Sun City Computer Club

Cyber Security SIG

December 2, 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??

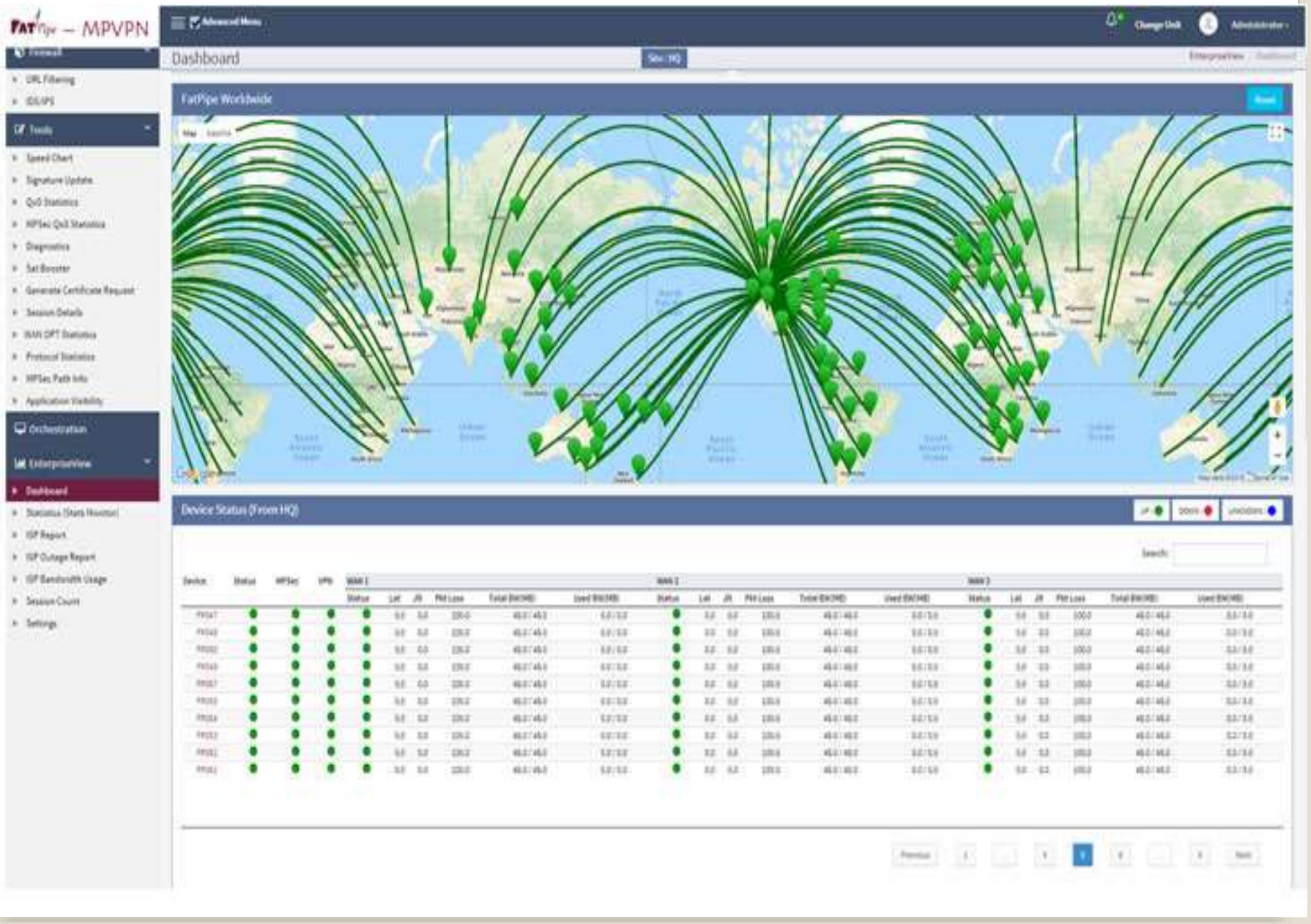
Presenter???

Current Issues

- BotenaGo Malware
  Golang
  potential to attack millions
- FBI flash alert 16-Nov-2021
  FatPipe MPVPN
- HP printer wormable security flaws
  Printing Shellz
  CVE-2021-39237
  CVE-2021-39238

HP Printer Patch Information

- DNA Diagnostics Center data breach 2Million+


FatPipe – MPVPN
Dashboard
URL Filtering
IDS/IPS
Tools
Speed Chart
Signature Update
QoS Statistics
MPSec QoS Statistics
Diagnostics
Sat Booster
Generate Certificate Request
Session Details
WAN OPT Statistics
Protocol Statistics
MPSec Path Info
Application Visibility
Orchestration
EnterpriseView
Dashboard
ISP Report
ISP Outage Report
ISP Bandwidth Usage
Session Count
Settings
FatPipe Worldwide
Device Status (From HQ)

Current Issues

- 127.1.0.0 – 127.255.255 proposal
  - 16 million more IPv4 addresses
- Microsoft honeypot stats
  - 6 characters
- GoDaddy breach
  - 1.2 million customers
  - 2 month window
- NetGear routers
  - UPnP remote code execution

Check home infrastructure regularly

Vulnerable Devices		
AC1450 - 1.0.0.36	D6220 - 1.0.0.72[1]	D6300 - 1.0.0.102
D6400 - 1.0.0.104[1]	D7000v2 - 1.0.0.66	D8500 - 1.0.3.60[1]
DC112A - 1.0.0.56	DGN2200v4 - 1.0.0.116	DGN2200M - 1.0.0.35
DGND3700v1 - 1.0.0.17	EX3700 - 1.0.0.88	EX3800 - 1.0.0.88
EX3920 - 1.0.0.88	EX6000 - 1.0.0.44	EX6100 - 1.0.2.28
EX6120 - 1.0.0.54	EX6130 - 1.0.0.40	EX6150 - 1.0.0.46
EX6920 - 1.0.0.54	EX7000 - 1.0.1.94	MVBR1210C - 1.2.0.35BM
R4500 - 1.0.0.4	R6200 - 1.0.1.58	R6200v2 - 1.0.3.12
R6250 - 1.0.4.48	R6300 - 1.0.2.80	R6300v2 - 1.0.4.52[1]
R6400 - 1.0.1.72[1]	R6400v2 - 1.0.4.106	R6700 - 1.0.2.16
R6700v3 - 1.0.4.118	R6900 - 1.0.2.16	R6900P - 1.3.2.134
R7000 - 1.0.11.123[1]	R7000P - 1.3.2.134	R7300DST - 1.0.0.74
R7850 - 1.0.5.68	R7900 - 1.0.4.38	R8000 - 1.0.4.68
R8300 - 1.0.2.144	R8500 - 1.0.2.136	RS400 - 1.5.0.68
WGR614v9 - 1.2.32	WGT624v4 - 2.0.13	WNDR3300v1 - 1.0.45
WNDR3300v2 - 1.0.0.26	WNDR3400v1 - 1.0.0.52	WNDR3400v2 - 1.0.0.54
WNDR3400v3 - 1.0.1.38	WNDR3700v3 - 1.0.0.42	WNDR4000 - 1.0.2.10
WNDR4500 - 1.0.1.46	WNDR4500v2 - 1.0.0.72	WNR834Bv2 - 2.1.13
WNR1000v3 - 1.0.2.78	WNR2000v2 - 1.2.0.12	WNR3500 - 1.0.36NA
WNR3500v2 - 1.2.2.28NA	WNR3500L - 1.2.2.48NA	WNR3500Lv2 - 1.2.0.66
XR300 - 1.0.3.56		

Current Issues

- HTTP Request Smuggling
  Modern WEB hosting is multi-tiered
  Load balancing, filtering, caching, etc.
  connection oriented i.e., persistent
  So request boundaries

Content-Length

```
POST /search HTTP/1.1
Host: normal-website.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
```

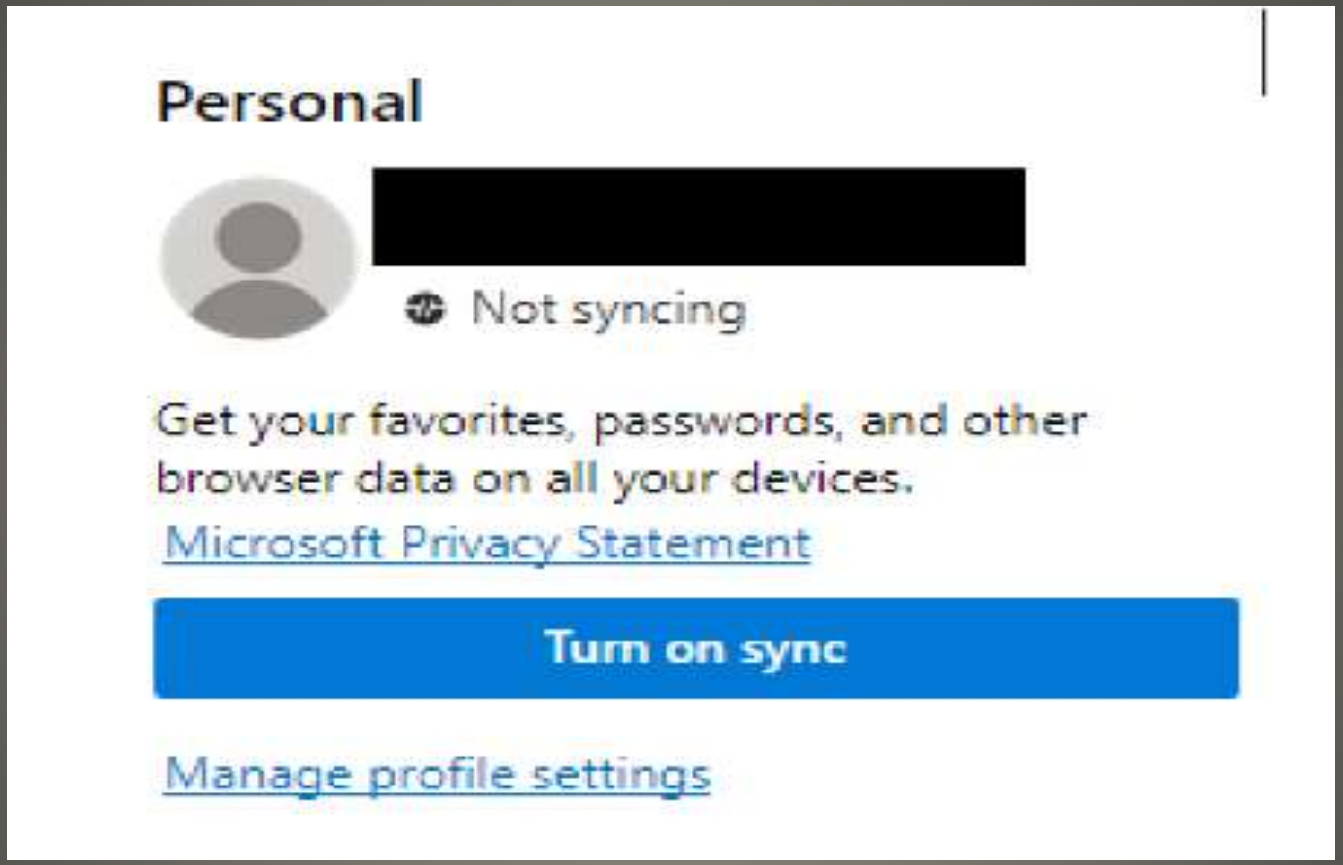
Transfer-Encoding

```
POST /search HTTP/1.1
Host: normal-website.com
Content-Type: application/x-www-form-urlencoded
Transfer-Encoding: chunked
```

Vulnerability understood and noted but

Current Issues

- Proposed UK law bans default passwords
  IoT devices
- Apple suing NSO group – Pegasus
  Facebook also suing NSO group
- Crypto meaning bleed
  Cryptography -> crypto currency
- Edge synching caution



Microsoft Edge synching

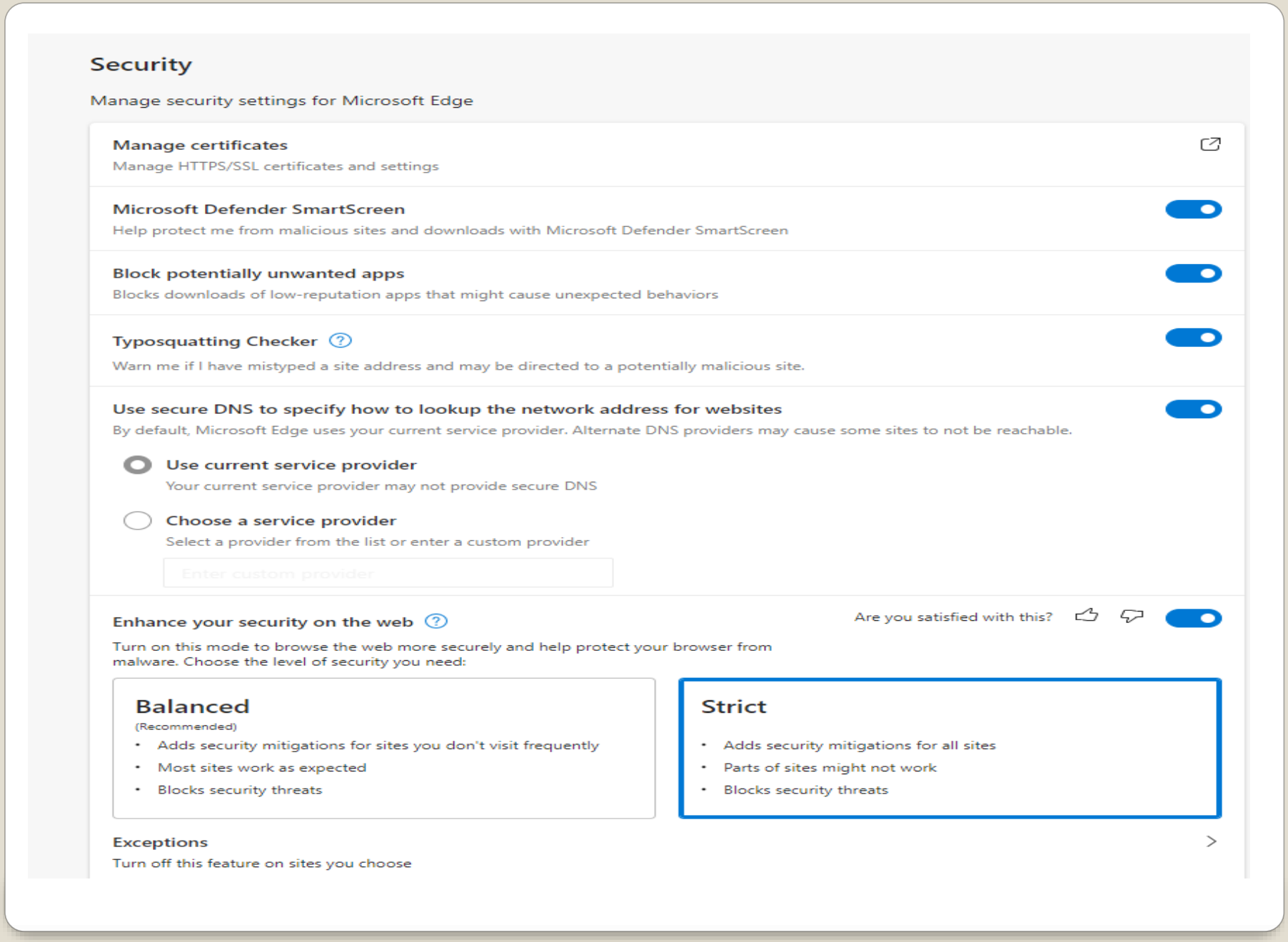
Get your favorites, passwords, and other browser data on all your devices.

- Buy now, pay later
- Quadpay

Microsoft Edge with Zip

- V96.0.1054.29 or higher
- Edge://settings/privacy

Edge “Super Duper Secure Mode”


Security
Manage security settings for Microsoft Edge
Manage certificates
Manage HTTPS/SSL certificates and settings
Microsoft Defender SmartScreen
Help protect me from malicious sites and downloads with Microsoft Defender SmartScreen
Block potentially unwanted apps
Blocks downloads of low-reputation apps that might cause unexpected behaviors
Typosquatting Checker
Warn me if I have mistyped a site address and may be directed to a potentially malicious site.
Use secure DNS to specify how to lookup the network address for websites
By default, Microsoft Edge uses your current service provider. Alternate DNS providers may cause some sites to not be reachable.
Use current service provider
Your current service provider may not provide secure DNS
Choose a service provider
Select a provider from the list or enter a custom provider
Enter custom provider
Enhance your security on the web
Are you satisfied with this?
Turn on this mode to browse the web more securely and help protect your browser from malware. Choose the level of security you need:
Balanced
(Recommended)
Adds security mitigations for sites you don't visit frequently
Most sites work as expected
Blocks security threats
Strict
Adds security mitigations for all sites
Parts of sites might not work
Blocks security threats
Exceptions
Turn off this feature on sites you choose

Edge "Super Duper Secure Mode"

- Remove Just-In-Time compilation
- Enable Intel Control-flow Enforcement Technology
- Balanced – learn mode
- Strict – No
- Exceptions
- Android & macOS to follow
- As will Arbitrary Code Guard

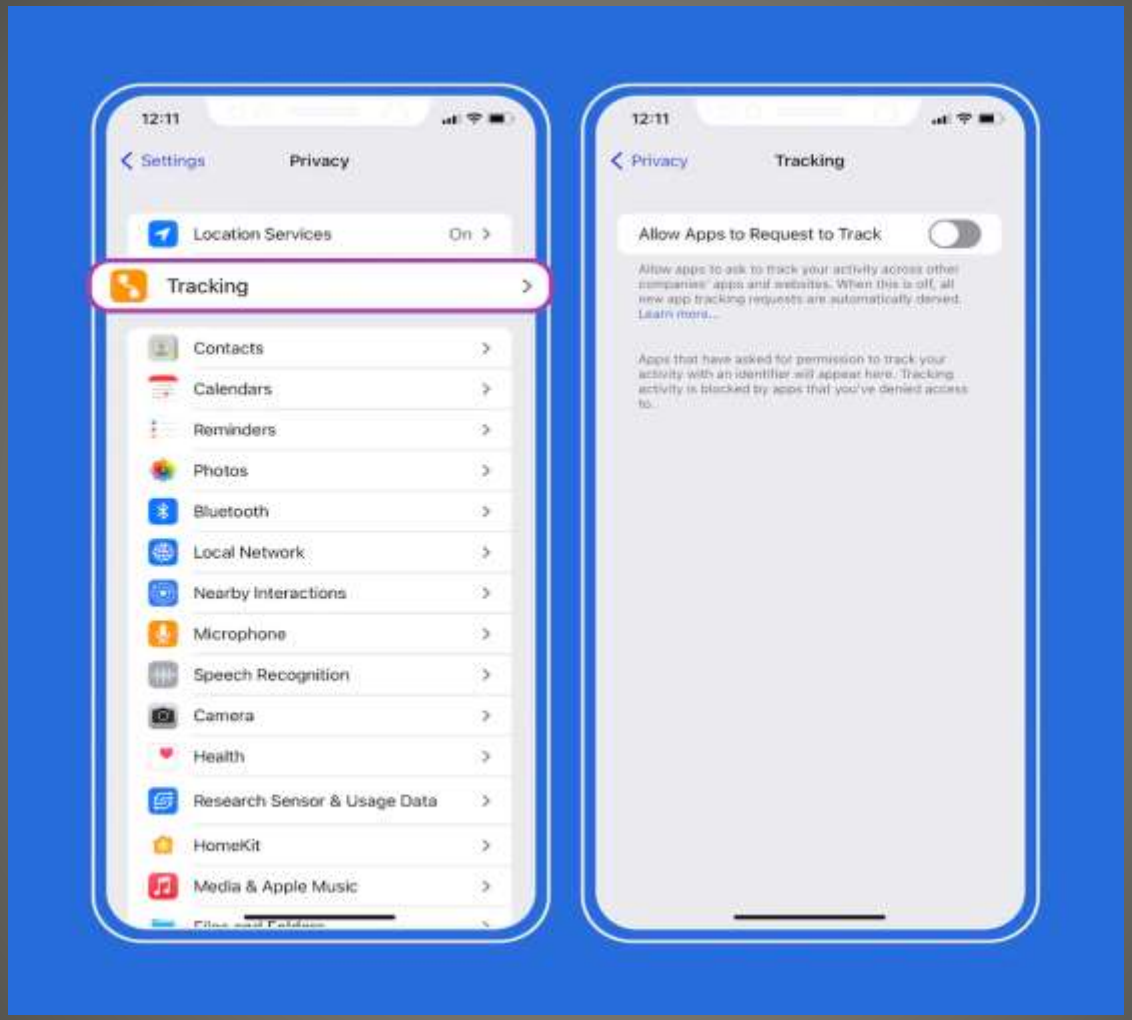
Current Issues

- IKEA reply-chain phishing attack
- MediaTek chips vulnerability

  low level – thus ALL apps using microphone
- RATDispenser

  OrderInformation.txt.js

  Clicking on links in eMail danger



iOS privacy Disable Tracking

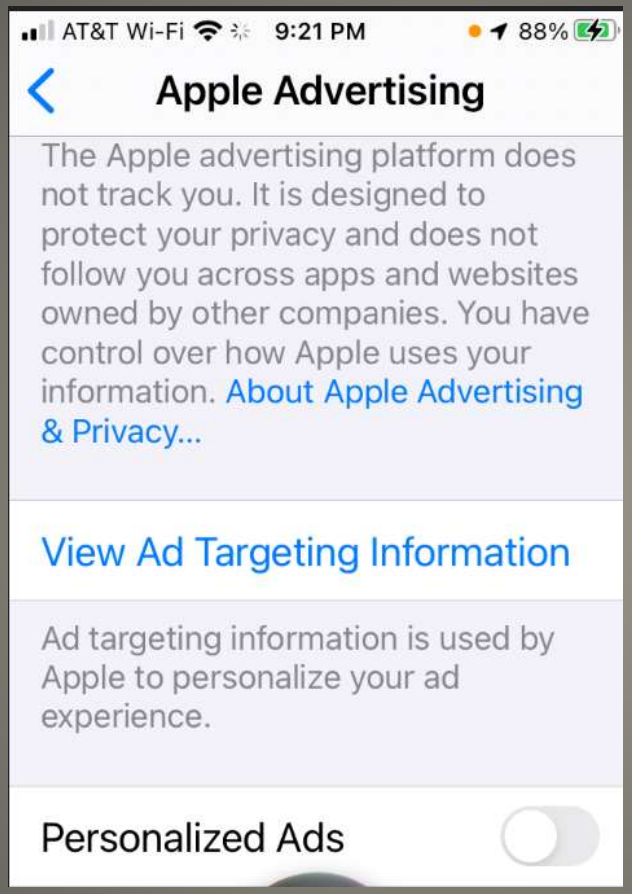
- Settings -> Privacy -> Record App Activity scroll down

iOS Privacy record App Activity

- Pick & Choose

Never
Ask
While Using
Always

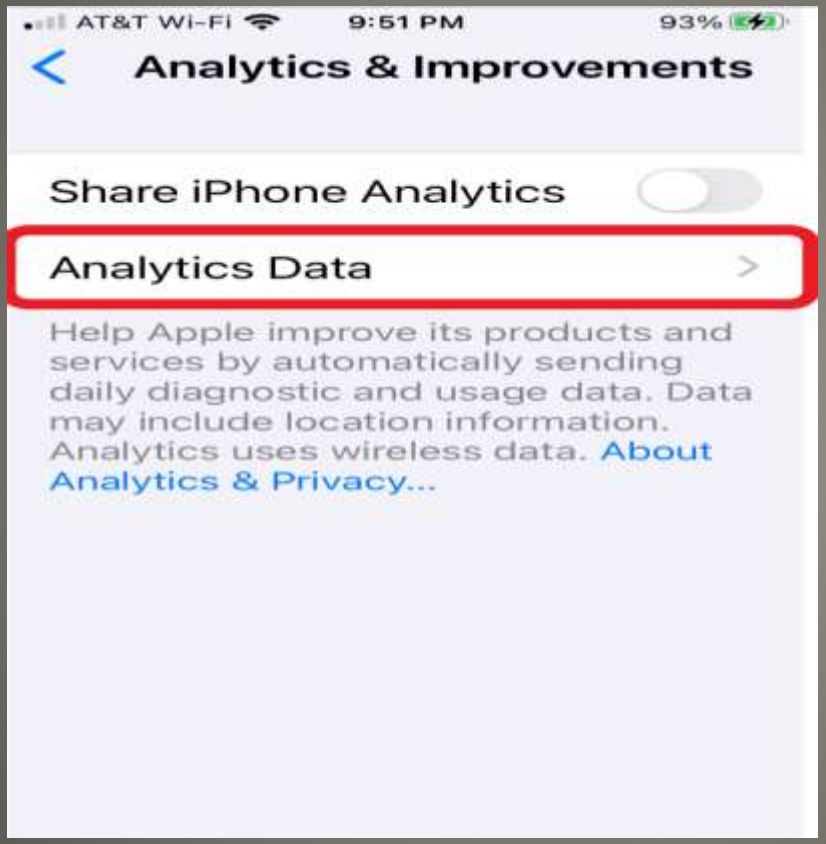
iOS Privacy Location Services



iOS Privacy Apple Advertising

iOS Privacy Analytics & Improvements

- Shared with developers

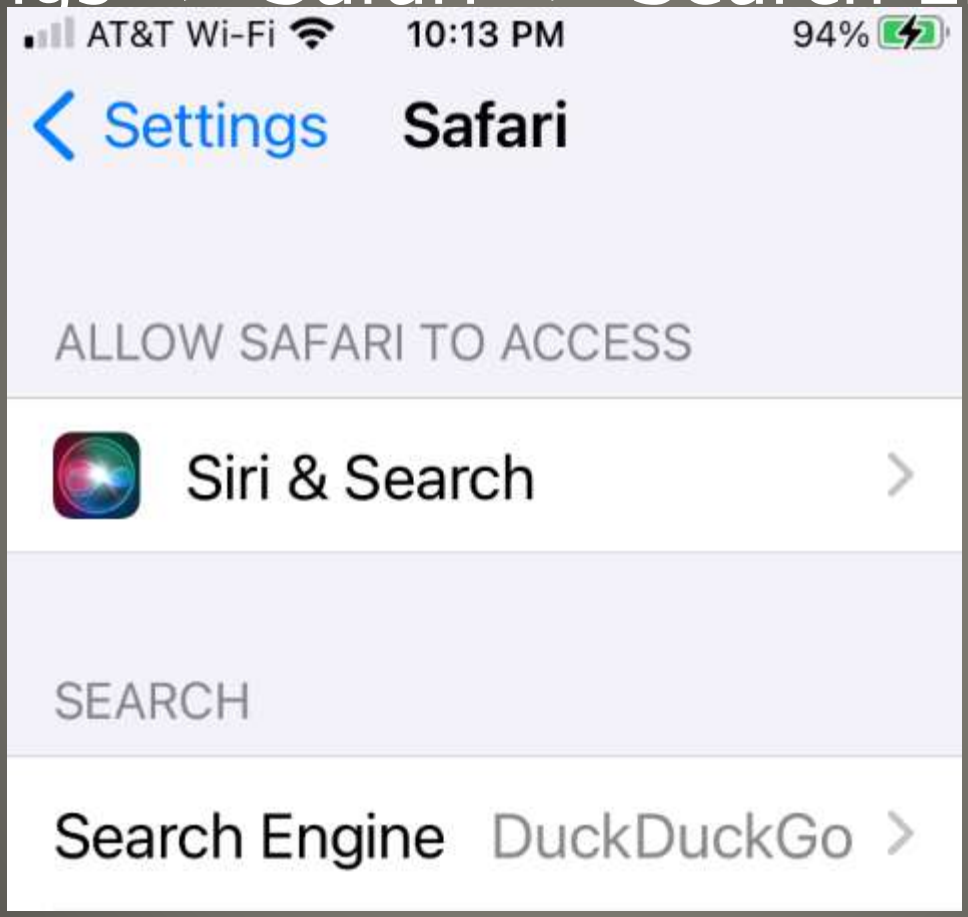


Analytics Data

- A LOT of data
- Removal Short scrub
- Removal iTunes sync
- Major version update
- Your method?

iOS Privacy Analytics Data

- Settings -> Safari -> Search Engine



iOS Privacy Safari

iOS Privacy Safari

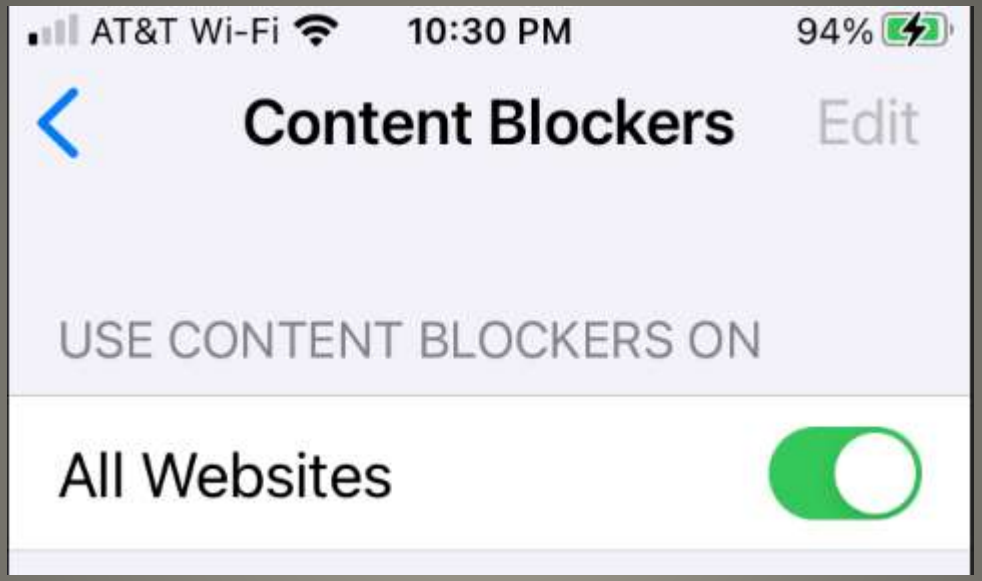
- Prevent Cross-Site Tracking
- Hide IP Address from Trackers
- Block All Cookies - CAUTION
- Fraudulent Website Warning
- Privacy Preserving Ad Measurement

iOS Privacy Safari Privacy & Security

iOS Privacy Safari Autofill

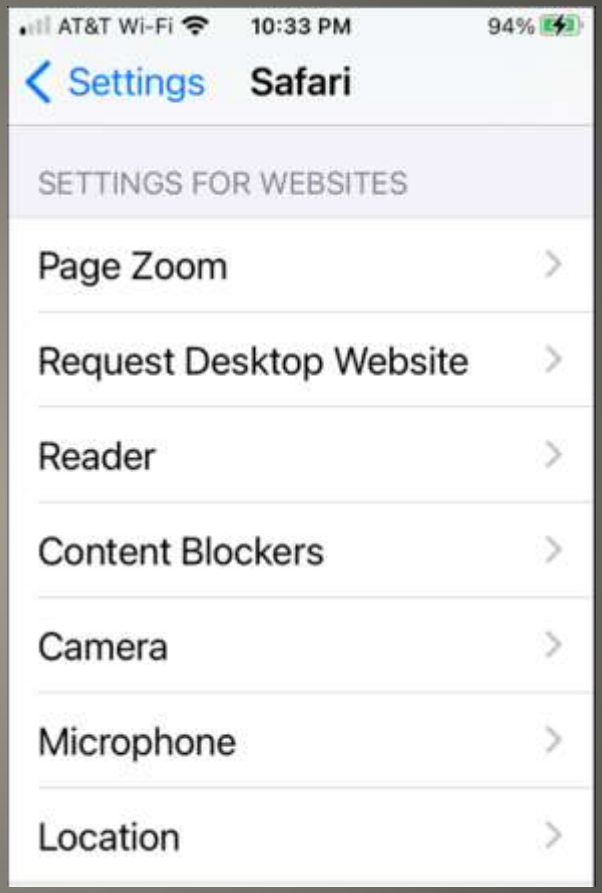
- Safari extensions Apple App Store

iOS Privacy Safari Extensions



iOS Privacy Content Blockers

- Camera – Ask
- Microphone – Ask
- Location – Ask



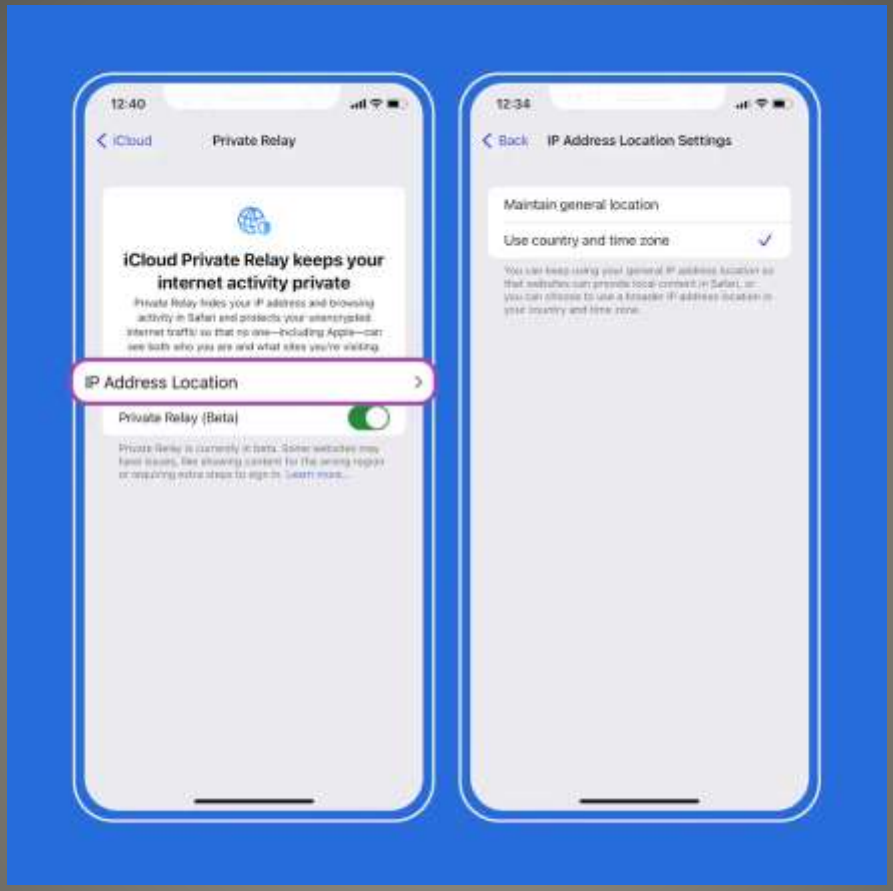
iOS Privacy Safari

- Search History ONLY

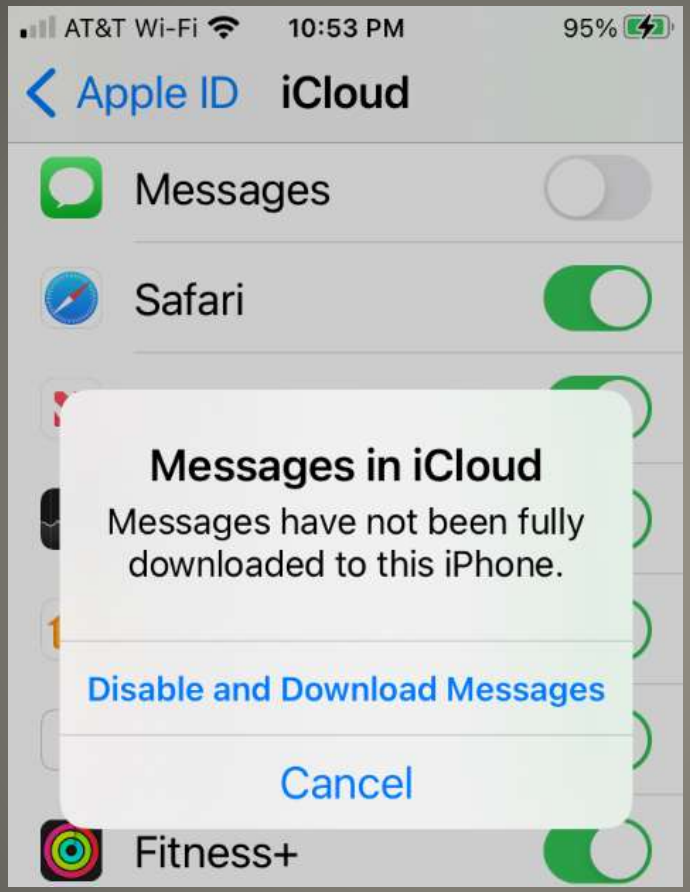
iOS Privacy Safari Private Browsing Mode

iOS Privacy Mail Privacy Protections

iOS Privacy Siri



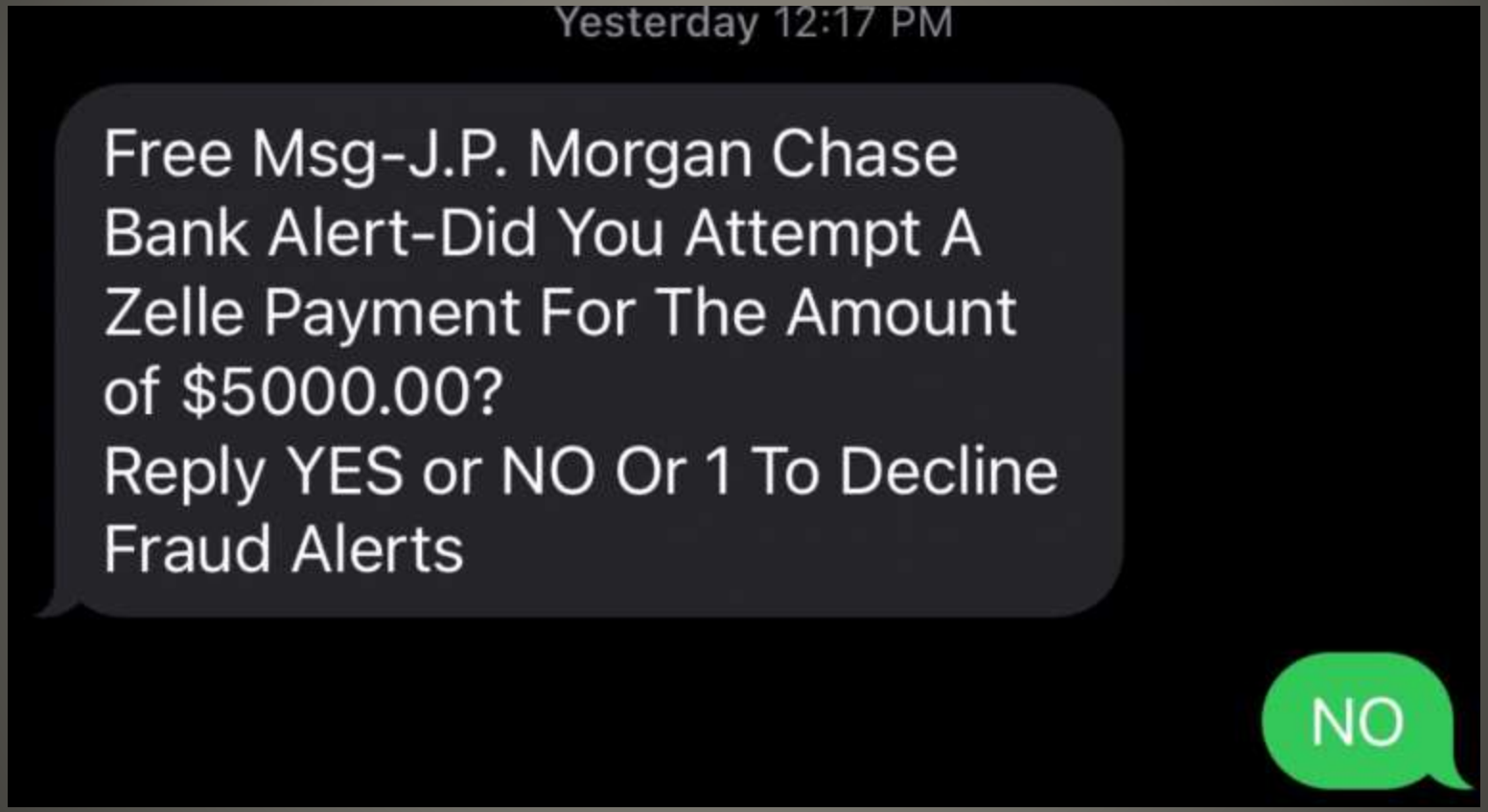
iOS Privacy iCloud Private Relay



iOS Privacy iMessage Backups

- End-to-End encryption
- BUT Subpoena

- Remember this from last presentation?



Zelle Fraud

Zelle Fraud

- Financial institutions offer self-serving options
- Regulation E protections
- If victim:

  Contact Consumer Financial Protection Bureau

  Subject: Docket No. CFPB-2021-0017

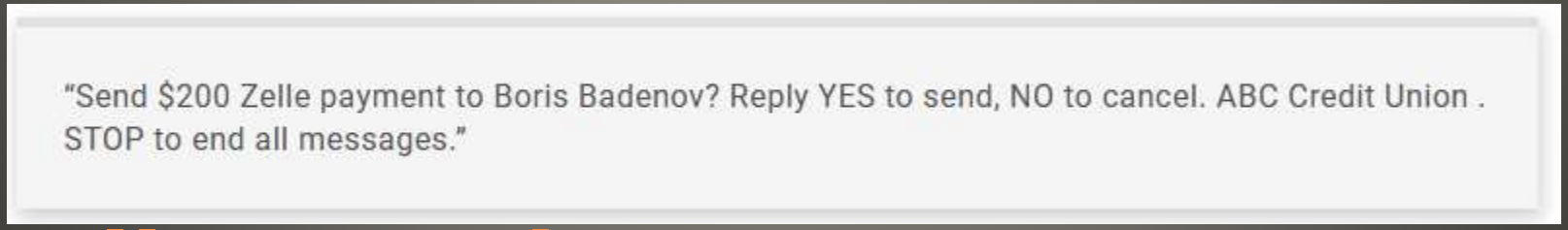
Hang up, Lookup, Call Back

Call back on different line Call back on looked up number

NOT redial

Zelle Fraud

- Few people know Zelle
- Fraudsters never learn victim's password
- Scheme script is well known/played
- "I need to verity you are not a scammer"
- "Your username?"
- "Read me the two-factor code"
- Code completes password reset
- Recent change to use out-of-band authentication with transaction details
- "That's just the system recovering the money"



- Hacked / Locked iOS device? Apple ID?
  BEFORE - choose trusted contact
  Contact with iOS 15 (like your iOS level)
  Contact must be over 13 years AND
  be using two-factor authentication

  Settings -> Apple ID -> Password & recovery
  Add recovery contact


Back
Account Recovery
iCloud secures your data by storing it in an encrypted format. If you forget your password or device passcode, iCloud Data Recovery Service can help you get your data back. For your privacy, there is some information the service can't recover. To make sure you can get all your data back, add someone you trust as a recovery contact or set up a recovery key. Learn More...
RECOVERY ASSISTANCE
iCloud Data Recovery Service
Add Recovery Contact
iCloud Data Recovery Service requires Apple to maintain access to your data to help you recover it. Recovery contacts can't access your data, but can help you get it back. Learn More...
Recovery Key
Off
Using a recovery key can help you restore all your data. When you create one, the only way to reset your password is by using another device already signed in with your Apple ID or by entering your recovery key.

Android Privacy

- An Android Advantage – Customizability
- Apps
- Settings -> Privacy -> Permissions Manager

  Location Uber probably Calculator Probably not

  App Audit Permissions Usage
- Unlock Form & Function

  Settings -> Security -> Screen Lock
- Notifications on Lock Screen

  Settings -> Apps & Notifications

  Sensitive Notifications Off

Android Privacy

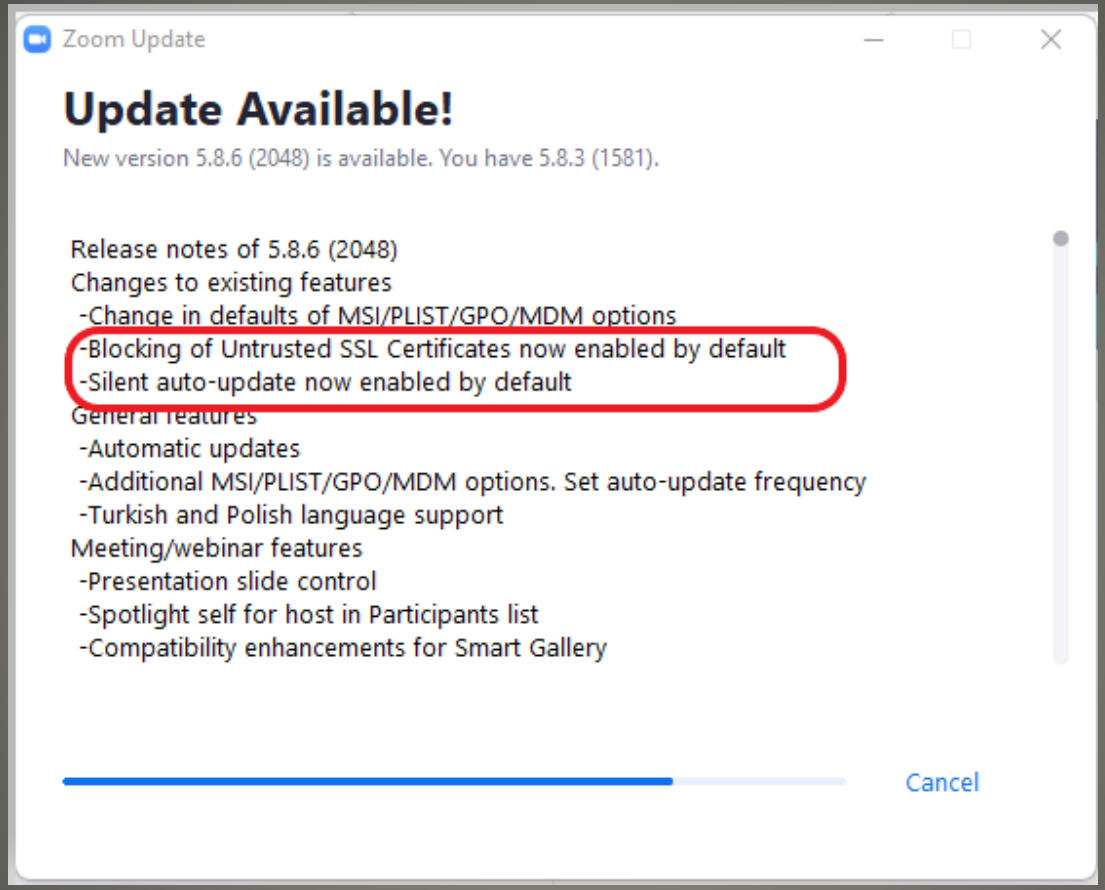
- Encrypted device

  Settings -> Security -> Advanced -> Encryption and Credentials

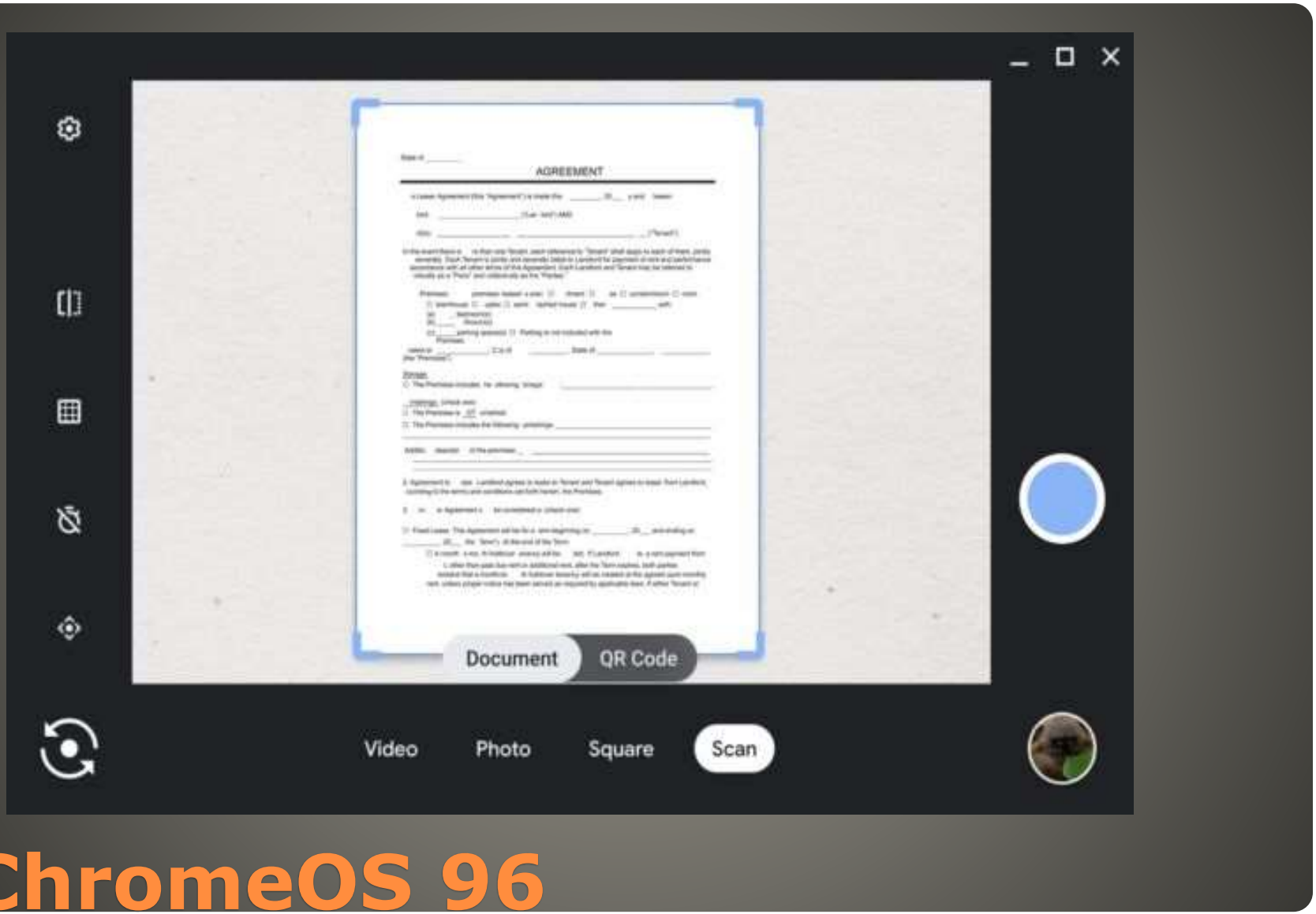
  Encrypt Phone - Can take some time to complete
- Browser Options Fit for Purpose
- Banking Trojan Risks

Current Issues

- Windows installer flaw
  Privilege escalation
- UK Ministry of Justice disabled poorly patched Wi-Fi access points
- Windows 11 Windows 10 21H2
  Microsoft Store many updates
- VoiceMail “electric service to be cut off”


Zoom Update
Update Available!
New version 5.8.6 (2048) is available. You have 5.8.3 (1581).
Release notes of 5.8.6 (2048)
Changes to existing features
-Change in defaults of MSI/PLIST/GPO/MDM options
-Blocking of Untrusted SSL Certificates now enabled by default
-Silent auto-update now enabled by default
General features
-Automatic updates
-Additional MSI/PLIST/GPO/MDM options. Set auto-update frequency
-Turkish and Polish language support
Meeting/webinar features
-Presentation slide control
-Spotlight self for host in Participants list
-Compatibility enhancements for Smart Gallery
Cancel

Zoom update



ChromeOS 96

- External camera Pan-Tilt-Zoom

ChromeOS 96

- 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