Sun City Computer Club

Cyber Security SIG

November 4, 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???

Browser Updates

- Browser extension updates
- Browser extension signature updates
- Firefox 94 – Site Isolation Technology
- Chromium site Isolation
  thus Edge, Brave, etc.
- Chrome 95 faster & less memory
- Safari Intelligent Tracking Protection
- Waterfox – Firefox fork

- Yet another stimulus check
- Just click and give up your information

Scams


Trojan
Source
Invisible Source Code Vulnerabilities

Trojan Source

- MOST code compilers and development environments
- Unicode – digital text encoding standard
- 154 language scripts 143,000 characters
- Bi-directional "Bidi" algorithm
  - Arabic, Chinese, etc.
  - Bidi override
  - Disguise file extensions
  - Open Source – *Manual review*
  - Copy & Paste
  - Compiler developers & maintainers
- Similar attack *Look-alike* characters in URLs
  - homograph attacks

- macOS vulnerability
  discovered by Microsoft
  bypass System Integrity Protection (SIP)
  Shrootless CVE-2021-30892
  Apple fixed October 26
- macOS WizardUpdate malware
  Update to bypass XProtect

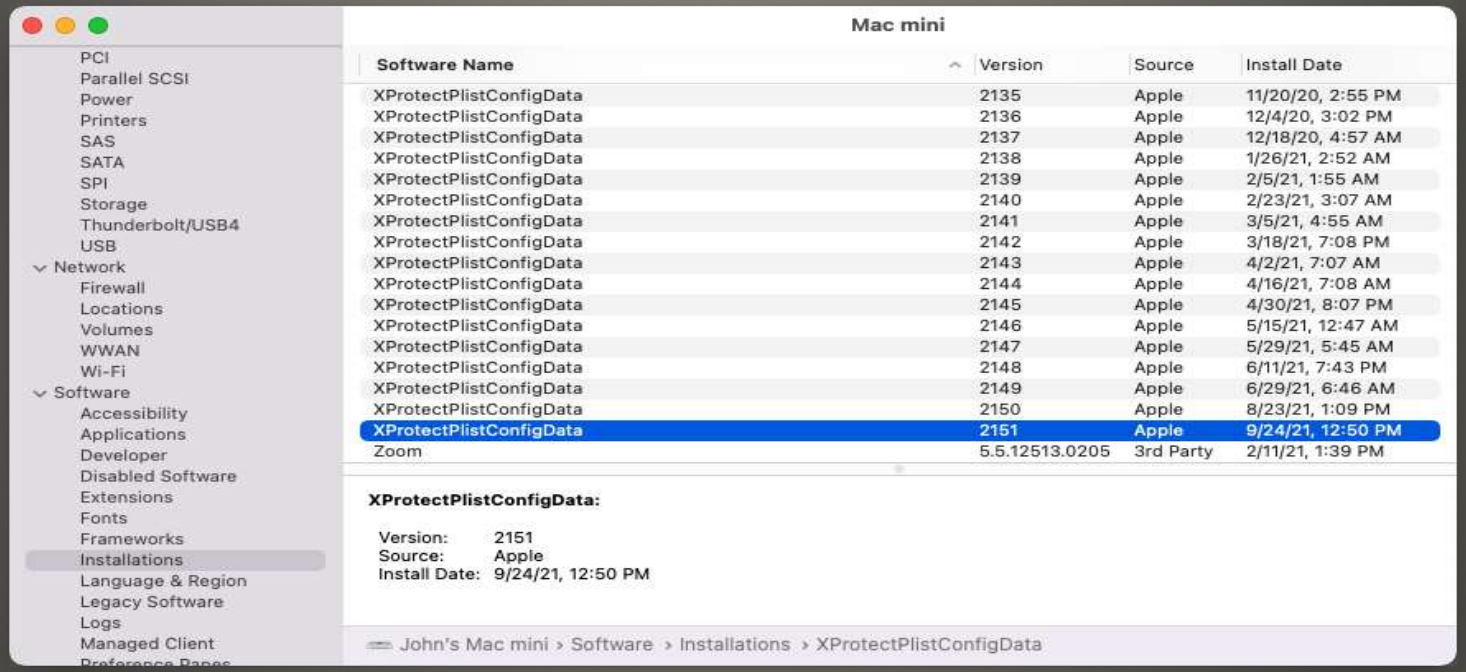
```
root@JBO-MAC ~ # csrutil status
System Integrity Protection status: enabled.
root@JBO-MAC ~ # head -n 1 /Library/Apple/System/Library/Extensions/AppleKextExcludeList.kext/Contents/Info.plist
<?xml version="1.0" encoding="UTF-8"?>
root@JBO-MAC ~ # echo hi > /Library/Apple/System/Library/Extensions/AppleKextExcludeList.kext/Contents/Info.plist
zsh: operation not permitted: /Library/Apple/System/Library/Extensions/AppleKextExcludeList.kext/Contents/Info.plist
root@JBO-MAC ~ # ./shrootless.sh "echo hi > /Library/Apple/System/Library/Extensions/AppleKextExcludeList.kext/Contents/Info.plist"
```


```
SIP bypass by Jonathan Bar Or ("JBO")

Checking command line arguments ..... [ OK ]
Checking if running as root ......... [ OK ]
Checking for system_installd ........ [ OK ]
Downloading Apple-signed package .... [ OK ]
Writing '/etc/zshenv' payload ....... [ OK ]
Running installer ................... [ OK ]
Cleaning up ......................... [ OK ]

> Great, the specified command should have run with no SIP restrictions. Hurray!
> Quitting.
root@JBO-MAC ~ # cat /Library/Apple/System/Library/Extensions/AppleKextExcludeList.kext/Contents/Info.plist
hi
root@JBO-MAC ~ # ls -laO /Library/Apple/System/Library/Extensions/AppleKextExcludeList.kext/Contents/Info.plist
-rw-r--r--  1 root  wheel  restricted 3 Jul 28 20:30 /Library/Apple/System/Library/Extensions/AppleKextExcludeList.kext/Contents/Info.plist
root@JBO-MAC ~ #
```

- System Information -> Software -> Installations



macOS automatic protections

Current Issues

- Microsoft Detection and Response Team (DART)

  Warning of large increase in credential spraying
  One third of account compromises
  One password, many accounts
  low and slow - multiple source IP addresses
  cloud administrators
- Harvard.com blogging platform online classes
- Zale's Jared Kay leaked data
- PAX Technology FBI raid
- Google after Pentagon contract
- Rickroll whole school district

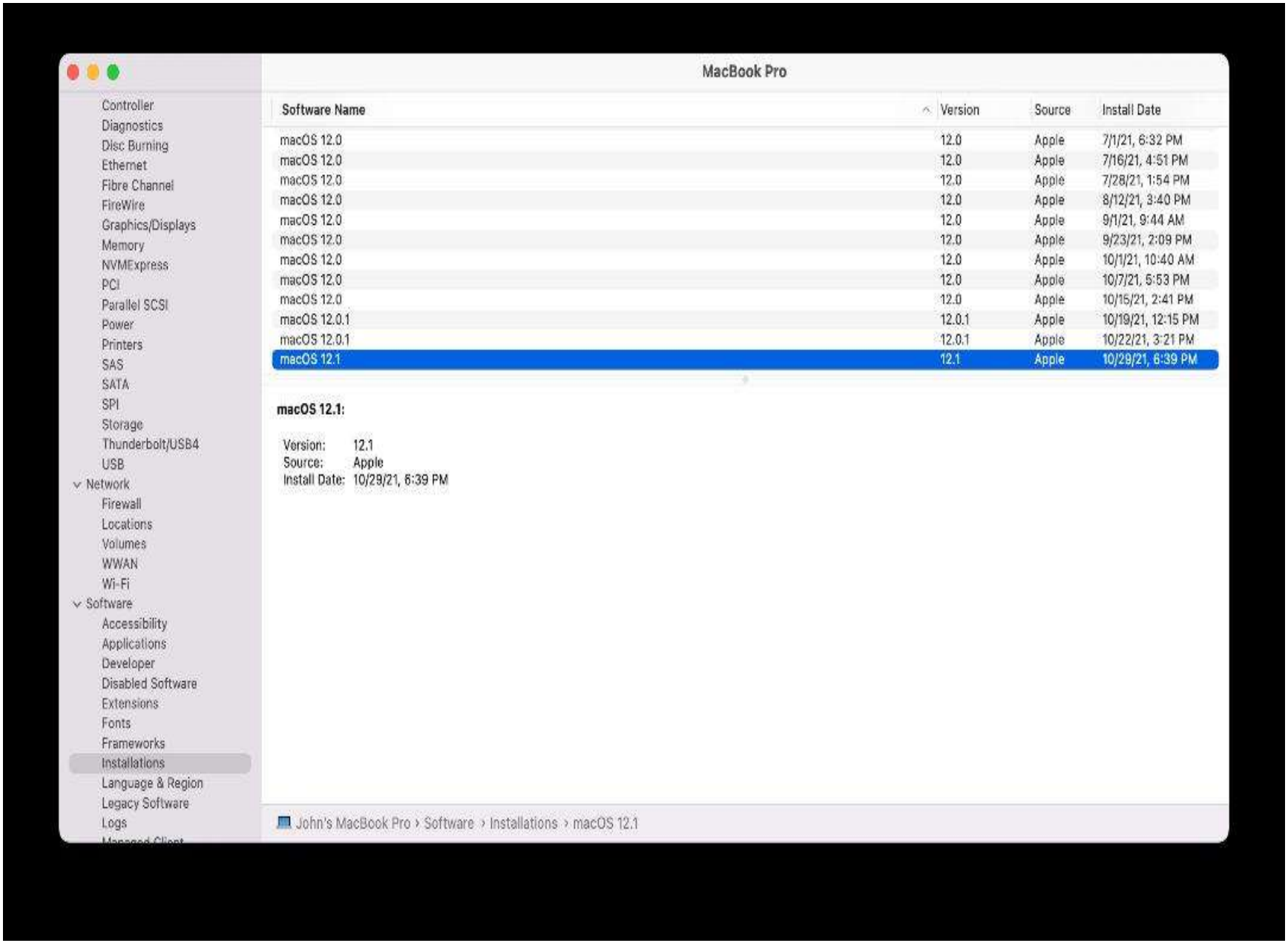
Current Issues

- “do you really want to leave?”
- Back button does not go back
- Adobe patches everything
  USE Adobe site to check and update
- Coordinated DDOS attacks of VoIP providers and their providers
  Thus police, …
- iPhone sound help
- iPhone sound spy
- Smart device recording
- Groove Ransomware - Hoax

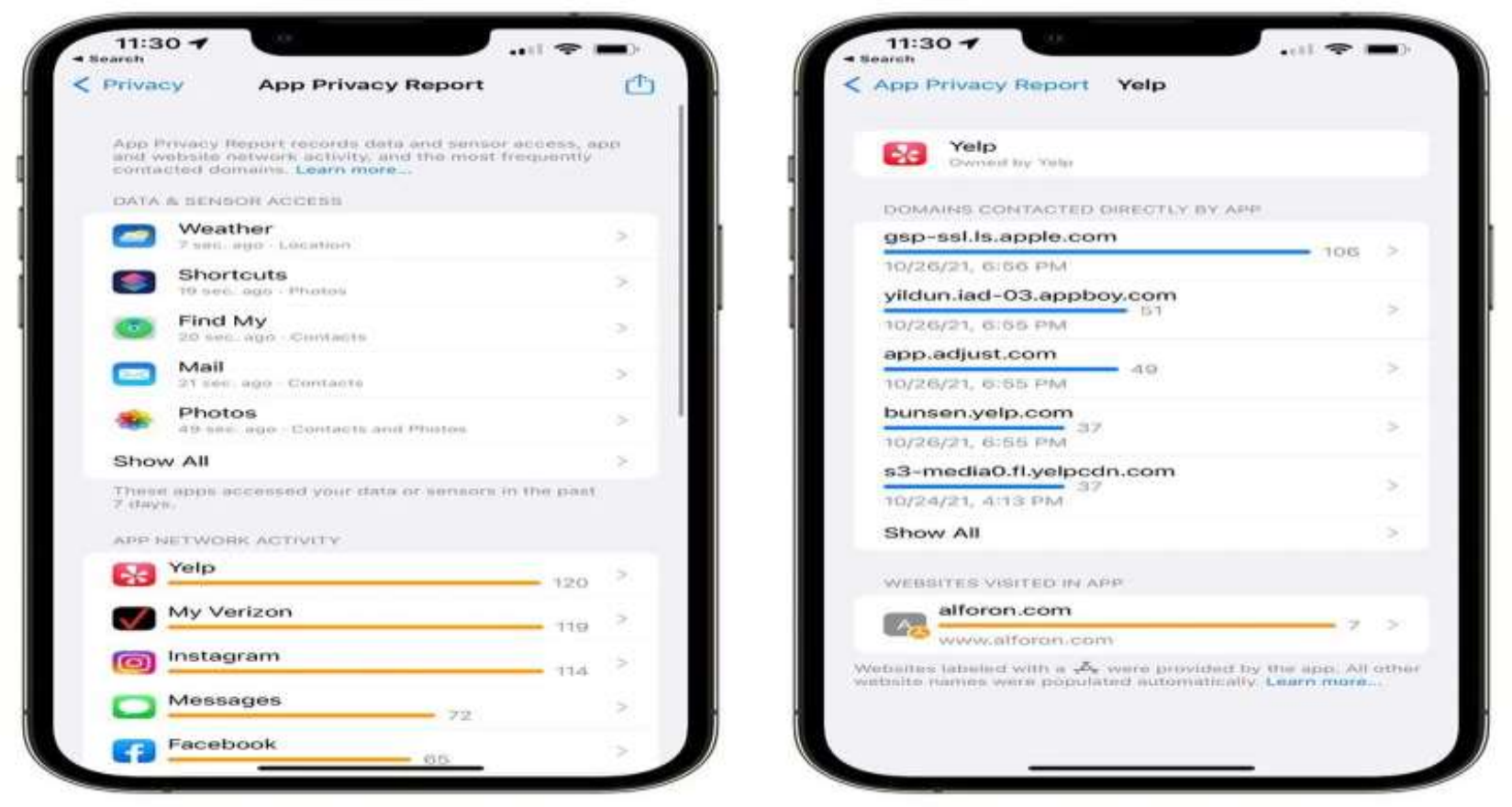
- Prosecute St Louis Post-Dispatch

  "*attempt to embarrass the state and sell headlines for their news outlet*"
- F12 view source

Missouri governor

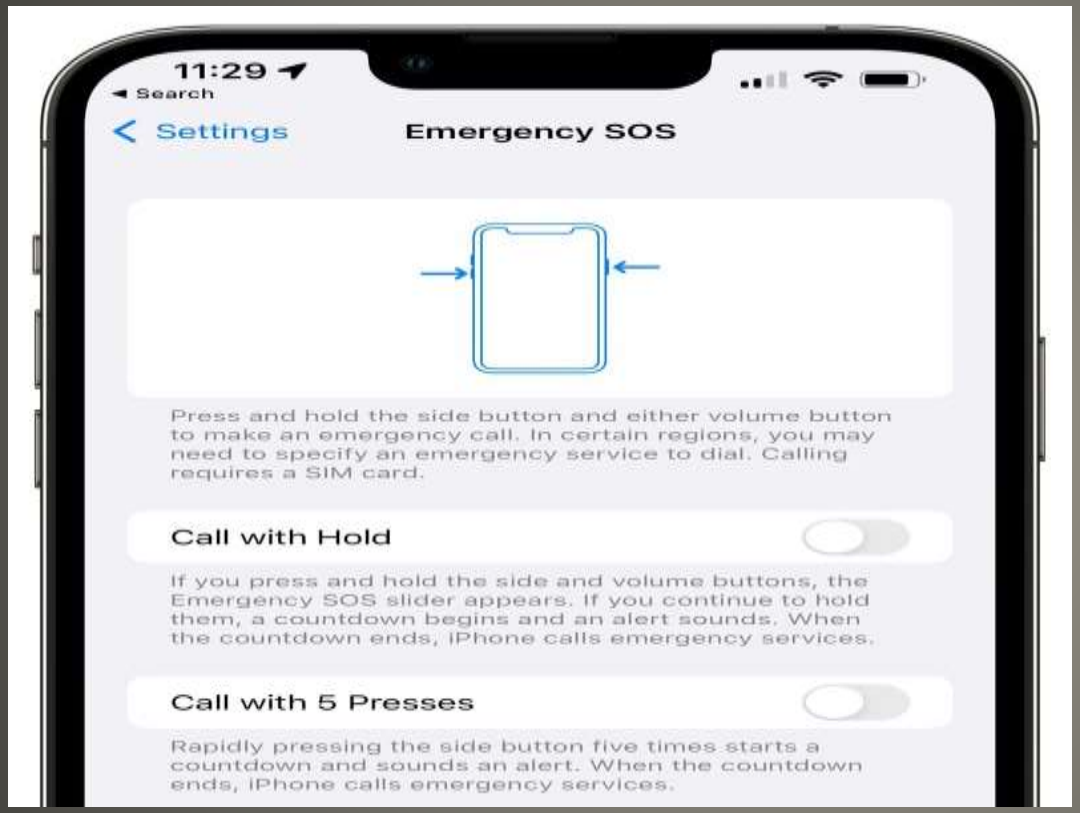

MacBook Pro
Controller
Diagnostics
Disc Burning
Ethernet
Fibre Channel
FireWire
Graphics/Displays
Memory
NVMExpress
PCI
Parallel SCSI
Power
Printers
SAS
SATA
SPI
Storage
Thunderbolt/USB4
USB
Network
Firewall
Locations
Volumes
WWAN
Wi-Fi
Software
Accessibility
Applications
Developer
Disabled Software
Extensions
Fonts
Frameworks
Installations
Language & Region
Legacy Software
Logs
Software Name
Version
Source
Install Date
macOS 12.0 12.0 Apple 7/1/21, 6:32 PM
macOS 12.0 12.0 Apple 7/16/21, 4:51 PM
macOS 12.0 12.0 Apple 7/28/21, 1:54 PM
macOS 12.0 12.0 Apple 8/12/21, 3:40 PM
macOS 12.0 12.0 Apple 9/1/21, 9:44 AM
macOS 12.0 12.0 Apple 9/23/21, 2:09 PM
macOS 12.0 12.0 Apple 10/1/21, 10:40 AM
macOS 12.0 12.0 Apple 10/7/21, 5:53 PM
macOS 12.0 12.0 Apple 10/15/21, 2:41 PM
macOS 12.0.1 12.0.1 Apple 10/19/21, 12:15 PM
macOS 12.0.1 12.0.1 Apple 10/22/21, 3:21 PM
macOS 12.1 12.1 Apple 10/29/21, 6:39 PM
macOS 12.1:
Version: 12.1
Source: Apple
Install Date: 10/29/21, 6:39 PM
John's MacBook Pro › Software › Installations › macOS 12.1

- App Privacy Report



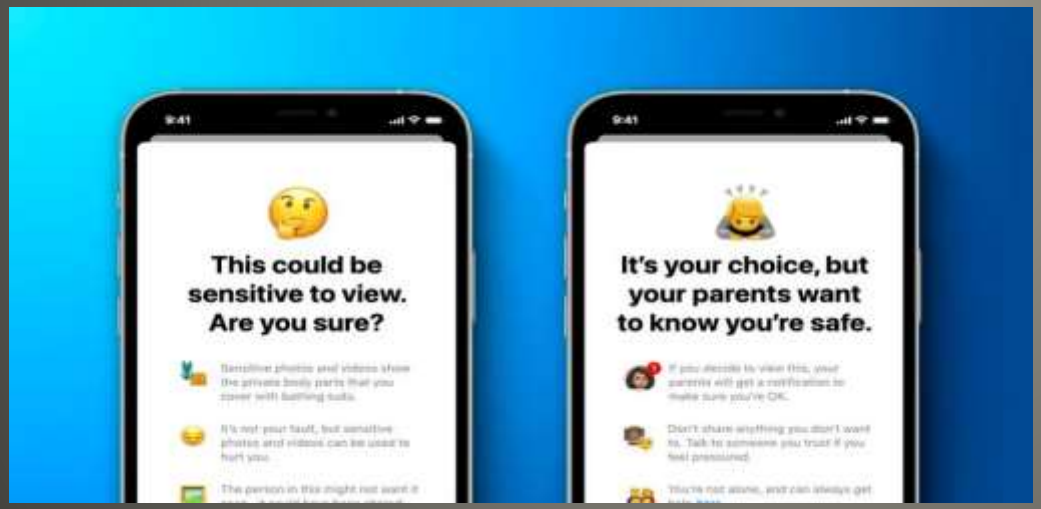
iOS 15.2

- Emergency SOS



iOS 15.2

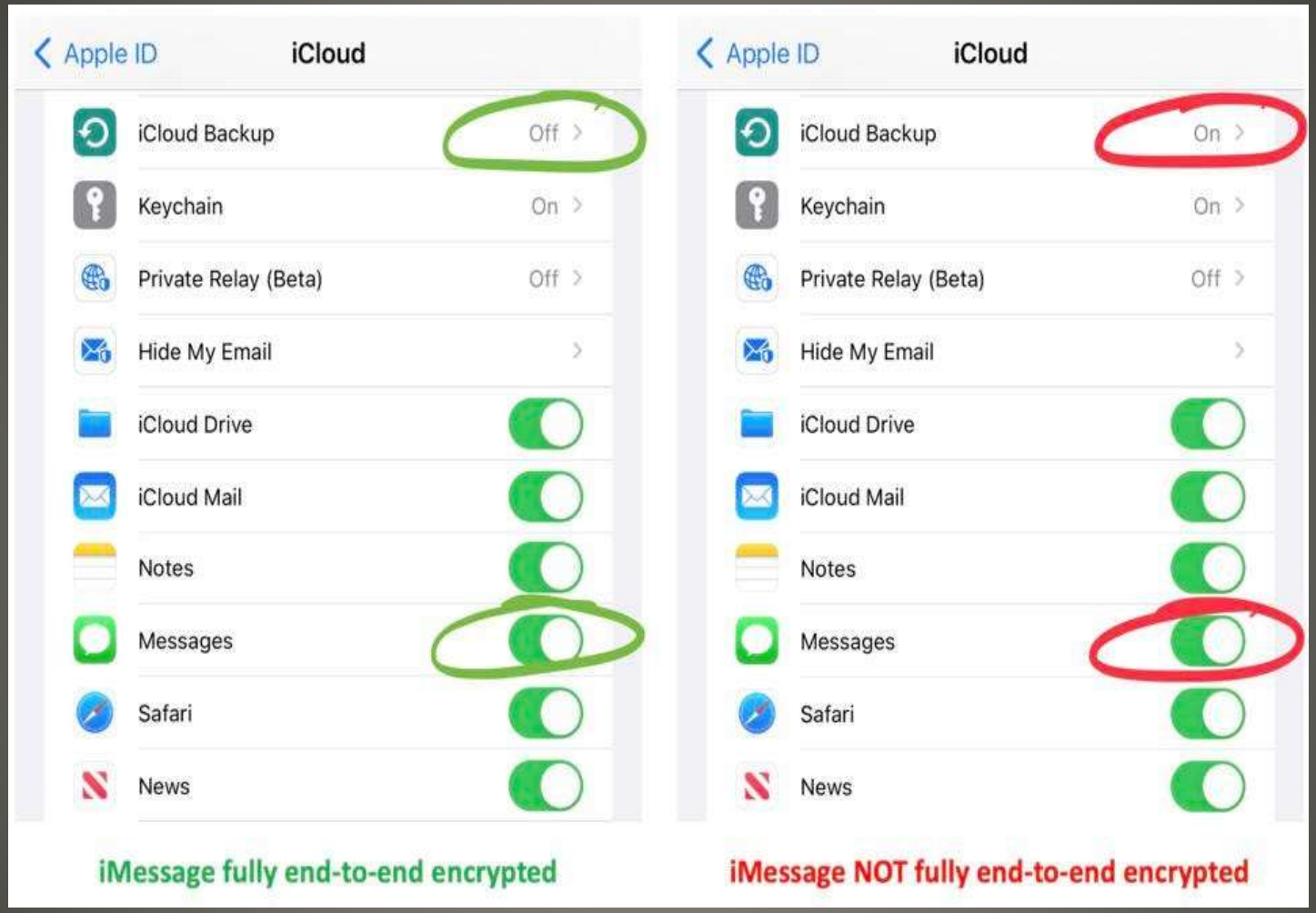
- Notification Summary
  card style look
- Communications Safety
  sexually explicit
  warning for children



iOS 15.2

- You are not alone and can always get help from a grownup you trust or with trained professionals. You can also block this person.
- You are not alone and can always get help from a grownup you trust or with trained professionals. You can also leave this conversation or block contacts.
- Talk to someone you trust if you feel uncomfortable or need help.
- This photo will not be shared with Apple, and your feedback is helpful if it was incorrectly marked as sensitive.
- Message a Grownup You Trust.
- Hey, I would like to talk with you about a conversation that is bothering me.
- Sensitive photos and videos show the private body parts that you cover with bathing suits.
- It's not your fault, but sensitive photos can be used to hurt you.
- The person in this may not have given consent to share it. How would they feel knowing other people saw it?
- The person in this might not want it seen-it could have been shared without them knowing. It can also be against the law to share.
- Sharing nudes to anyone under 18 years old can lead to legal consequences.
- If you decide to view this, your parents will get a notification to make sure you're OK.
- Don't share anything you don't want to. Talk to someone you trust if you feel pressured.
- Do you feel OK? You're not alone and can always talk to someone who's trained to help here.
- Nude photos and videos can be used to hurt people. Once something's shared, it can't be taken back.
- It's not your fault, but sensitive photos and videos can be used to hurt you.
- Even if you trust who you send this to now, they can share it forever without your consent.
- Whoever gets this can share it with anyone-it may never go away. It can also be against the law to share.

Text in iOS 15.2



Apple iMessage app

iCloud backup

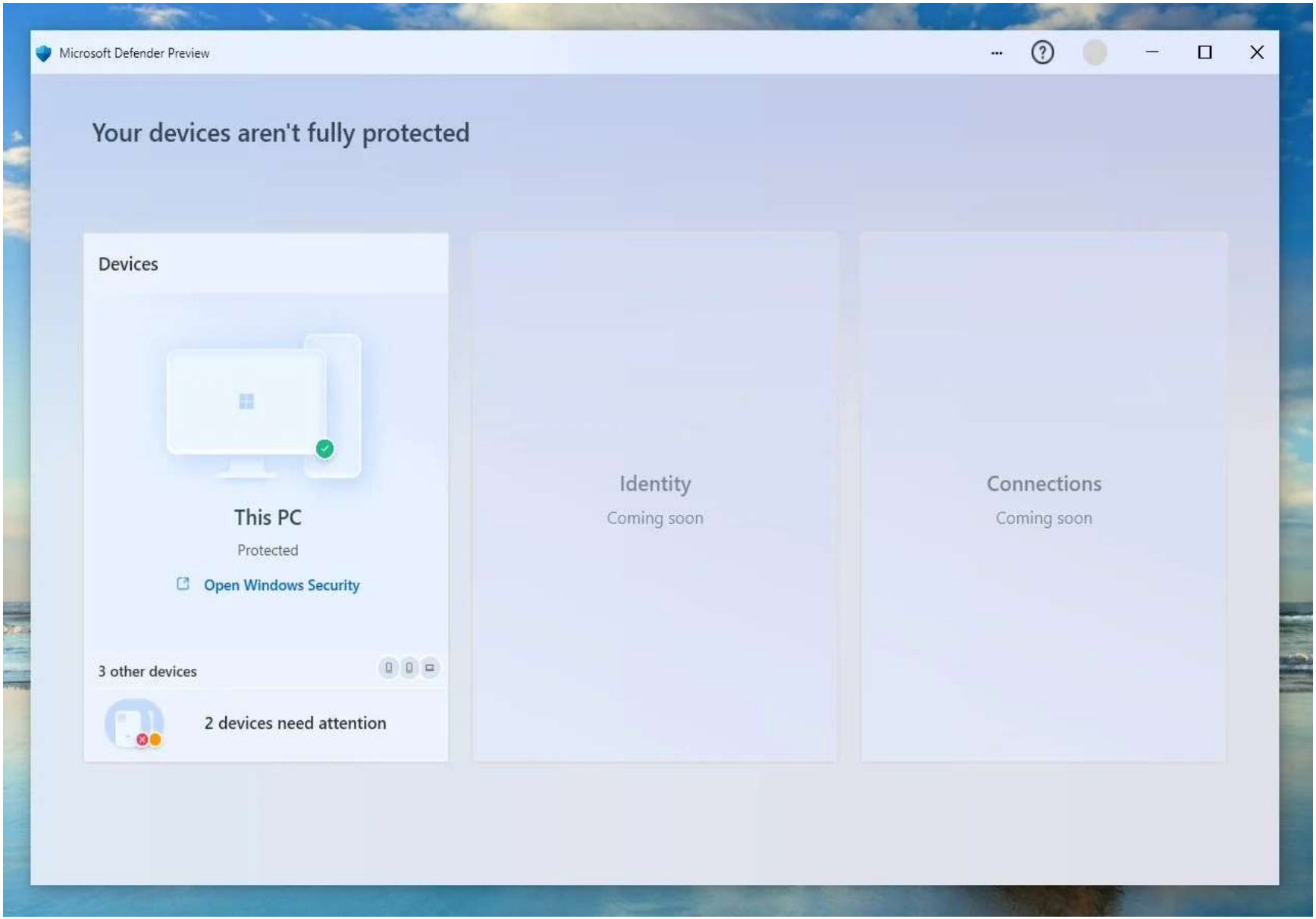
- YeahBut
  Apple needs to read so YOU can recover
- WhatsApp
  unencrypted version of WhatsApp chat history

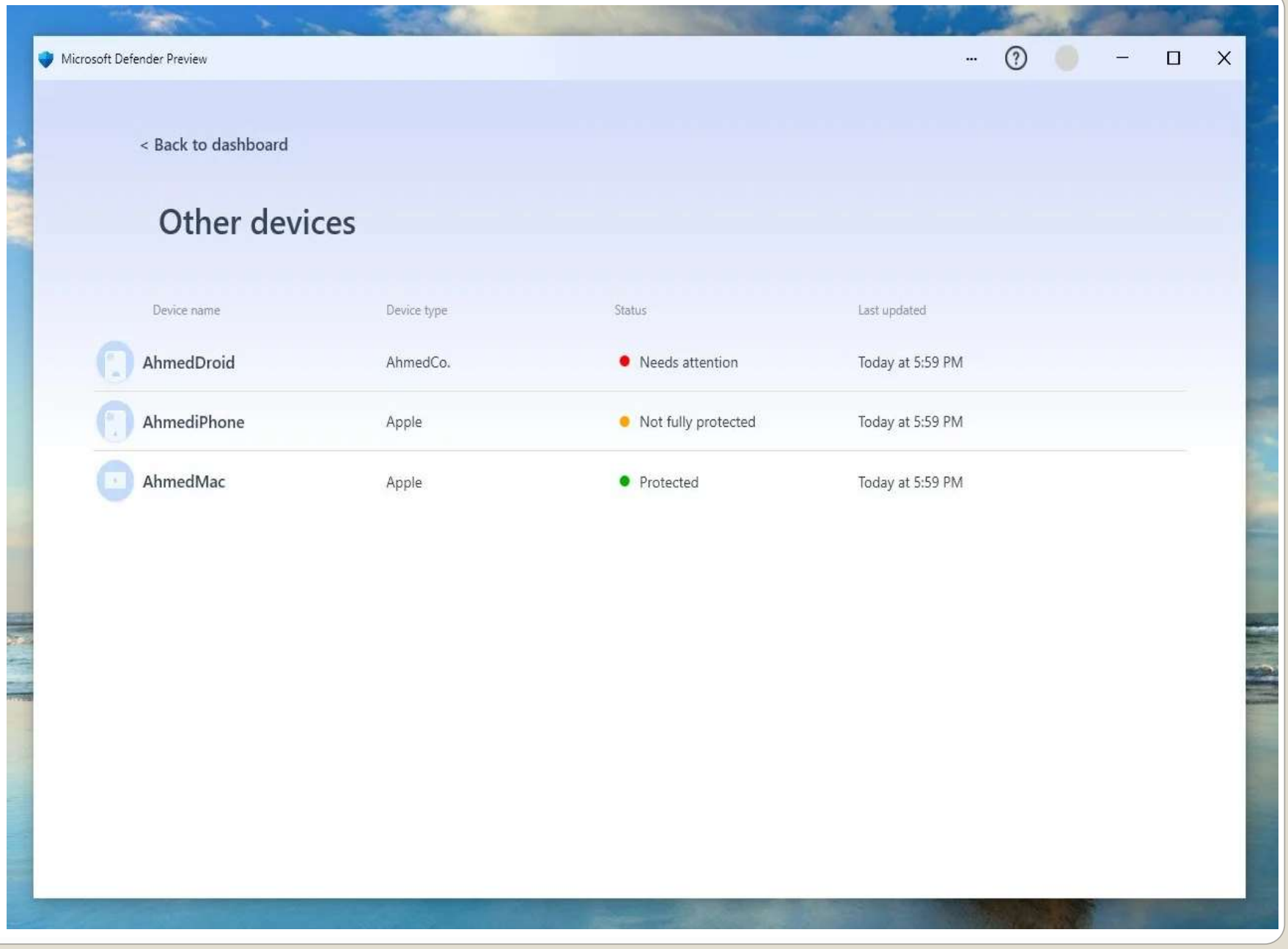
- Rich Communication Services (RCS) next generation SMS
- Use messaging systems fir for purpose

Google

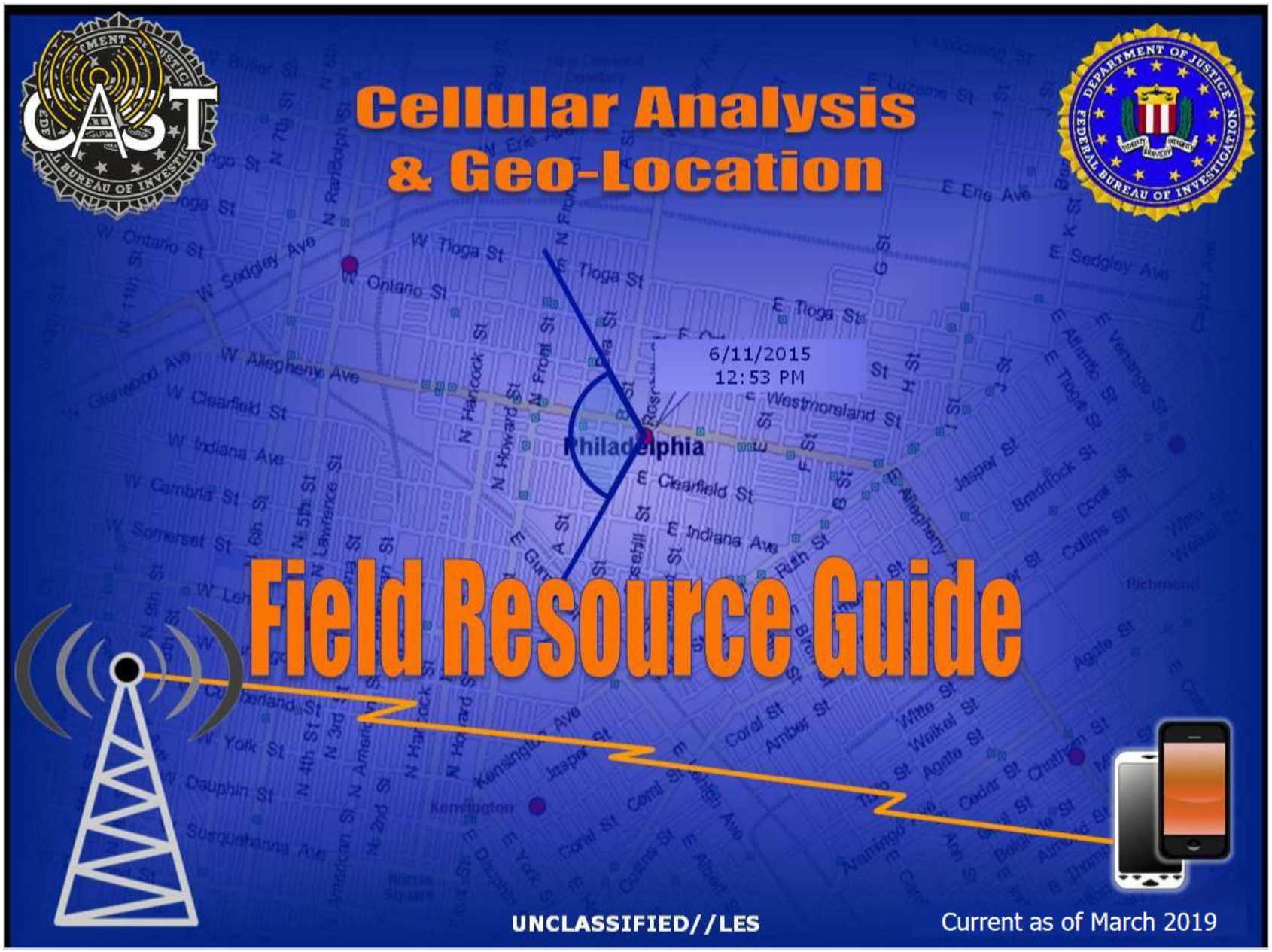
Microsoft Defender

- Remember Windows Defender?
- Home network administrators
  Android, iOS, Mac, ??
- Home networks
  Complicated
  Connected
  Diverse
- *Gibraltar*
- Phishing protection
- password breach detection
- IDentity theft protection
- Security recommendations
- And more


Microsoft Defender Preview
Your devices aren't fully protected
Devices
This PC
Protected
Open Windows Security
3 other devices
2 devices need attention
Identity
Coming soon
Connections
Coming soon


Microsoft Defender Preview
< Back to dashboard
Other devices
Device name
Device type
Status
Last updated
AhmedDroid
AhmedCo.
Needs attention
Today at 5:59 PM
AhmediPhone
Apple
Not fully protected
Today at 5:59 PM
AhmedMac
Apple
Protected
Today at 5:59 PM

Cellular Analysis & Geo-Location



Field Resource Guide

UNCLASSIFIED//LES

Current as of March 2019

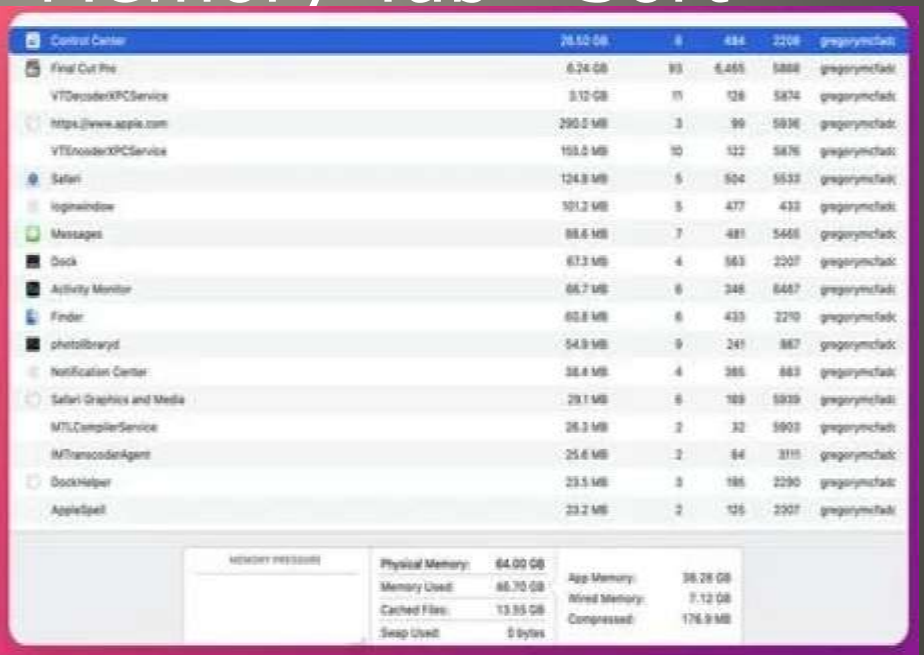
Disclaimer

Studying this manual and attending the basic training does **NOT** constitute an individual as certified to testify.

Cell analysis is a great investigative tool. However, testifying in court regarding cell phone records is difficult and requires significant training. Prior to testifying, CAST agents receive over **500** hours of training.

Cellular Analysis Survey Team

- Some MACs get “bricked”
  Cyber Security News Archive
- Some MACs have “memory leak”
  Activity Monitor Memory Tab Sort



macOS Monterey

- 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