Sun City Computer Club

Cyber Security SIG

June 1, 2023

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??

- Apple Users Group SIG
- Join Now
- First meeting September 8

- Until then, iDevices topics in Mac Users Group

Presenter???

Recent Presentation Postings

- Cyber Security SIG Seminars
- NRO Anti-Fraud Town Hall May 12, 2023
- Enquiring Minds A Computer Club Presentation May 16, 2023
- Self Defense Club
  Self & Home Security SIG
  Cybersecurity and Older Americans
  Telephone Scans from FCC
- Current Issues Club
  Program Background Sheets
  Consequences of Disinformation / Misinformation
  Cybersecurity
- Investment Education Club
  Crypto Currency and Blockchain
- Computer Club
  Past Presentations
  SIGs

GPT

- Generative Pre-trained Transformer
- GPT & Autism

Recent 60 Minutes Episode

- May 21, 2023
- Targeting Seniors
- $10.3 Billion in losses, FBI report
- Very few losses are reported - embaressed
- Everyone is vulnerable
- Why not a national crisis?
- Awareness, Preparedness, Understanding
- Doorbell cameras, alarms, etc.
- More likely to be scammed from afar
- AI, available apps, social engineering
- REPORT IT

Current Issues

- Dish Network pay ransom?
- GhostTouch ability to access smartphones
  Under the table electromagnetic signals
- Teen hacks 60,000 DraftKings accounts
  Credential stuffing
  Add new payment method
  Then withdraw all funds
- Android devices with malware from factory
  Android devices e.g. TVs
  AllWinner T95, RockChip X12 Plus, and others
  C&C Shutdown, but …
- FBI misuse of surveillance tool
  Section 702 FISA

- Joint Cyber Security Advisory

Current Issues

- Twitter in EU
  Drop out of voluntary agreement
- €1.2 billion Euro fine
  Ireland's Data Protection Commission
  Meta
  GDPR rules
  PII of EU users data transferred w/o approval
  Determent to EU users?
- Indiana, Iowa, Tennessee pass comprehensive privacy laws (8 states total)
- So many fines and ransomware incidents
- Barracuda Email Security Gateway flaw

Brave Browser OTR

- Off The Record
- WEB sites suggest browser forget visit
- Visit in clean temporary area
- No history No cookies No data to disk
- Hide from device
- Hide too much “suspicion”
- Hide too little
- After site visit
- Delete cookies & permissions
- Not delete browsing history & caches

Brave Browser OTR

- Quick exit button/method
- Site defined methods – not browser
- Site “Want OTR”?
- User must approve
- Tied to that site only
- Thus no suspicious gaps
- Header *Request-OTR*
- Pre-loaded OTR partner sites

Brave Browser OTR

- Caveats
- No protections:

  Extensions, spyware, sniffers, OS logs, crash logs, memory harvesters, etc.
- Brave 1.53

Passwords

- Donald Trump
  Twitter *yourfired*
  Twitter *maga2020!*
- Paris Hilton
  T-Mobile *Tinkerbell*
- Mark Zuckerberg
  Pinterest, Twitter, Instagram *dadada*
- Lisa Kudrow
  Sticky note in picture
- Evan Williams
  Reuse of Foursquare
- Celebgate
  No limit to password attempts

Apple & AI

- Bann on other platforms
- Several AI acquisitions
- Bobcat for AppleTV

Scams

- ATM
  "That your money?"
  swap ATM card with counterfeit one
- Stay Vigilant
- Shield PIN
- Use Secure ATMs
- Inspect ATMs
- Beware strangers
- Monitor Accounts
- Enable transaction alerts
- Keep Card Secure
- Awareness

- Windows CTRL+SHIFT+Delete
- MAC Command+Shift+Delete

Quickly Clear browsing History

- Brute Force
- Social Engineering
- Phishing scams

Passwords

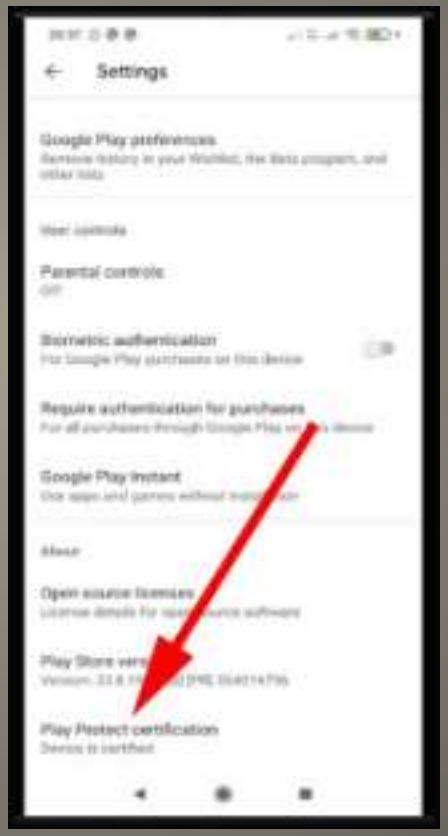
Asus router issue

- May 16
- Most should be functional again
- Cause: corrupt configuration file

- Firmware Update
- Malicious backdoor
- Mustang Panda

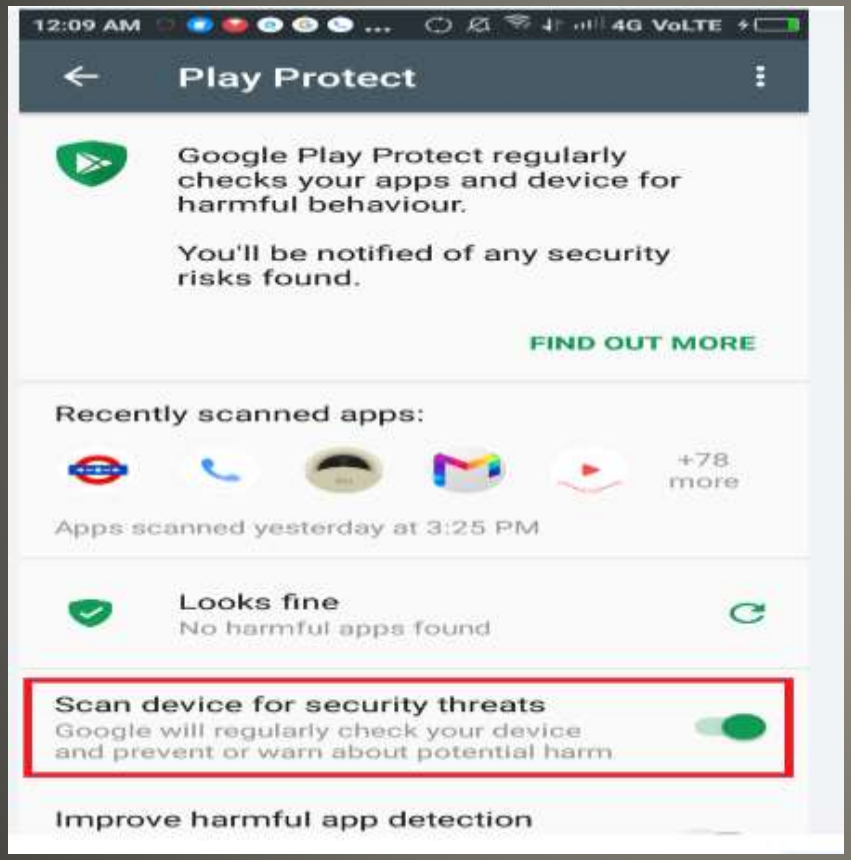
TP-Link

- Android Google Play Protect?
  Google Play Store App > Profile > Settings
  About



Settings Android & iPhone

- Scan apps with Play Protect on



Settings Android & iPhone

- iPhone
  Mail Privacy Protection
  Hides your IP address
  Prevents senders seeing if/when that email opened
  Settings > Mail > Privacy Protection
  Protect Mail Activity

Settings Android & iPhone

Hidden Files Android & iPhone

- Samsung
  Settings > Display hidden files
- Xiaomi
  File Management > Settings > Display hidden files
- Pixel
  Files app > Settings > Display hidden files
- Other
  third-party file management app Play Store
  ES File Explorer -or- Total Commander
  Launch > Settings

Hidden Files Android iPhone

- Third-party iExplorer on Computer
  Attach iPhone to that computer USB
  Browse iTunes Backups
  Select which iTunes backup
  Data
  View
- Terminal App on Mac
  Connect iPhone via USB
  On Terminal

Write com.apple.finder as the default AppleShowAllFiles YES

  Restart Finder

- Jailbreak – Not Recommended

KeePass

- Unpatched (so far) KeePass exploit
  Helps retrieve cleartext master password
  Retrieves from memory
  So even with database locked
  CVE-2023-3278
  Just memory access / memory dump
  process dump, swapfile, hibernation file, ..
  Windows, macOS, Linux,
  2.53.1 and older are vulnerable
  Version 2.54 should fix the issue
  BUT

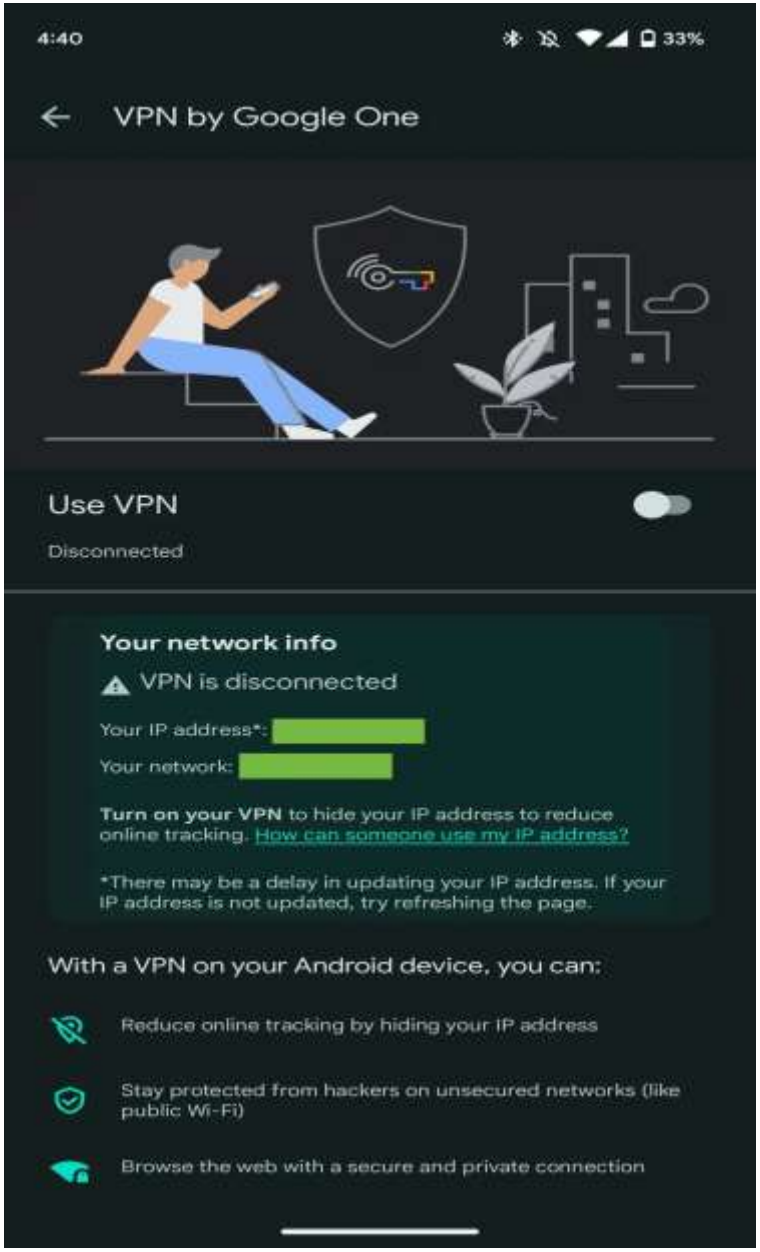
KeePass master password may still exist in memory
BEWARE of apps that can dump/access memory

- Terms and conditions
- “collect information about the audio and video content you watch, the channels you view, and the duration of your viewing sessions.”
- All smart TVs do it,

Telly TV

Wi-Fi

- Strong encryption
- Strong passphrase
- Wi-Fi placement in home
  - Center, high, avoid high interference objects
- Inventory
- Bandwidth creep
- Check your channel
- Download schedule

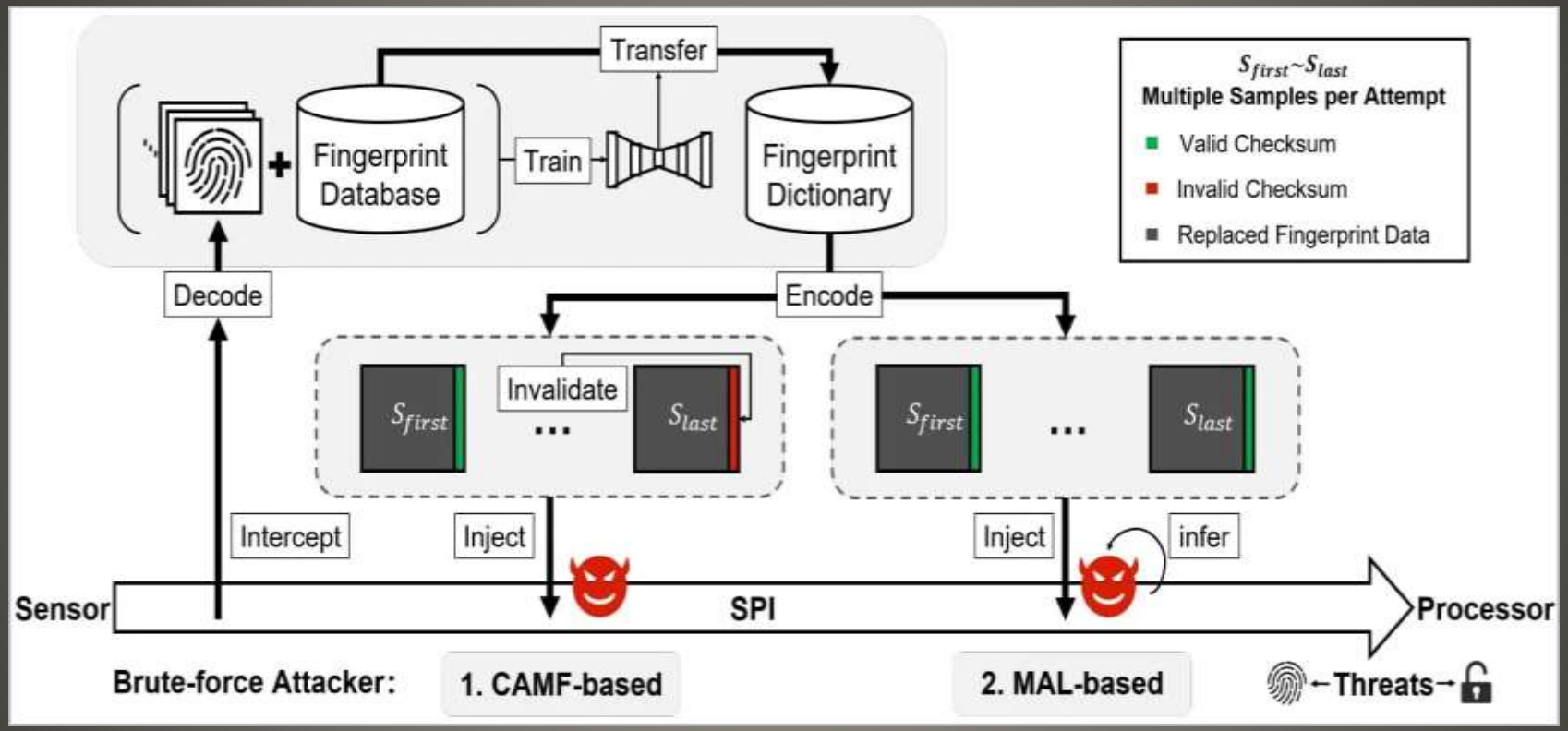

4:40
33%
VPN by Google One
Use VPN
Disconnected
Your network info
VPN is disconnected
Your IP address*:
Your network:
Turn on your VPN to hide your IP address to reduce online tracking. How can someone use my IP address?
*There may be a delay in updating your IP address. If your IP address is not updated, try refreshing the page.
With a VPN on your Android device, you can:
Reduce online tracking by hiding your IP address
Stay protected from hackers on unsecured networks (like public Wi-Fi)
Browse the web with a secure and private connection


4:39
33%
VPN by Google One
Use VPN
Connected. Your online activity is private.
Snooze for 5 min
Your network info
VPN is connected
Your IP address: hidden
Your network: hidden
Your IP address and network are hidden to reduce online tracking. How can someone use my IP address?
*There may be a delay in updating your IP address. If your IP address is not updated, try refreshing the page.
With a VPN on your Android device, you can:
Reduce online tracking by hiding your IP address
Stay protected from hackers on unsecured networks (like public Wi-Fi)

Android Devices brute-force fingerprint attack

- BrutePrint
- Brute-force trial and error crack a code, key, or password and gain unauthorized access
- Overcome safeguards and liveness detection
- Cancel-After-Match-fail (CAMF)
- Match-After-Lock (MAL)
- Biometric data on fingerprint sensors' Serial Peripheral Interface (SPI) inadequately protected
  Allowing man-in-the-middle (MiTM) hijack fingerprint images

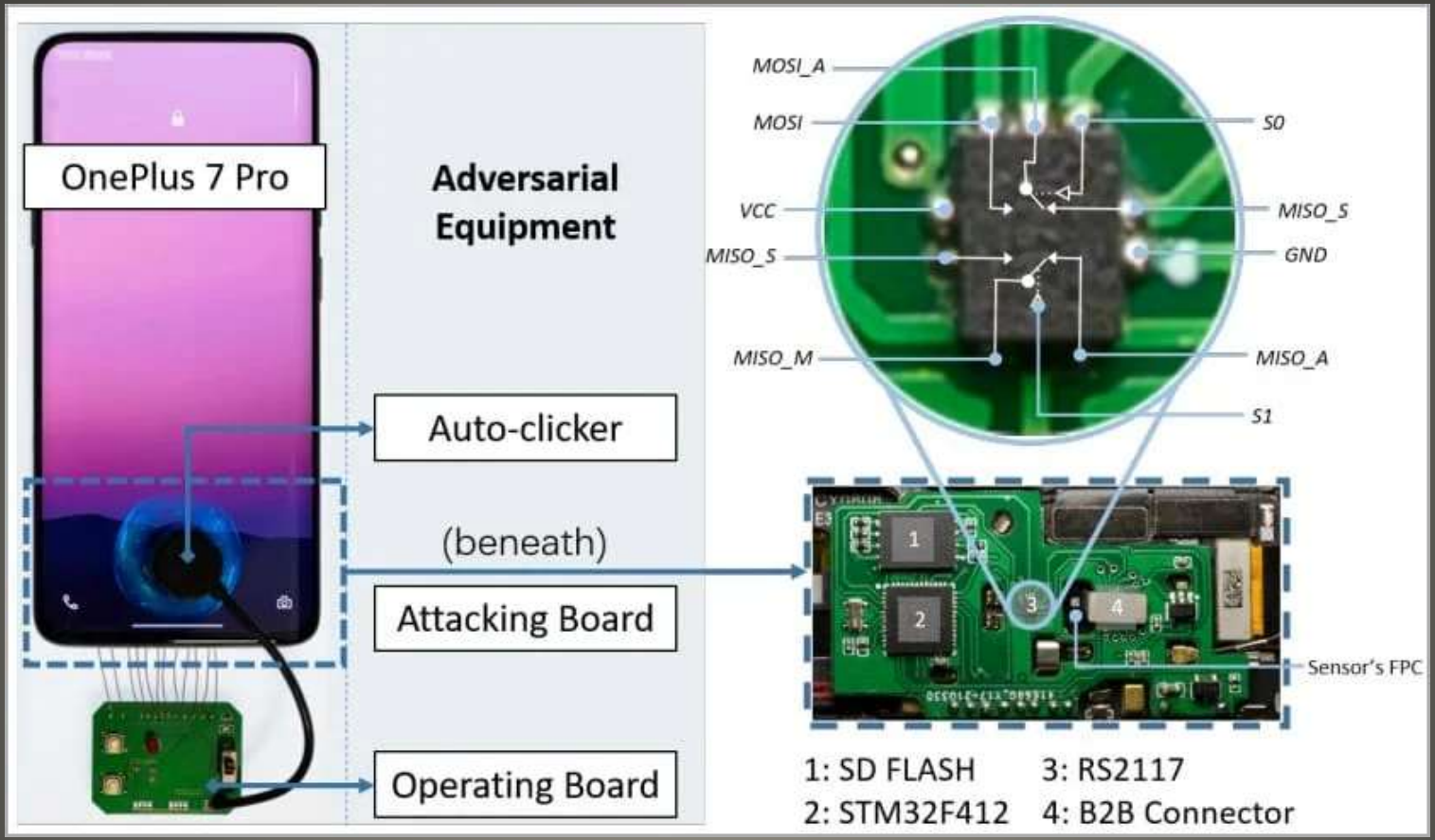
- Tested on Android, HarmonyOS (Huawei)



Android Devices brute-force fingerprint attack

- Unlimited number of submissions
  Until target is matched
- Physical access to device
- Fingerprint database
  Academic Datasets
  Biometric Data Leaks
  Equipment $15

Android Devices brute-force fingerprint attack

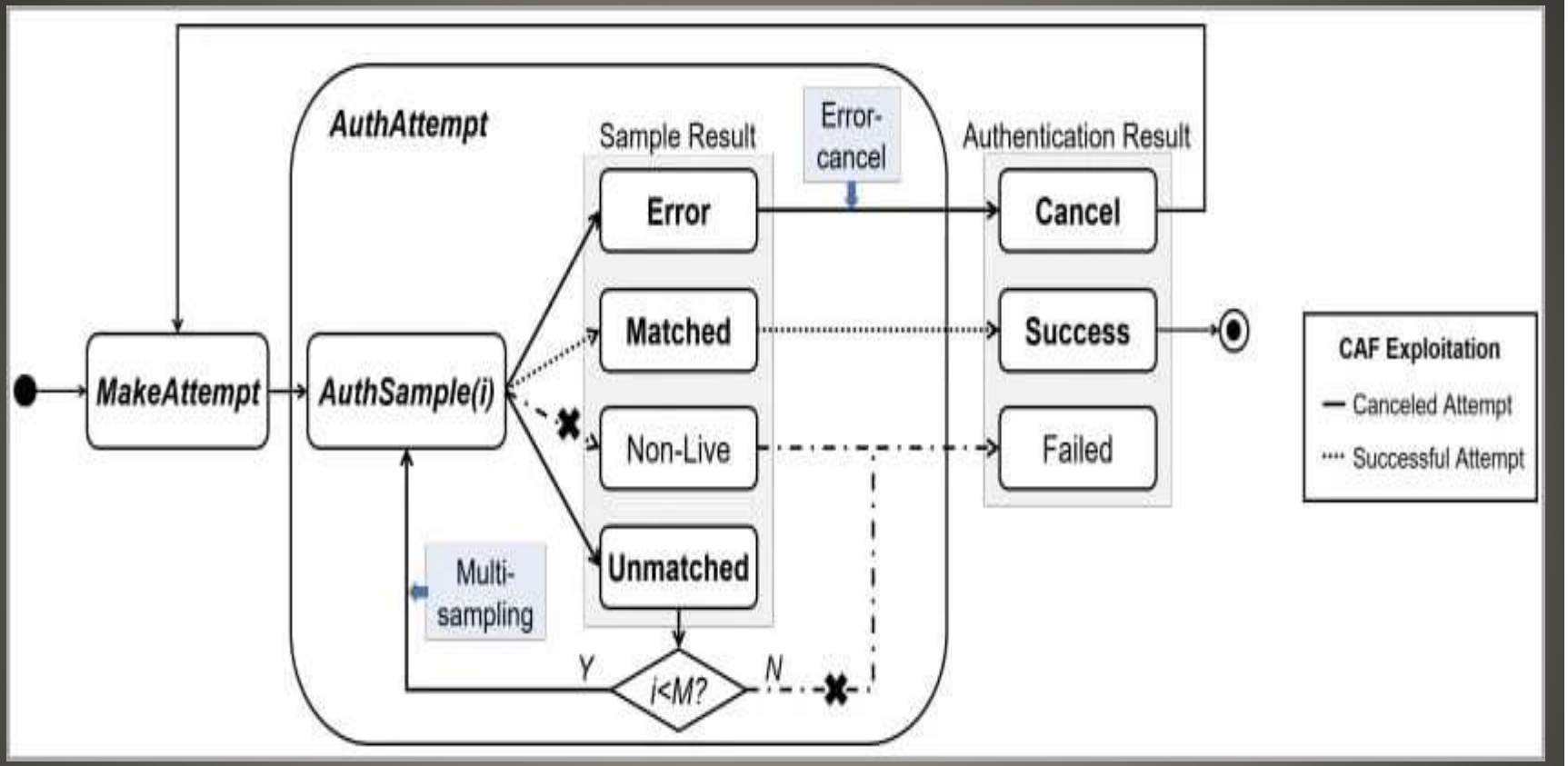


Android Devices brute-force fingerprint attack

- Manipulate False Acceptance Rate (FAR)
- BrutePrint between fingerprint sensor and CAMF flaw to manipulate multi-sampling and error-cancelling mechanism of fingerprint authentication
- CAMF injects checksum error in fingerprint data to stop authentication at pre-mature moment

Ability to try fingerprints while protection will not register failed attempts

Android Devices brute-force fingerprint attack



Android Devices brute-force fingerprint attack

- MAL flaw enables attacker to infer authentication results – even in lockout mode

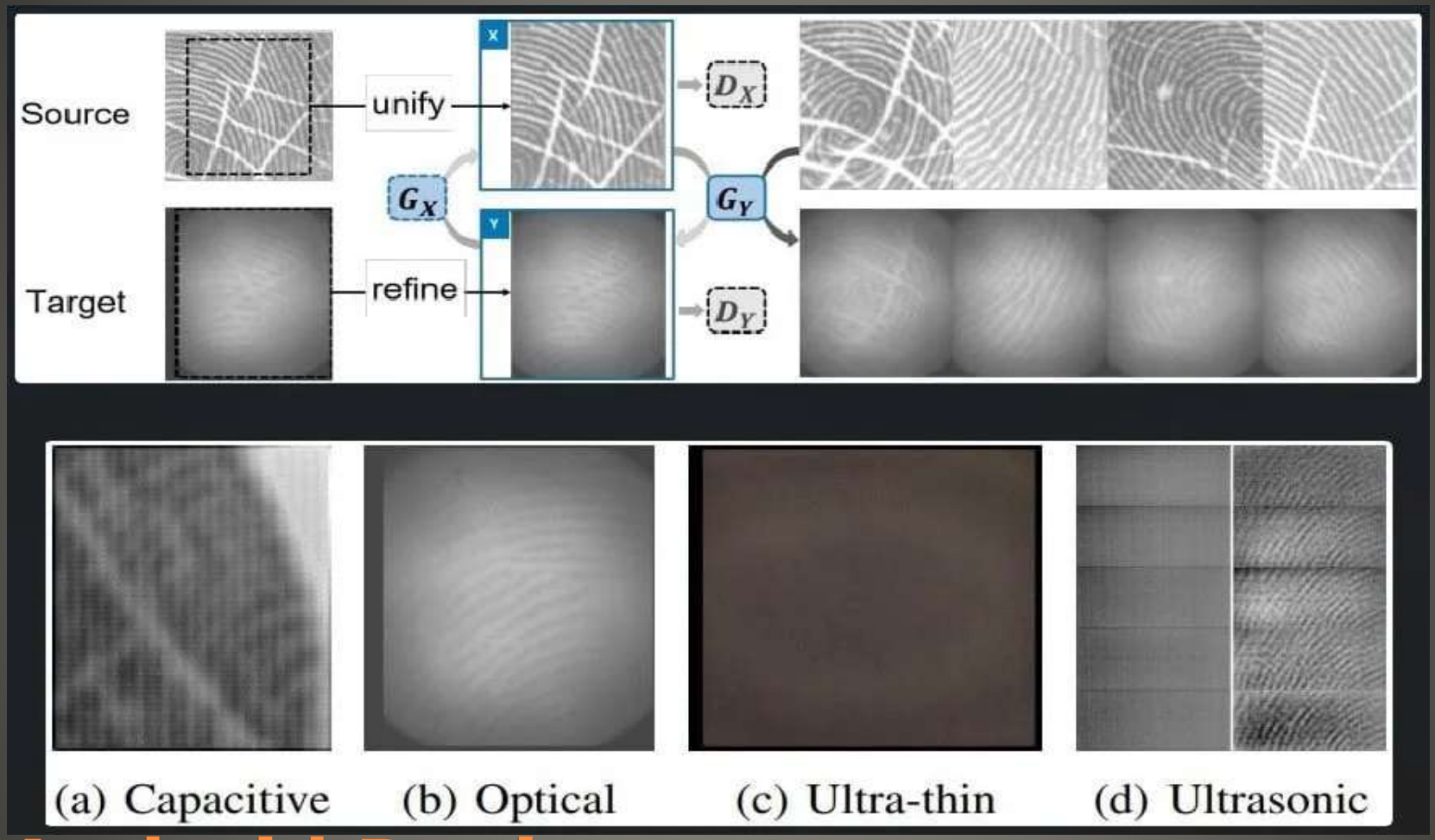
```
1  @override // com.android.server.biometrics.
       BiometricServiceBase
2  private void startAuthentication(
       AuthenticationClientImpl client, String
       opPackageName) {
3      ...
4      int lockoutMode = getLockoutMode();
5      if (lockoutMode != AuthenticationClient.
       LOCKOUT_NONE) {
6  +       if (ignoreLockout(onPackageName)) {
       /* isKeyguard: do nothing. */}
7          else { /* Lockout mode: disallowing
       authentication and return. */ }
8      }
9      /* Calls HAL to switch to the task. */
10     startClient(client, true);
11 }
```

Android Devices brute-force fingerprint attack

- Lockout protection activated after a number of failed attempts

  MAL helps by bass this restriction
- Neural transfer all images in fingerprint database to appear as target device sensor scanned them

Android Devices brute-force fingerprint attack



Android Devices brute-force fingerprint attack

Device				Sensor		Attempt Limit		
Manuf./Model	OS/Ver.	TEE	r_{max}	Manuf.	Type	ScreenLock[1]	Payment[2]	Privacy[3]
Xiaomi Mi 11 Ultra	Android 11	QTEE	5	Goodix	Optical (ultra-thin)*	5×4	5×4	5
Vivo X60 Pro	Android 11	Kinibi	5	Goodix	Optical*	5	∞	5
OnePlus 7 Pro	Android 11	QTEE	5	Goodix	Optical*	5	5	5
OPPO Reno Ace	Android 10	QTEE	5	Goodix	Optical*	5×4	5×4	5×4
Samsung Galaxy S10+	Android 9	Knox	4	Qualcomm	Ultrasonic*	5×10	5	5×10
OnePlus 5T	Android 8	QTEE	5	Goodix	Capacitive	5×4	5×4	5×4
Huawei Mate30 Pro 5G	HarmonyOS 2	TrustedCore	5	Goodix	Optical*	5×4	5×∞	5×∞
Huawei P40	HarmonyOS 2	TrustedCore	5	Novatek	Optical*	5×4	5×∞	5×∞
Apple iPhone SE	iOS 14.5.1	Secure Enclave	5	AuthenTec	Capacitive	5	5	5
Apple iPhone 7	iOS 14.4.1	Secure Enclave	5	AuthenTec	Capacitive	5	5	5

Android Devices brute-force fingerprint attack

	Attributes					Vulnerability	Attacks		
	Samples	Cancel	Hot-Plug	Decode	f_{SPI} (MHz)		Bypassing	Hijacking	Brute-force
Xiaomi Mi 11 Ultra	2	✔	✔	✔	32	CAMF, MAL	(∞,∞,∞)	✔	(✔,✔,✔)
Vivo X60 Pro	3	✔	✔	✔	25	CAMF, MAL	(∞,∞,∞)	✔	(✔,✔,✔)
OnePlus 7 Pro	4	✔	✔	✔	25	CAMF	(∞,∞,∞)	✔	(✔,✔,✔)
OPPO Reno Ace	3	✔	✔	✔	25	CAMF	(∞,∞,∞)	✔	(✔,✔,✔)
Samsung Galaxy S10+	2~4*	✔	✔	✔	24	CAMF	(∞,∞,∞)	✔	(✔,✔,✔)
OnePlus 5T	2	✔	✔	✔	4.8	CAMF	(∞,∞,∞)	✔	(✔,✔,✔)
HUAWEI Mate30 Pro 5G	2	N/A†	✔	✔	23	MAL	(∞,∞,∞)	✔	(✔,✔,✔)
HUAWEI P40	2	N/A†	✔	✔	23	MAL	(∞,∞,∞)	✔	(✔,✔,✔)
Apple iPhone SE	3	✔	✔	✘	7.7	CAMF	(15,15,15)	✘	(✘,✘,✘)
Apple iPhone 7	3	✔	✔	✘	7.7	CAMF	(15,15,15)	✘	(✘,✘,✘)

Android Devices brute-force fingerprint attack

Android Devices brute-force fingerprint attack

- All tested Android devices vulnerable
- iOS limited to only 15 attempts
  Fingerprint data on SPI is encrypted
- Time to attack 2.9 – 13.9 hours one print
- Time to attack 0.66 – 2.78 hours multiple prints
- Typically 3 locations for scanners:
  Side mounted
  Back mounted
  Under display

A $15 TOOLS BREAKS SMARTPHONES FINGERPRINT SCANNERS PROTECTION

- iDevices
- Safer fingerprint database is encrypted
- Yeahbut Close enough?

- Older devices
- Older Android

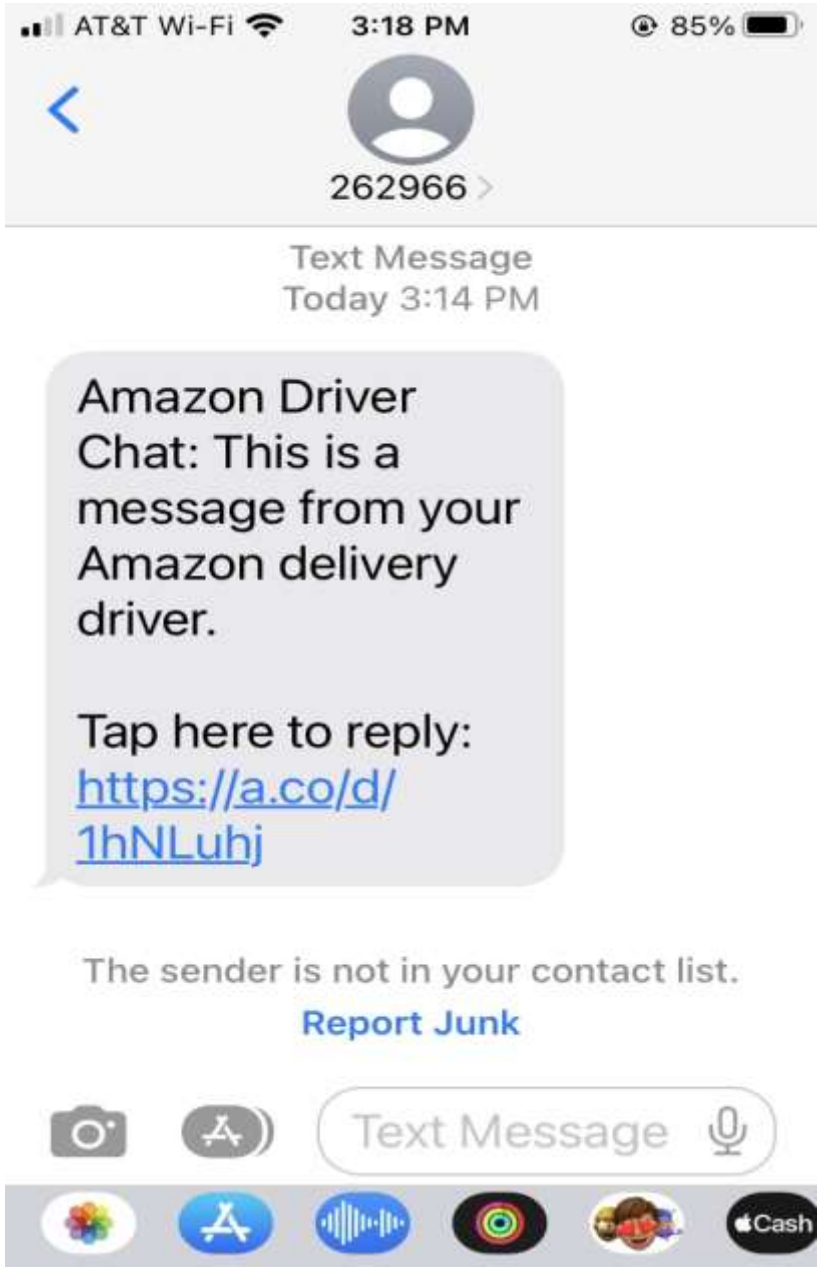
Android Protections

Current Issues

- PyPI – open-source Python package repository disables new user registrations and uploading of new projects due to unmanageable flood of malicious codes
- Android *iRecorder – Screen Recorder*
  Now reported as malicious App
  Version 1.3.8
  Removed from Google Play Store
  Manually remove if you have downloaded
- Android 11 and up
  App hibernation several months
  Resets all permissions
- Super VPN
  No Logs claim
  yeahbut Logs – detailed logs - exposed

PyPI

- Follow on
- Efforts to purge IP addresses
- Efforts to encrypt IP addresses
- Salt NOT stored
- WHY?
- US DOJ subpoena


AT&T Wi-Fi
3:18 PM
85%
262966
Text Message
Today 3:14 PM
Amazon Driver Chat: This is a message from your Amazon delivery driver.
Tap here to reply: https://a.co/d/1hNLuhj
The sender is not in your contact list.
Report Junk
Text Message
Cash

Intuit
www.intuit.com

Visit site →

You got Owned

Yahoo/Inbox

Got You <quickbooks@notification.intuit.com>
To: coin2-other@pro.space

Sat, May 27 at 4:38 PM

Hello

I know your password!

I infected you with a malware (RAT)/(Remote Administration Tool), some time ago and since then, I have been observing your actions. The malware gave me full access and control over your system, meaning, I can see everything on your screen, turn on your camera or microphone and you won't even notice about it, yes such things exist, you can Google it!
I have also access to all your contacts, I collected everything private from you, pictures, videos, everything!

And I MADE A VIDEO SHOWING BOTH YOU (through your webcam) AND THE VIDEO YOU WERE WATCHING (on the screen) WHILE [redacted]

I can send this video to all your contacts (email, social network) and publish all your private stuff everywhere!

You can prevent me from doing this!
To stop me, transfer exactly: 900$ with the current bitcoin (BTC) price to my bitcoin address.

If you don't know how to get bitcoin, Google - "How to buy Bitcoin", it's very simple for example with credit card. The wallet you can create here: https://www.blockchain.com

My bitcoin address is: [redacted]

Copy and paste my address - it's (CASE-sensitive).

You know this all isn't a joke, you got the proof above!
I think it's a very good price compared to the damage and hell it can bring into your life!

After receiving the payment, I will delete everything about you and you can live your life in peace like before. I give you 3 days to get the bitcoins!
Don't share this email with anyone, this should stay our little secret!

Intuit

- TurboTax – US Tax Prep
- Mint – personal finance
- QuickBooks – small business accounting
- Credit Karma – credit monitoring
- Mailchimp – email marketing

TurboTax Free File -> Paid TurboTax Free Edition

search engine delisting & military discount

Major account & password issues

Quicken

PayPal

- Online shopping
- Peer payments
- Money transfers
- Mobile App and web
- Phishing & Identity fraud
- Recent PayPal incidents
- Attacker then places order
  - Fake on non-existent physical address
  - Monitors delivery
  - Ooops, use this address
  - Shipper delivers to re-routed address
  - Attacker files complaint – not delivered
  - Since re-routed no proof of delivery
  - Attacker keeps items and money
  - Then not covered by seller protections

PayPal

- Fake invoice
- Overpays then asks for refund of overpayment
  Attacker claims the overpayment from your bank
- Use my preferred shipper

- Generic greeting?
- Bad grammar
- Investigate attachments
- Request personal information
- Payment request
- Use **Goods and Services** as payment
- PayPal's safeguard program
- STRONG passphrase with MFA
- Monitor PayPal account

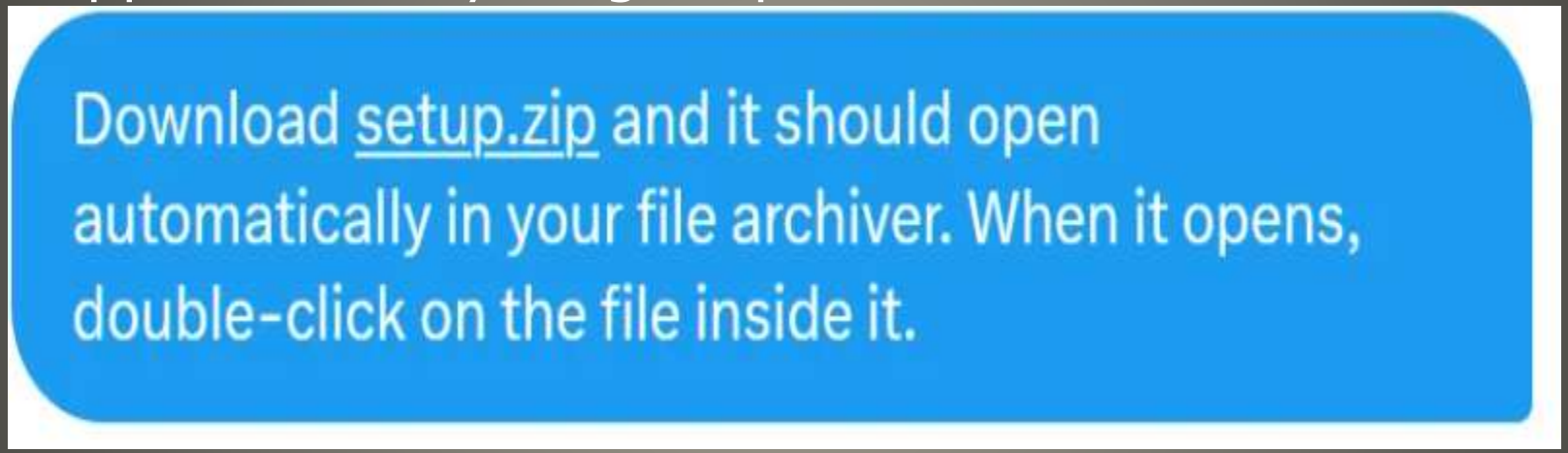
PayPal & Others

Mobile

- Hardware
- OS
- Apps
- Other apps
- malware

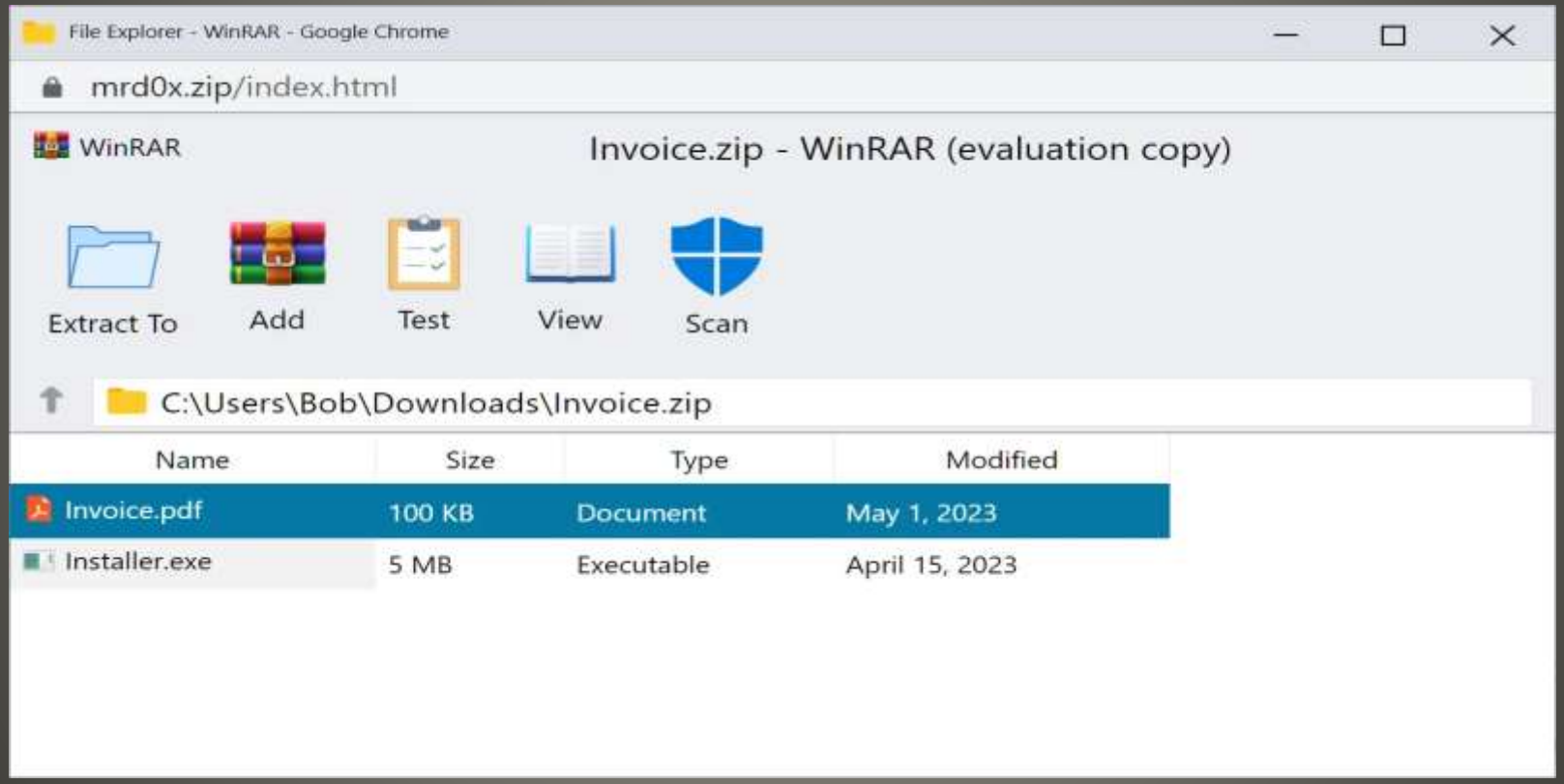
File Archivers in the Browser

- Phishing kit
- Fake WinRAR or File Explorer windows in browser
- .zip TLD domains
- Apps turn <anything>.zip into clickable link



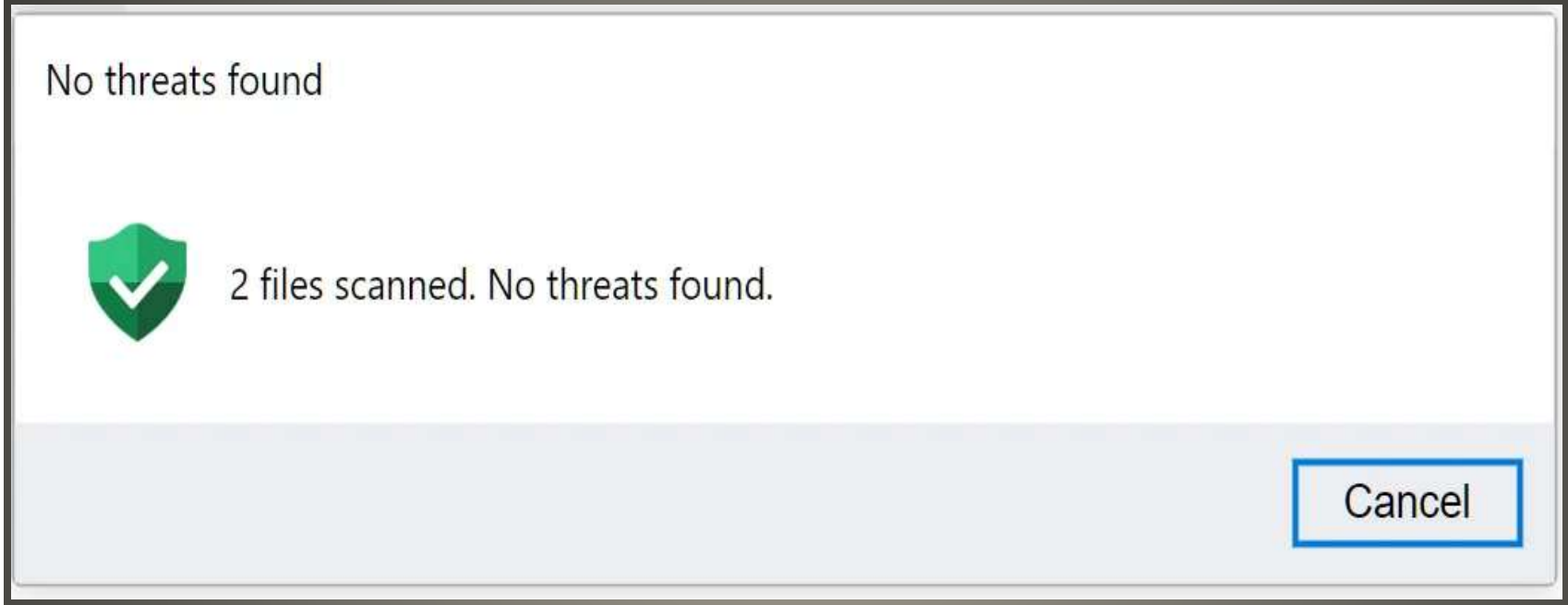
- How to trick victim to click?
- Redirect to another site
- Download a malicious file

- FAKE File Explorer window in Browser
- FAKE WinRAR window in Browser

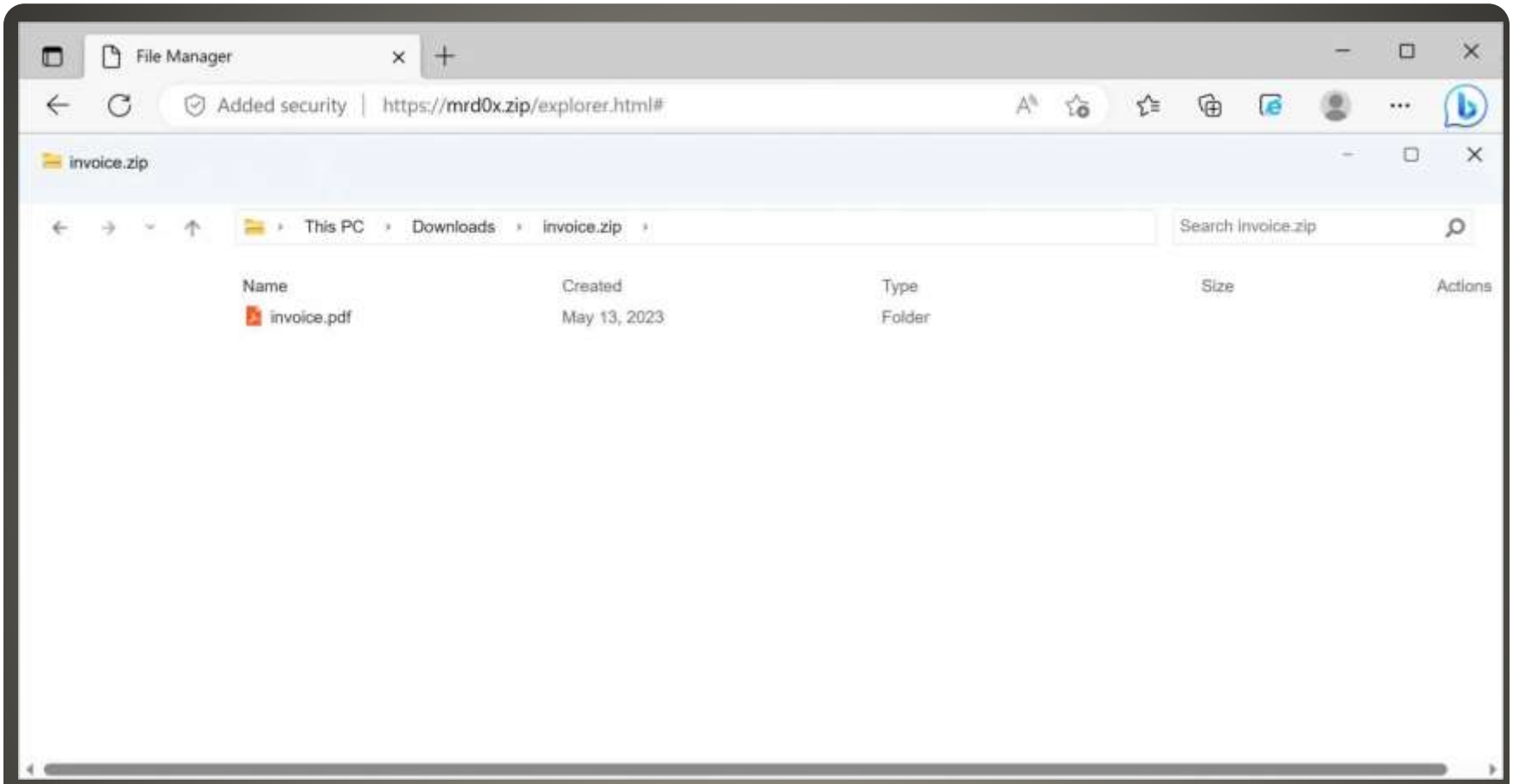


File Archivers in Browser

- With FAKE Security scan



Fake Archivers in Browser



Fake Archivers in Browser

Fake Archivers in Browser

- Click on PDF > redirect to credential stealing page
- Click on file link, download malicious file
- If windows set to not display file extensions !!
- Windows search configured to search WEB

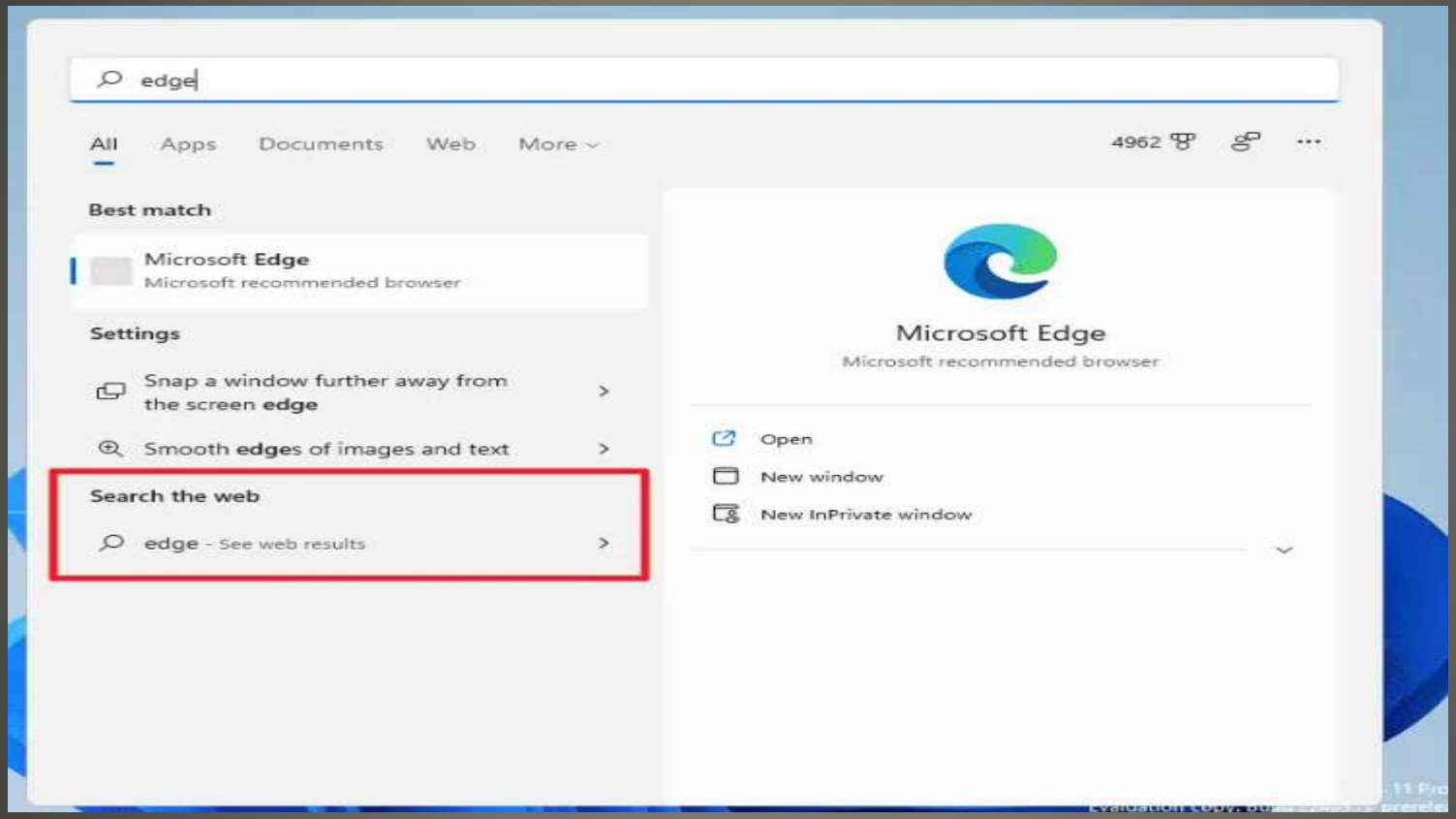
- .zip domains potential for abuse
- .mov domains potential for abuse
- Other TLD .dad .phd .prof .esq .foo .nexus

https://github.com/kubernetes/kubernetes/archive/refs/tags/v1.27.1.zip
https://github.com/kubernetes/kubernetes/archive/refs/tags/@v1.27.1.zip

- Unicode characters
- Example forward slashes NOT interpreted as separators

Image NOT Links

- Disable WEB search in Windows Edge

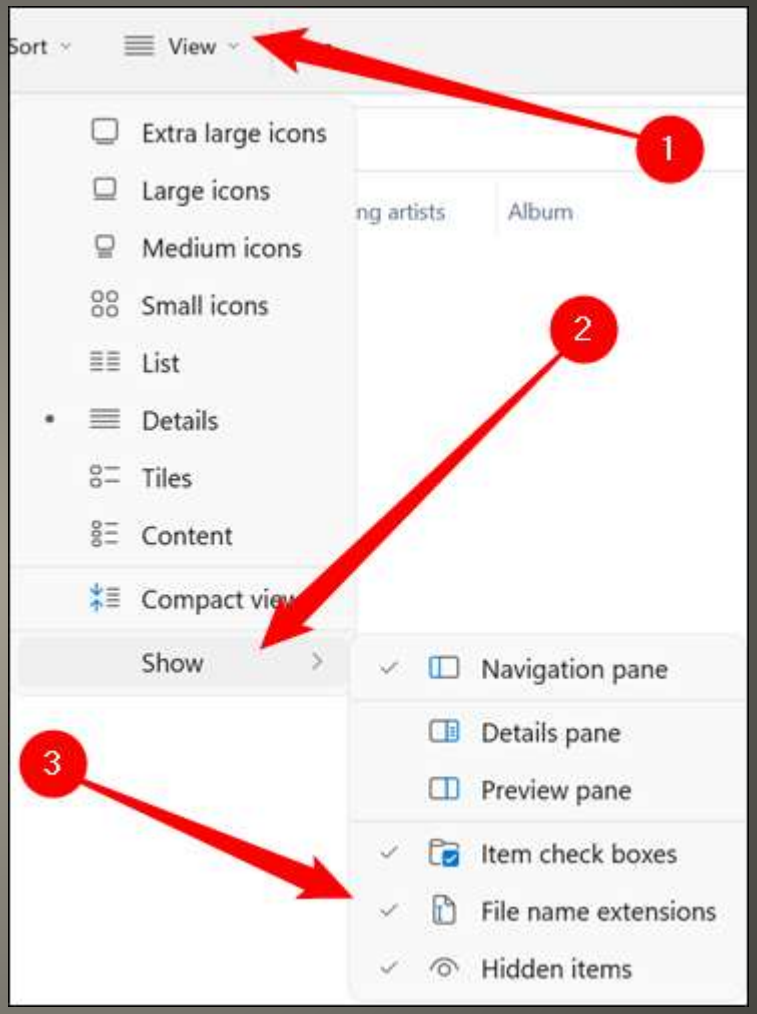


Suggested Changes

- Disable WEB Search in Windows Search Regedit or Group Policy

Suggested Changes

- File Explorer > View



Suggested Changes

Control Overlays

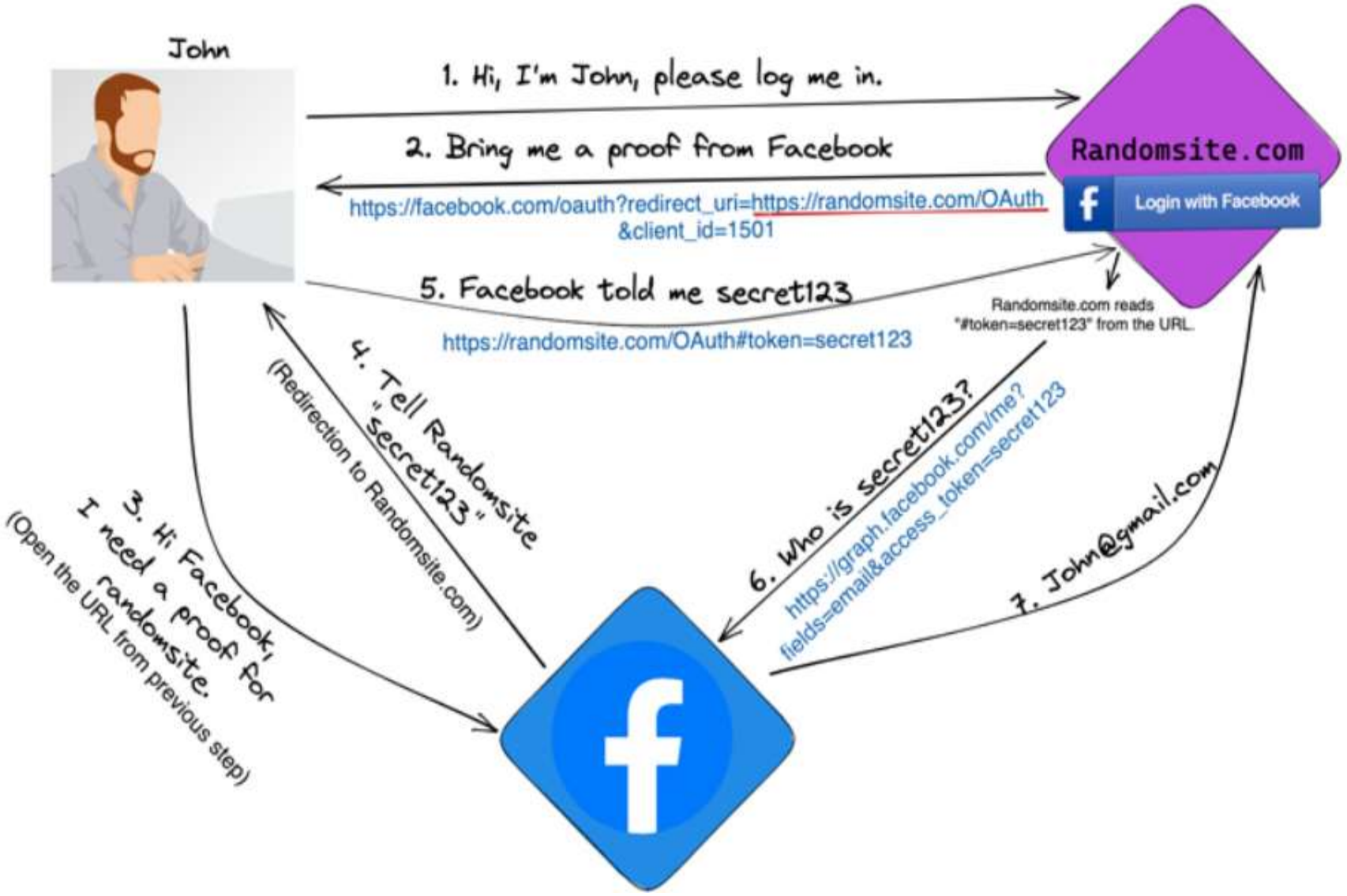
- *BehindTheOverlay* browser extension
- Cmd+Shift+X macOS
- Ctrl+Shift+X Windows

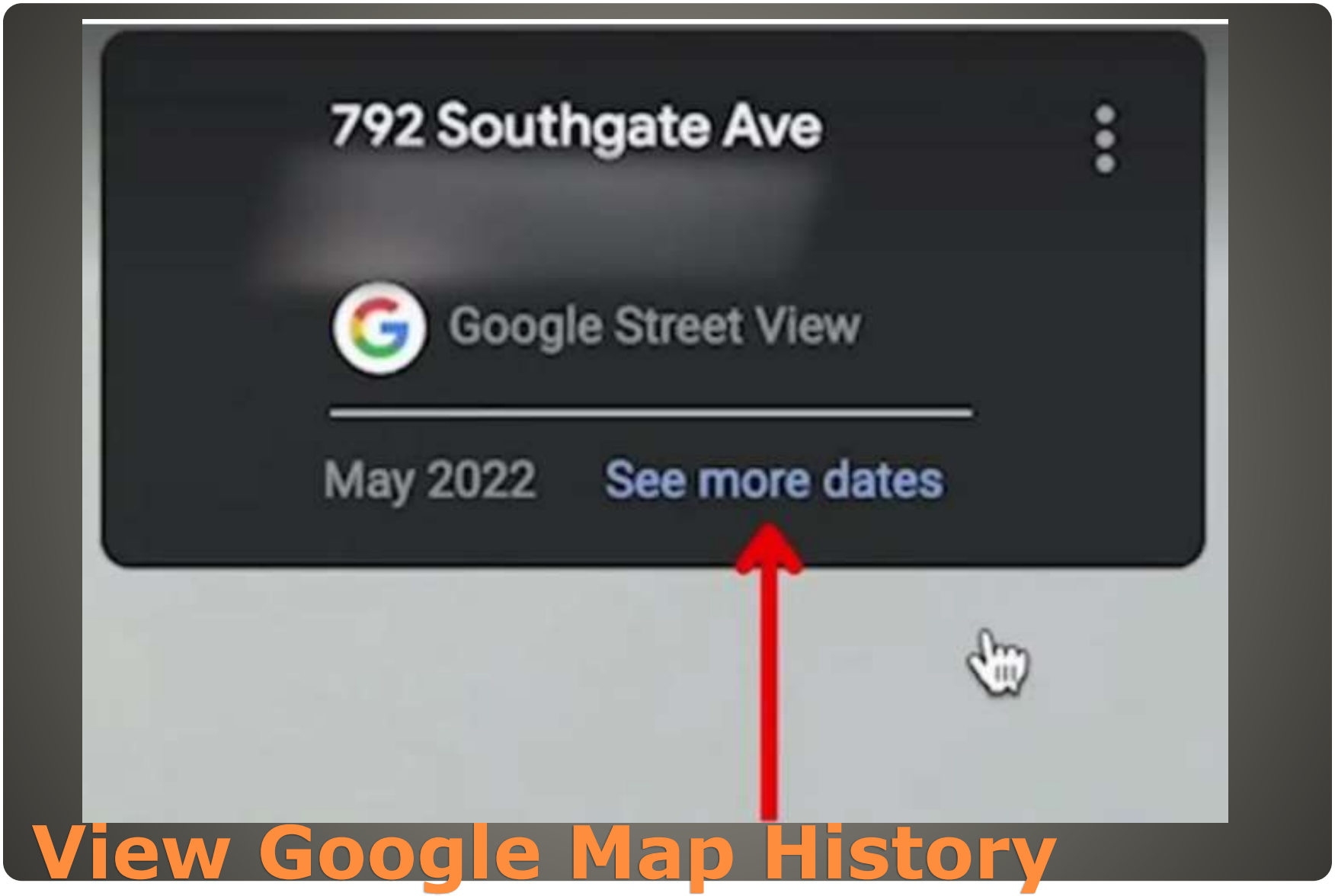
AirTags

- Beep No Beep
- Notify law enforcement for stolen items
- Especially autos

Oauth vulnerability

- Application development framework *Expo.io*
- CVSS score 9.6
- Credential leakage


John
1. Hi, I'm John, please log me in.
2. Bring me a proof from Facebook
https://facebook.com/oauth?redirect_uri=https://randomsite.com/OAuth
&client_id=1501
Randomsite.com
Login with Facebook
5. Facebook told me secret123
https://randomsite.com/OAuth#token=secret123
Randomsite.com reads
"#token=secret123" from the URL.
4. Tell Randomsite
"secret123"
(Redirection to Randomsite.com)
3. Hi Facebook,
I need a proof for
randomsite.
(Open the URL from previous step)
6. Who is secret123?
https://graph.facebook.com/me?
fields=email&access_token=secret123
7. John@gmail.com



View Google Map History

- Search Labs Testing Sign-up
- Search Generative Experience SGE

Google AI-boosted search trial

Current Issues

- Chrome update

Version 114.0.5735.91 (Official Build) (64-bit)

- Brave Update

Version 1.52.117 Chromium: 114.0.5735.90

- Firefox 113.0.2
- Edge 113.0.1774.57
- Vivaldi 6.0.2979.22
- Mullvad 12.0.6
- Safari 16.5 (18615.2.9.11.4)
- Tor 12.0.6

Alternative Browsers

- Epic
  Security & Anonymity
  Chromium based
  built-in VPN
  Hidden Reflex – removes all Google Services
  Few plugins
- Tor
  requires some knowledge -
  not plug-and-play
- Maxthon
  Feature rich
  Not private

Alternative Browsers

- Ungoggled Chromium
  Linux lightweight
- Torch
  Torch your history

Personal Devices

- iPhone
- Much worse than home burglary
- 18 seconds
- Snatch iPhone from your hand/table/…
- Keychain Bank apps Financial shopping
- Contact, messages, photos, digital life
- Apple ID password changed
- You then can NOT recover - ever
- Recovery key - Apple’s proof if Identity
- FindMy
- iCloud backup

IMPORTANT

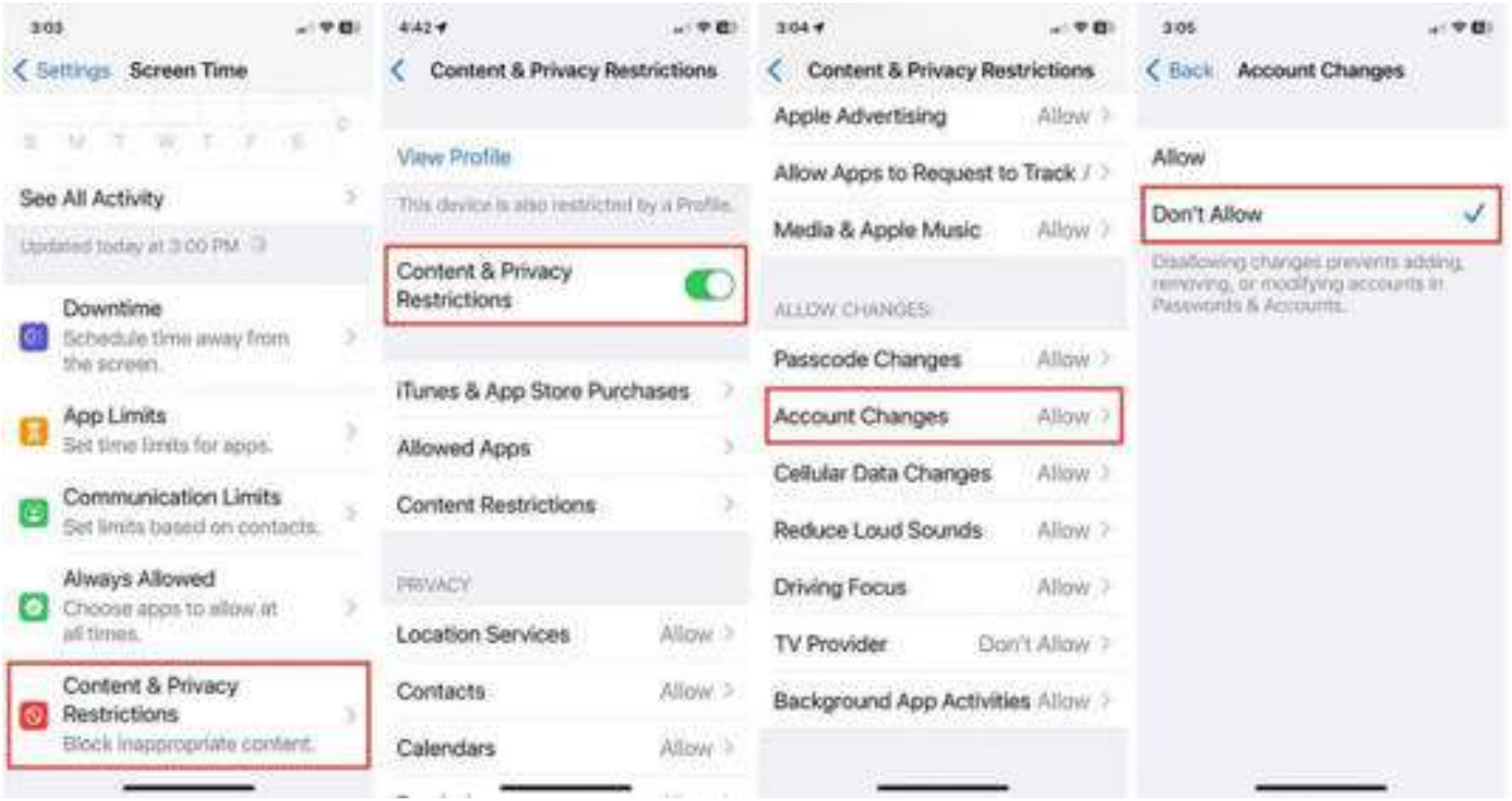
https://vimeo.com/804354706?share=copy

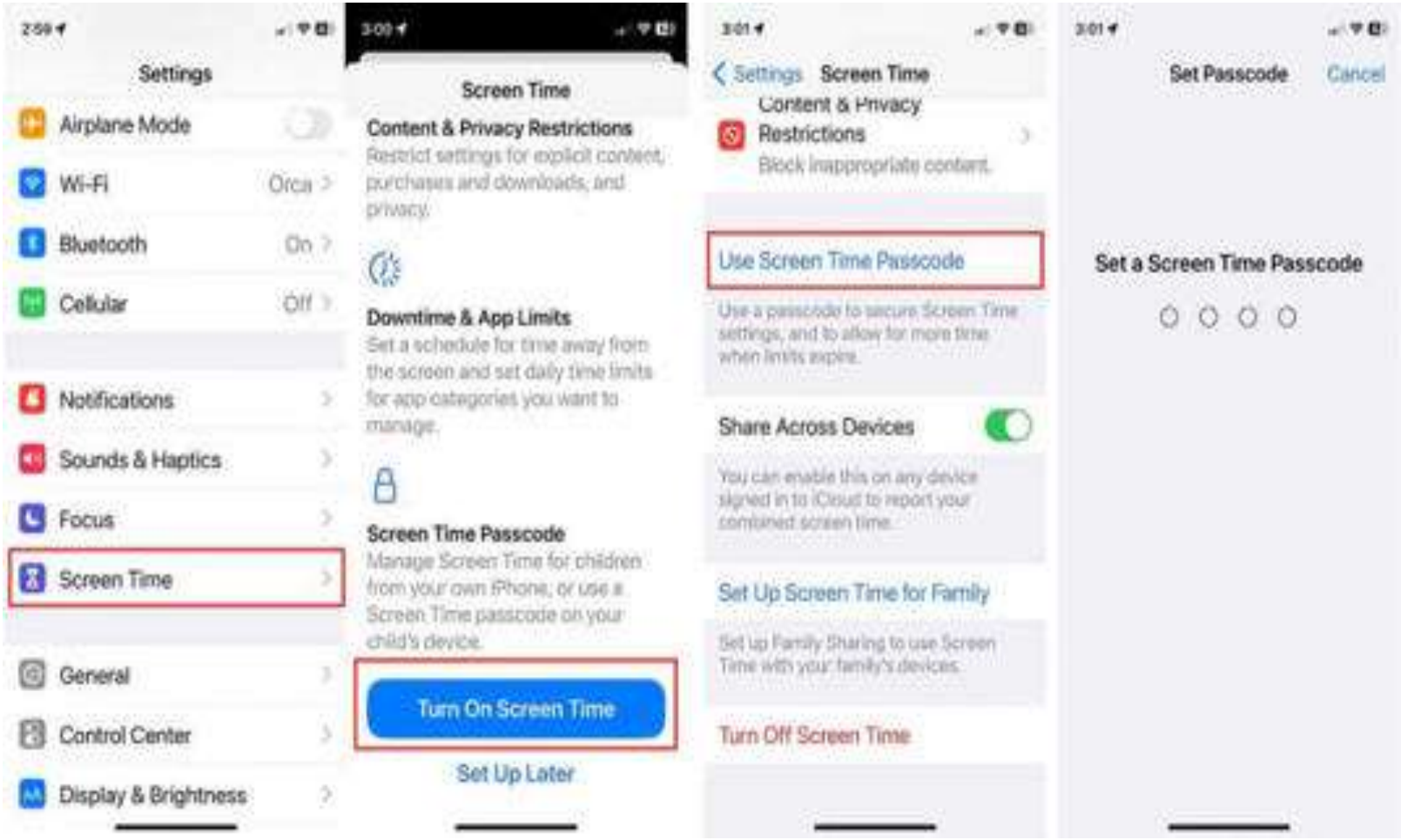
After CA login with Resident ID
Cyber Security SIG 2023 Presentations

Important

- Screen Time
- A preventative measure designed for minors
- Preventative Measure

Important iPhone Protections


3:03
Settings
Screen Time
See All Activity
Downtime
Schedule time away from the screen.
App Limits
Set time limits for apps.
Communication Limits
Set limits based on contacts.
Always Allowed
Choose apps to allow at all times.
Content & Privacy Restrictions
Block inappropriate content.
4:42
Content & Privacy Restrictions
View Profile
This device is also restricted by a Profile.
Content & Privacy Restrictions
iTunes & App Store Purchases
Allowed Apps
Content Restrictions
PRIVACY
Location Services
Allow
Contacts
Allow
Calendars
Allow
3:04
Content & Privacy Restrictions
Apple Advertising
Allow
Allow Apps to Request to Track
Media & Apple Music
Allow
ALLOW CHANGES:
Passcode Changes
Allow
Account Changes
Allow
Cellular Data Changes
Allow
Reduce Loud Sounds
Allow
Driving Focus
Allow
TV Provider
Don't Allow
Background App Activities
Allow
3:05
Back
Account Changes
Allow
Don't Allow
Disallowing changes prevents adding, removing, or modifying accounts in Passwords & Accounts.


Settings
Airplane Mode
Wi-Fi
Orca
Bluetooth
On
Cellular
Off
Notifications
Sounds & Haptics
Focus
Screen Time
General
Control Center
Display & Brightness
Screen Time
Content & Privacy Restrictions
Restrict settings for explicit content, purchases and downloads, and privacy.
Downtime & App Limits
Set a schedule for time away from the screen and set daily time limits for app categories you want to manage.
Screen Time Passcode
Manage Screen Time for children from your own iPhone, or use a Screen Time passcode on your child's device.
Turn On Screen Time
Set Up Later
Settings
Screen Time
Content & Privacy Restrictions
Block inappropriate content.
Use Screen Time Passcode
Use a passcode to secure Screen Time settings, and to allow for more time when limits expire.
Share Across Devices
You can enable this on any device signed in to iCloud to report your combined screen time.
Set Up Screen Time for Family
Set up Family Sharing to use Screen Time with your family's devices.
Turn Off Screen Time
Set Passcode
Cancel
Set a Screen Time Passcode

- Awareness
- Preparedness
- Understanding

Important Measure
Not the ONLY measure

Smartphone

- Constant connection
- Contains your life information
- Can deliver information
- Can receive information
- 24x7
- Wait, are *they* after *me*?
- Attempts to logon to your AppleID
- Popups, notifications, messages, …
- Gather evidence
- **Screen Recorder**
  Not all apps allow screen recording

- Amazon polarized sunglasses
  WITH Alexa
  AND audio books
  AND news
  audio level adjusts

- Add Screen Recording to Control Center
  Settings > Control Center +Screen Recording

Screen Recording for evidence


100%
Not Playing
Focus

- CISA order
- All Federal Civilian Executive Branch Agencies
- Patch all Apple devices by June 12

- Modified to attack macOS

Goland Cobalt Strike variant

- iCloud Keychain
- Credit Card data
- Cryptocurrency wallet
- Browser cookies
- weed.dmg

- Keep Up to Date
- Only install from trusted sources

MacStealer

- iCloud Keychain
- Credit Card data
- Cryptocurrency wallet
- Browser cookies
- Notion-7.0.6.dmg
  Photoshop cc 2023.dmg
  Tor Browser.dmg

  More and More targeting macOS
- Keep Up to Date
- Only install from trusted sources

Atomic macStealer

Google Android Bug Bounty Program

- Mobile Vulnerability Reward Program
- First-party Android apps
- Start $500 tier 3 apps
- Tier 1 $30,000
- Tier 2 $25,000
- Tier 3 $20,000

- Attacker with physical access to iPhone
- Scan QR code on PC Monitor with victim iPhone
- View call history, iMessages, Notifications
- iPhone owner unaware
- Bluetooth settings “Forget device”
- Notifications on PhoneLink, not on iPhone

Windows PhoneLink iOS

- Good

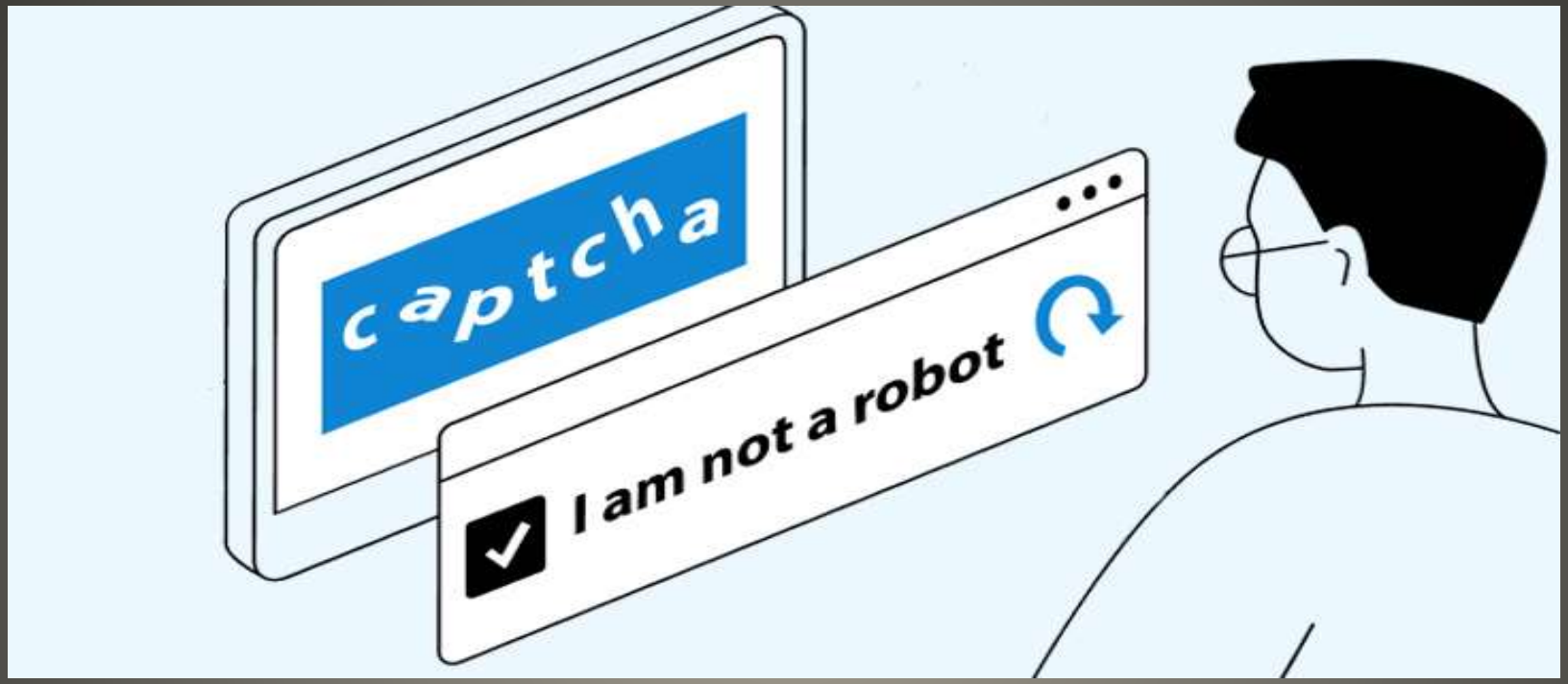
IoT Auto Updating

IoT Auto Updating

- HP 9020e
- Bricked printers auto update
- Detect non HP Ink

- HP Ooopsie

- Malicious ??



Completely Automated Public Turing Test CAPTCHA solving services

CAPTCHA-breaking services Human Solvers

- Recognize anyone in this photo?

Classmates

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

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

- Questions, suggestions, comments?

SCCCCyber@gmail.com