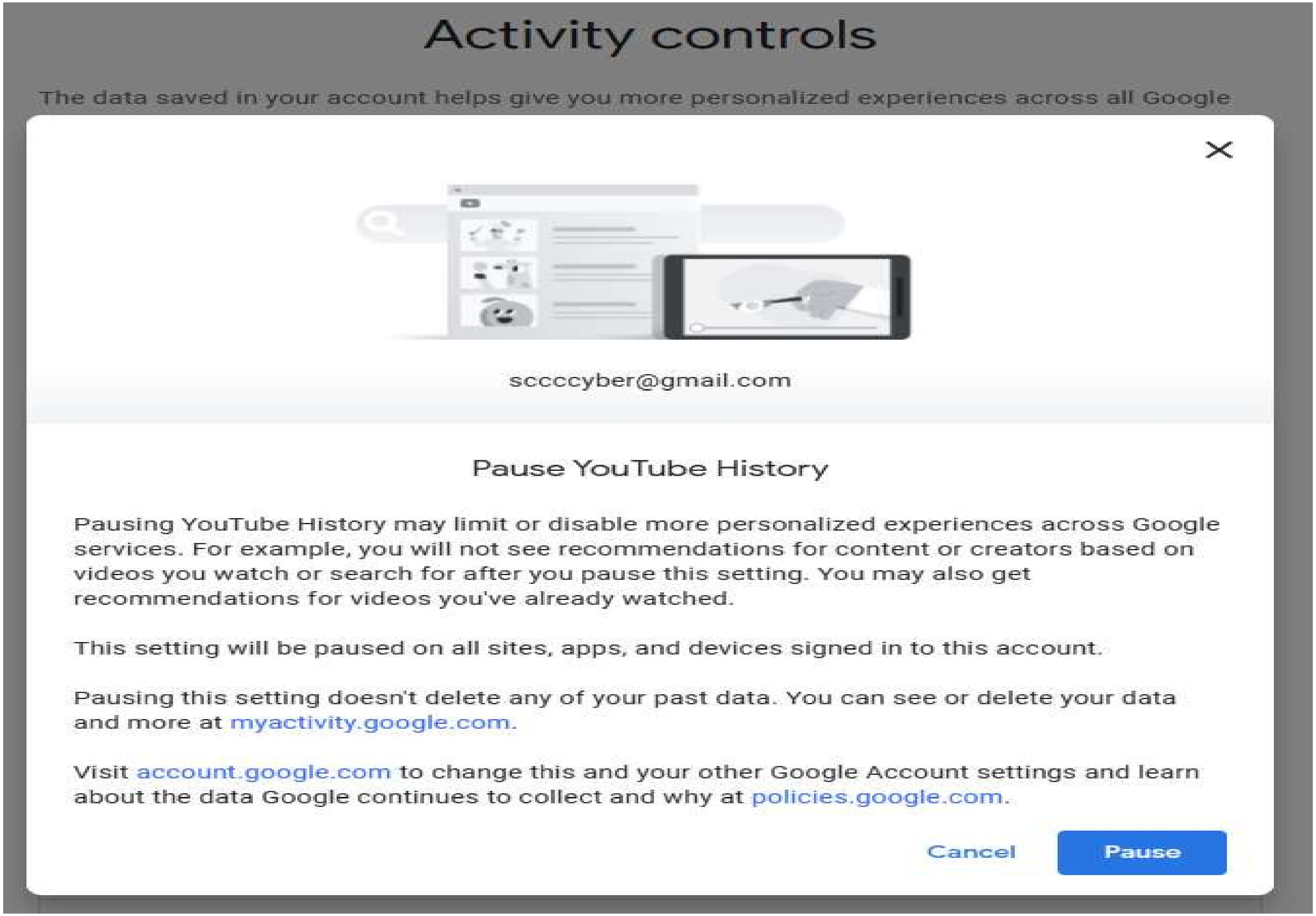
YouTube controls

Your YouTube activity is saved in your Google Account. Examples of your activity include your watch and search history.

YouTube Watch History

✓ On ›

Makes it easier to find YouTube videos that you've watched and improves your recommendations in YouTube and in other Google services, like Search



Activity controls

The data saved in your account helps give you more personalized experiences across all Google

sccccyber@gmail.com

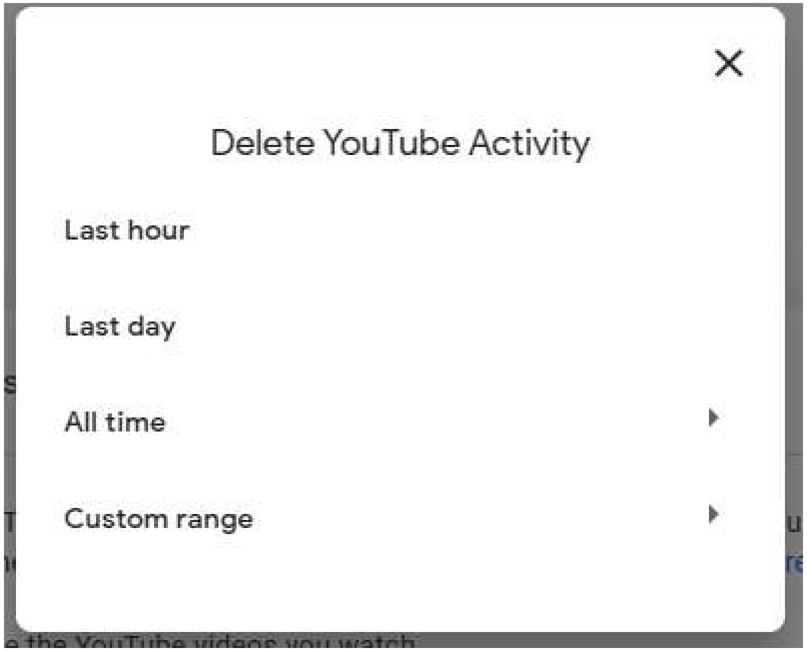
Pause YouTube History

Pausing YouTube History may limit or disable more personalized experiences across Google services. For example, you will not see recommendations for content or creators based on videos you watch or search for after you pause this setting. You may also get recommendations for videos you've already watched.

This setting will be paused on all sites, apps, and devices signed in to this account.

Pausing this setting doesn't delete any of your past data. You can see or delete your data and more at myactivity.google.com.

Visit account.google.com to change this and your other Google Account settings and learn about the data Google continues to collect and why at policies.google.com.

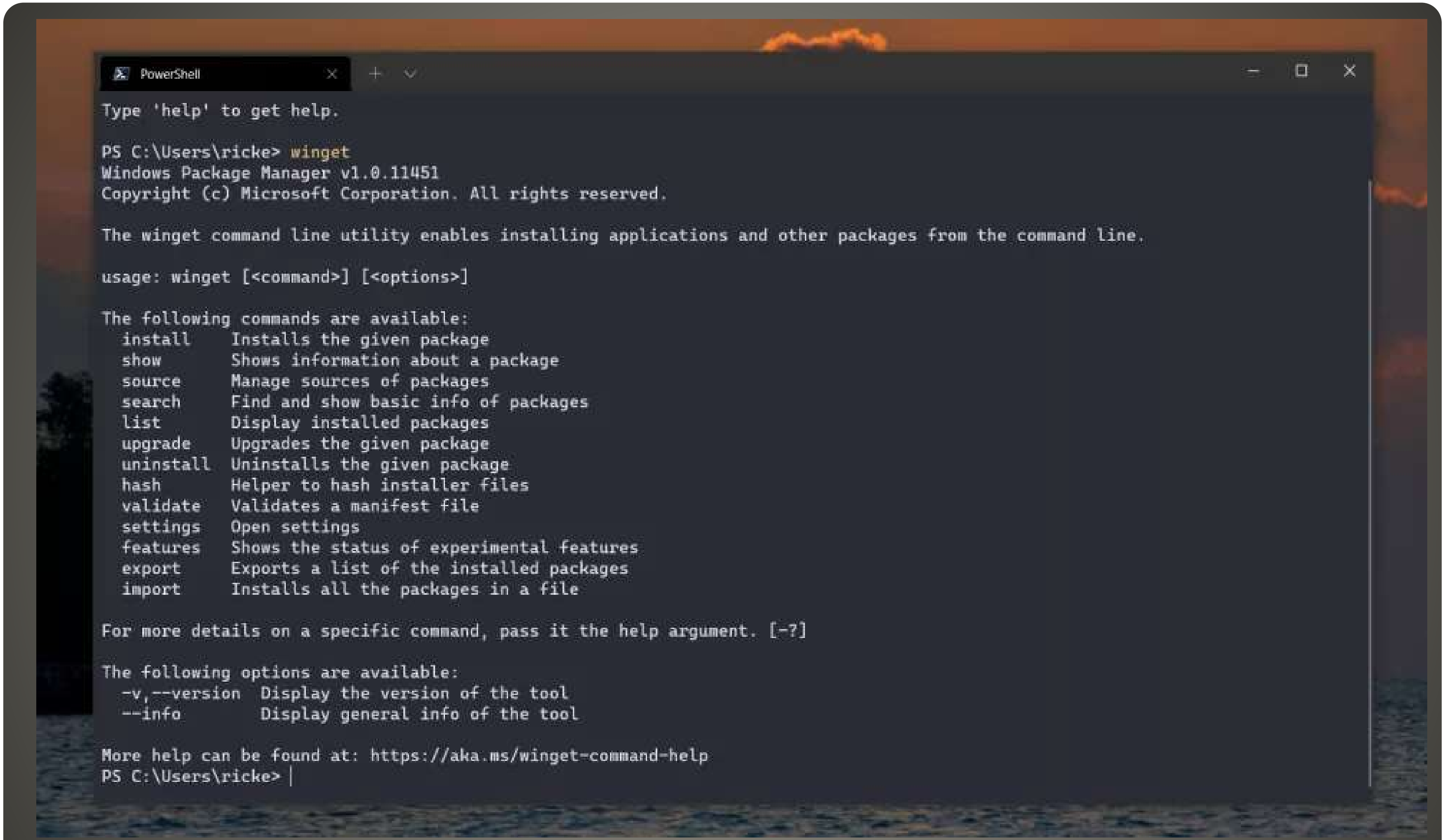

Delete YouTube Activity
Last hour
Last day
All time
Custom range
e the YouTube videos you watch

Google Helpful <-> Harmful

- Windows 11 – *general* release
- Your experience? - Windows SIG 10/12
- Calm
- CPU upgrade vs system upgrade
- Windows 10 support to continue
- Windows File Explorer memory leak
- Slow UDP Search Bar AMD CPU 3-15%
- Spectre and Meltdown

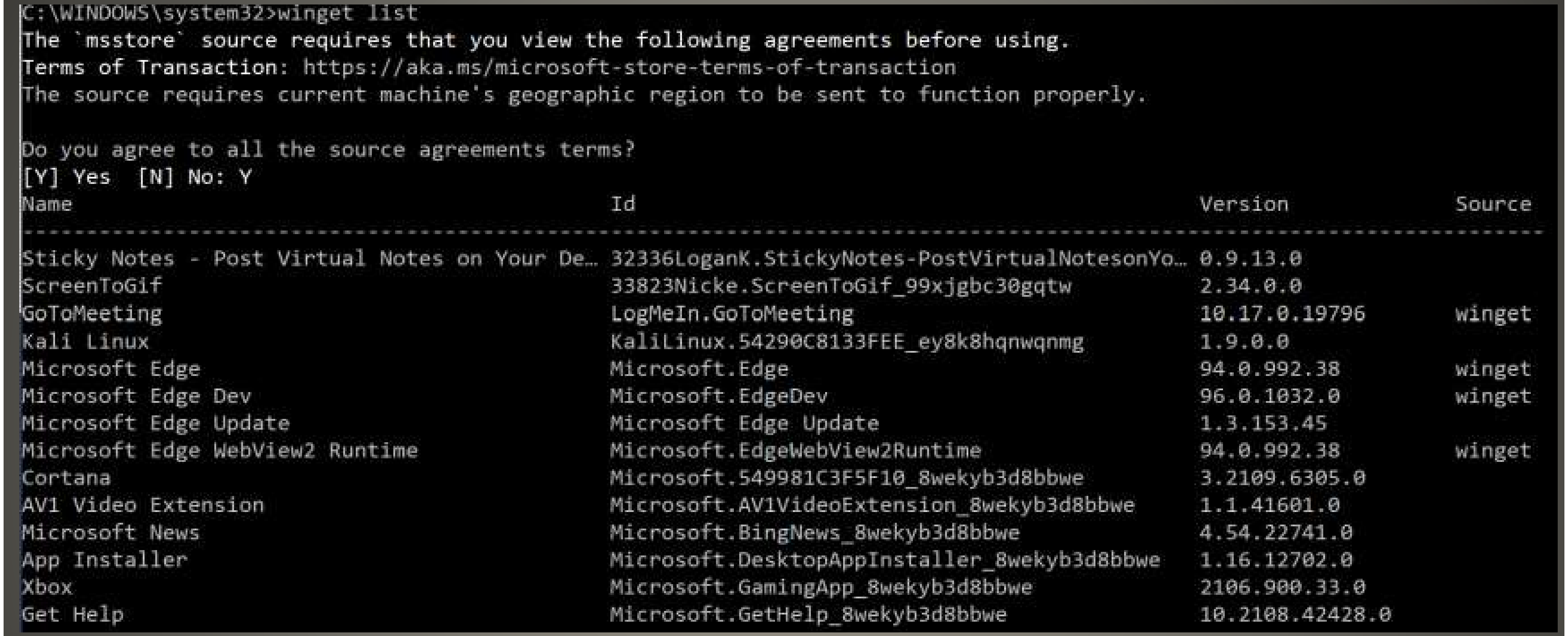
CPU predictive execution flaws new silicon
Intel Generation8 AMD
TPM + Secure boot + certain CPUs > security

Windows



```
Type 'help' to get help.

PS C:\Users\ricke> winget
Windows Package Manager v1.0.11451
Copyright (c) Microsoft Corporation. All rights reserved.

The winget command line utility enables installing applications and other packages from the command line.

usage: winget [<command>] [<options>]

The following commands are available:
  install    Installs the given package
  show       Shows information about a package
  source     Manage sources of packages
  search     Find and show basic info of packages
  list       Display installed packages
  upgrade    Upgrades the given package
  uninstall  Uninstalls the given package
  hash       Helper to hash installer files
  validate   Validates a manifest file
  settings   Open settings
  features   Shows the status of experimental features
  export     Exports a list of the installed packages
  import     Installs all the packages in a file

For more details on a specific command, pass it the help argument. [-?]

The following options are available:
  -v,--version  Display the version of the tool
  --info        Display general info of the tool

More help can be found at: https://aka.ms/winget-command-help
PS C:\Users\ricke> 
```

winget



```
C:\WINDOWS\system32>winget list
The `msstore` source requires that you view the following agreements before using.
Terms of Transaction: https://aka.ms/microsoft-store-terms-of-transaction
The source requires current machine's geographic region to be sent to function properly.

Do you agree to all the source agreements terms?
[Y] Yes  [N] No: Y
Name                                          Id                                            Version             Source
-----------------------------------------------------------------------------------------------------------------------
Sticky Notes - Post Virtual Notes on Your De… 32336LoganK.StickyNotes-PostVirtualNotesonYo… 0.9.13.0
ScreenToGif                                   33823Nicke.ScreenToGif_99xjgbc30gqtw          2.34.0.0
GoToMeeting                                   LogMeIn.GoToMeeting                           10.17.0.19796       winget
Kali Linux                                    KaliLinux.54290C8133FEE_ey8k8hqnwqnmg         1.9.0.0
Microsoft Edge                                Microsoft.Edge                                94.0.992.38         winget
Microsoft Edge Dev                            Microsoft.EdgeDev                             96.0.1032.0         winget
Microsoft Edge Update                         Microsoft Edge Update                         1.3.153.45
Microsoft Edge WebView2 Runtime               Microsoft.EdgeWebView2Runtime                 94.0.992.38         winget
Cortana                                       Microsoft.549981C3F5F10_8wekyb3d8bbwe         3.2109.6305.0
AV1 Video Extension                           Microsoft.AV1VideoExtension_8wekyb3d8bbwe     1.1.41601.0
Microsoft News                                Microsoft.BingNews_8wekyb3d8bbwe              4.54.22741.0
App Installer                                 Microsoft.DesktopAppInstaller_8wekyb3d8bbwe   1.16.12702.0
Xbox                                          Microsoft.GamingApp_8wekyb3d8bbwe             2106.900.33.0
Get Help                                      Microsoft.GetHelp_8wekyb3d8bbwe               10.2108.42428.0
```

Winget list

- 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