Sun City Computer Club

Cyber Security SIG

October 1, 2020

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

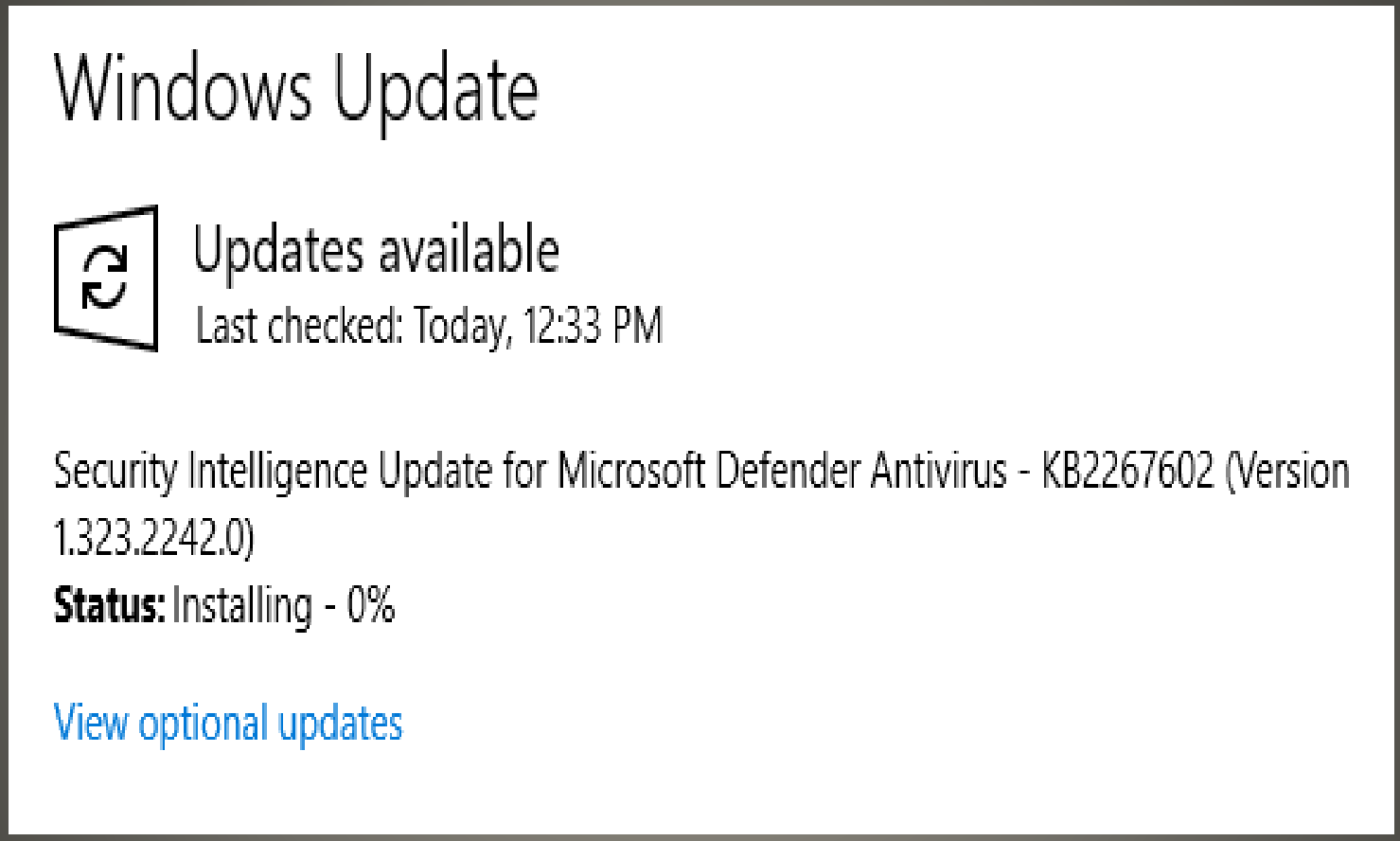
SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law

Current events

- Ransomware fatality? Fatalities?
- Mole – Location vision service
  Mole & agent 50¢ / minute
- Dept of the Interior wireless audit
  OPM Data breach
- Firefox on Android
- Firefox send & notes
- Homeland Security Emergency Directive
  20-04
  Microsoft “Zerologon” Domain Controller
  AND SAMBA
- Bing search records unprotected

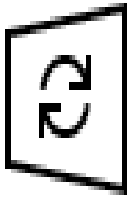
Current Events

- US CERT warns Federal agency compromise – zerologin? Pulse VPN?
- Ring doorbell drone inside home
- Cyberbackgroundchecks.com
- ChromeOS update, 100% CPU HCF 85.0.4183.108
- Microsoft 365 et al outage 9/28



Windows Optional Updates

Windows Update



Updates available

Last checked: Today, 12:33 PM

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.323.2242.0)

Status: Installing - 0%

View optional updates

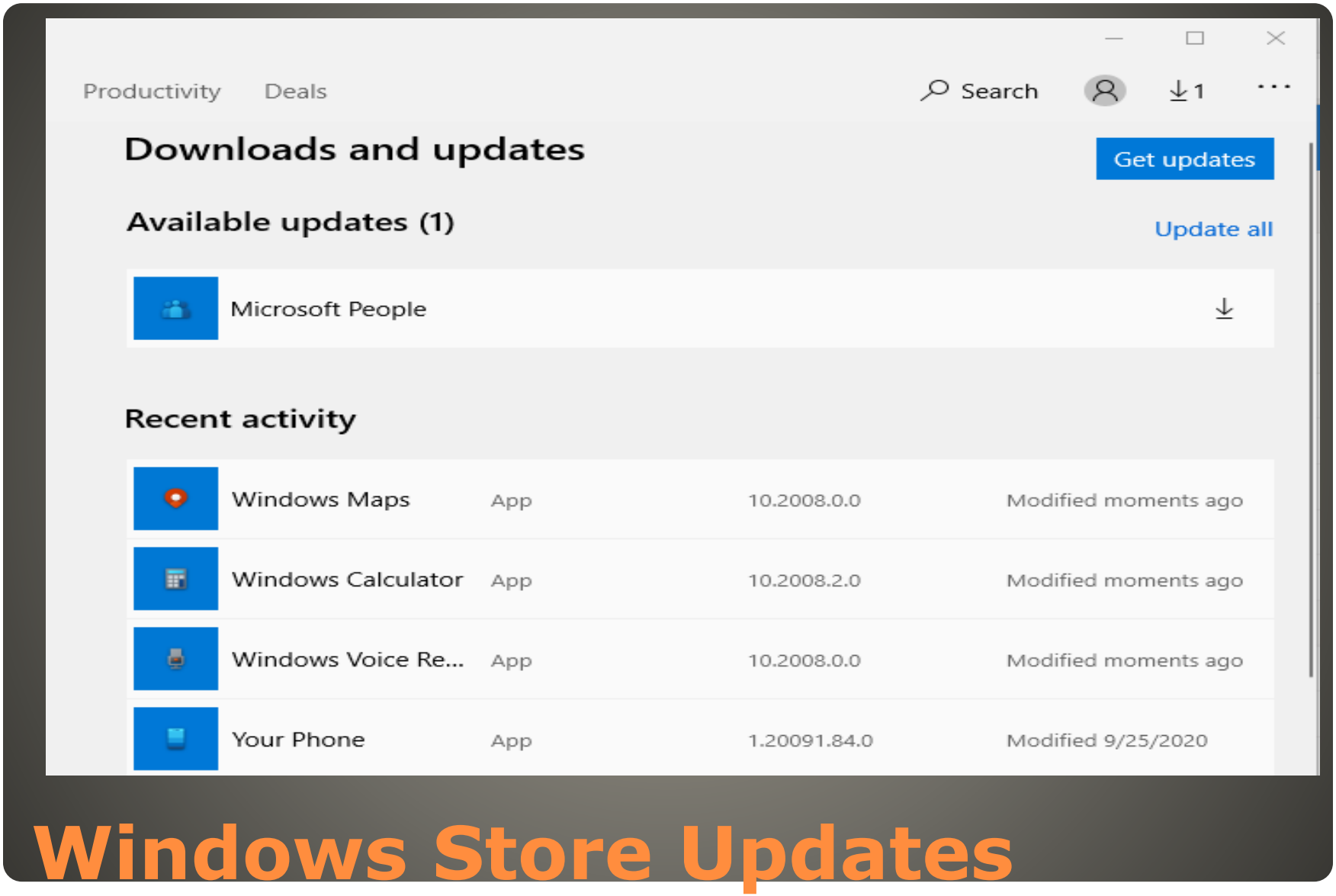
Optional updates

Choose the updates you want and then select Download and install.

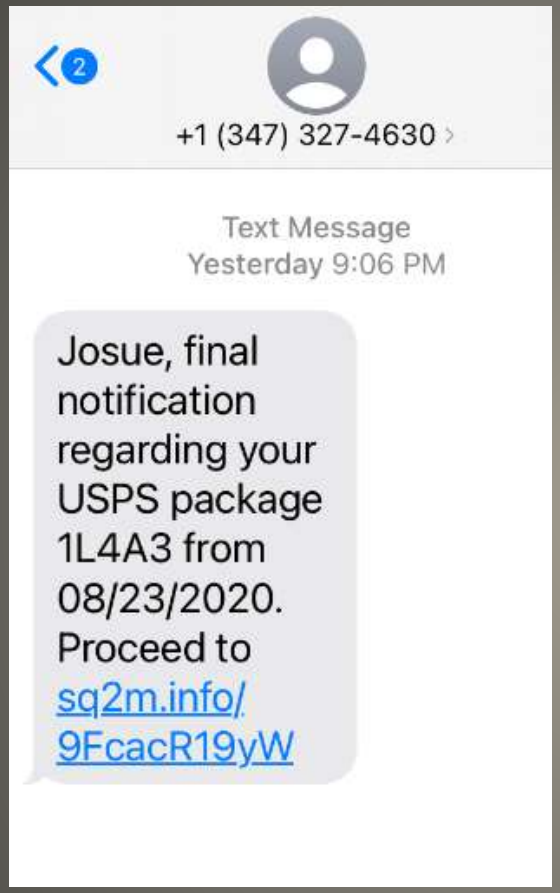
Driver updates

If you have a specific problem, one of these drivers might help. Otherwise, automatic updates will keep your drivers up to date.

- [ ] Realtek - Net - 6/27/2017 12:00:00 AM - 10.19.627.2017
- [ ] Realtek - LAN - Realtek USB FE Family Controller
- [ ] INTEL - System - 7/18/1968 12:00:00 AM - 10.1.1.45
- [ ] INTEL - System - 7/18/1968 12:00:00 AM - 10.1.1.45
- [ ] INTEL - System - 7/18/1968 12:00:00 AM - 10.1.1.45

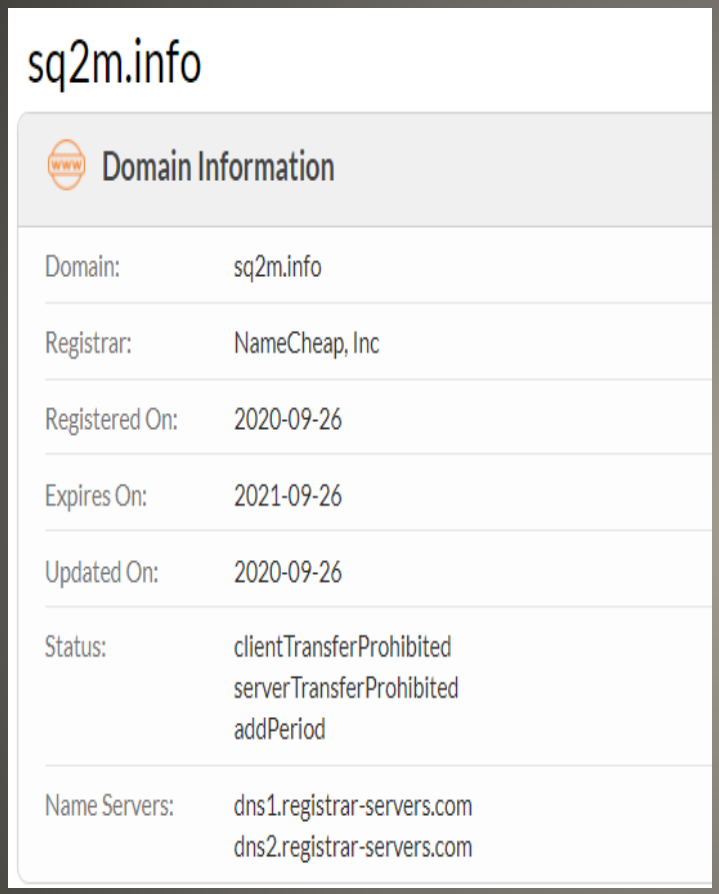


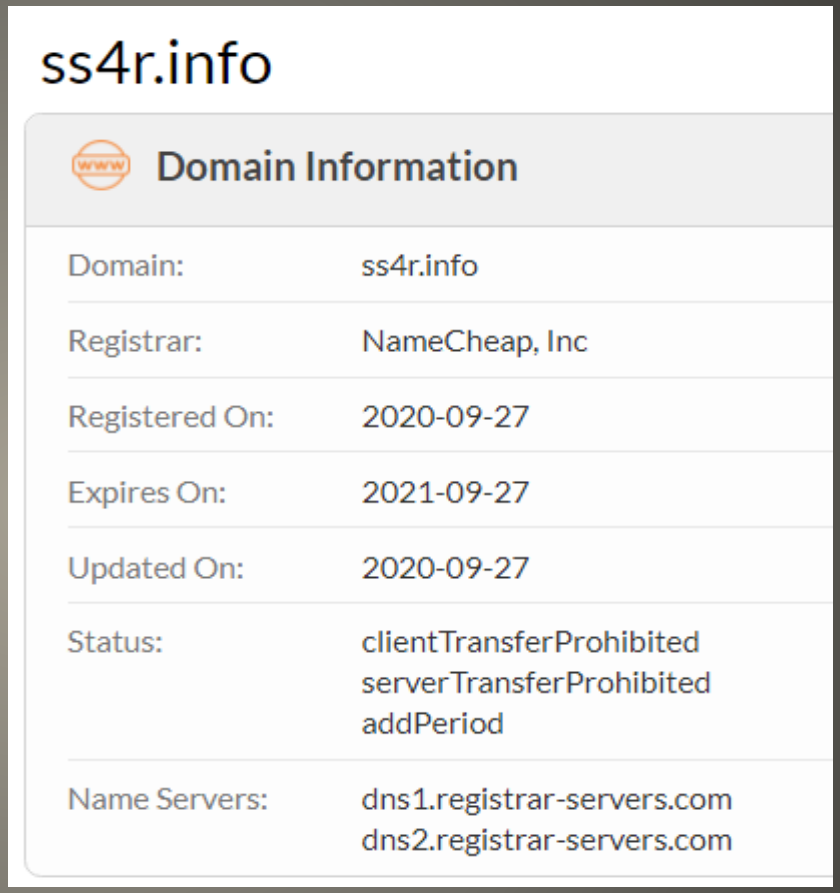
Windows Store Updates


2
+1 (347) 327-4630
Text Message
Yesterday 9:06 PM
Josue, final notification regarding your USPS package 1L4A3 from 08/23/2020. Proceed to sq2m.info/9FcacR19yW

1
+1 (216) 327-0441
Text Message
Today 10:01 AM
Sanieki, important notification regarding the USPS package 1D86R2 from 06/13/2020. Click: ss4r.info/V2vQxLqzu

scams


sq2m.info
Domain Information
Domain: sq2m.info
Registrar: NameCheap, Inc
Registered On: 2020-09-26
Expires On: 2021-09-26
Updated On: 2020-09-26
Status: clientTransferProhibited
serverTransferProhibited
addPeriod
Name Servers: dns1.registrar-servers.com
dns2.registrar-servers.com


ss4r.info
Domain Information
Domain: ss4r.info
Registrar: NameCheap, Inc
Registered On: 2020-09-27
Expires On: 2021-09-27
Updated On: 2020-09-27
Status: clientTransferProhibited
serverTransferProhibited
addPeriod
Name Servers: dns1.registrar-servers.com
dns2.registrar-servers.com

whois

Coffee Maker

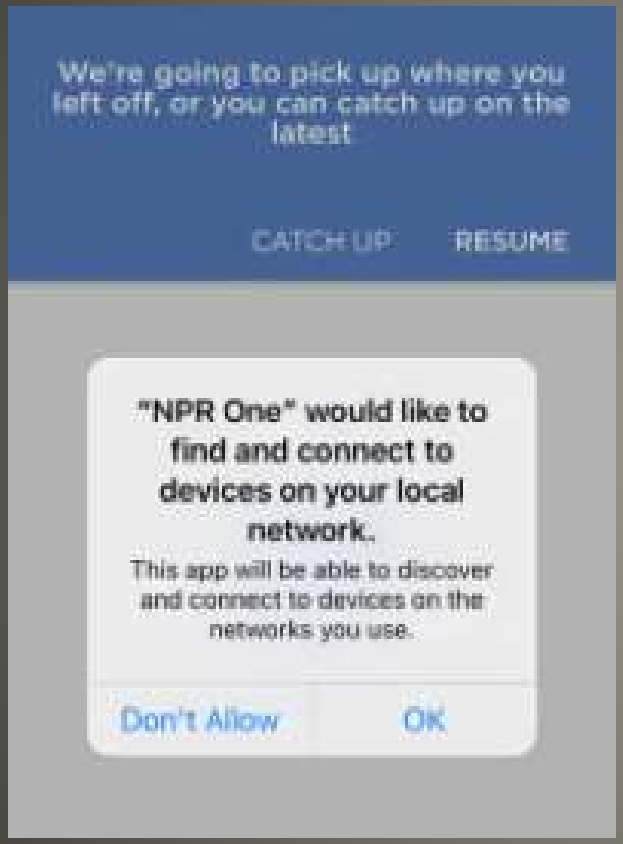
- Turn on burner, dispense water, spin grinder, display any message
- If so, how so?
- Out of the box, device acts as WAP
- Smartphone app to configure device
- Connect to home Wi-Fi
- NO AUTHENTICATION
- Update firmware via smartphone
- NO CODE SIGNING
- Reverse engineer firmware

smarter
CAUTION!
Please read instructions before removing the colour panels.

Android 11

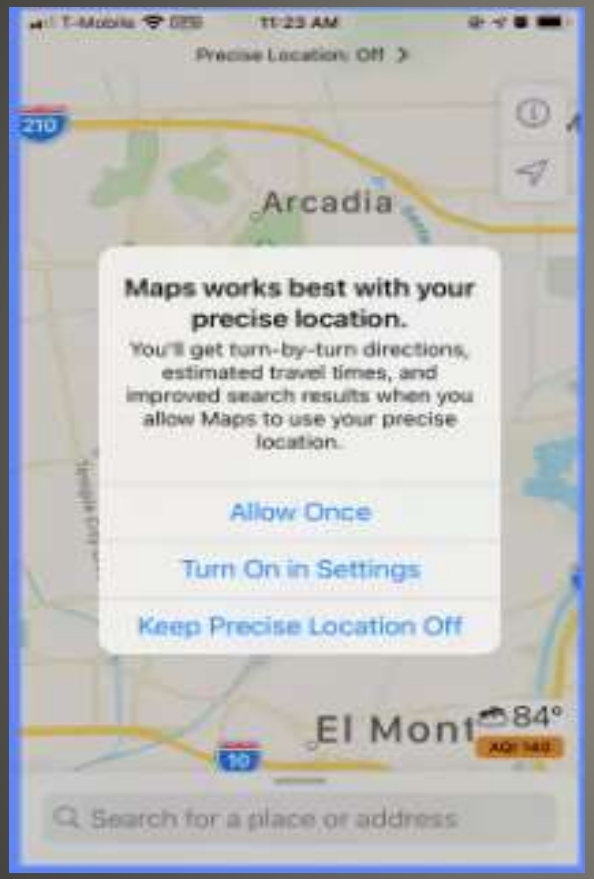
- One time permissions
- Revoke permissions for long unused apps
- (App updates) Play Store > My Apps & Games
- Incremental Updates
- Location awareness
- Silo storage
- Encryption after over-the-air update
  Before login
- App developers
- Screen recorder

- Local Area Network permission



iOS 14

- Precise Location

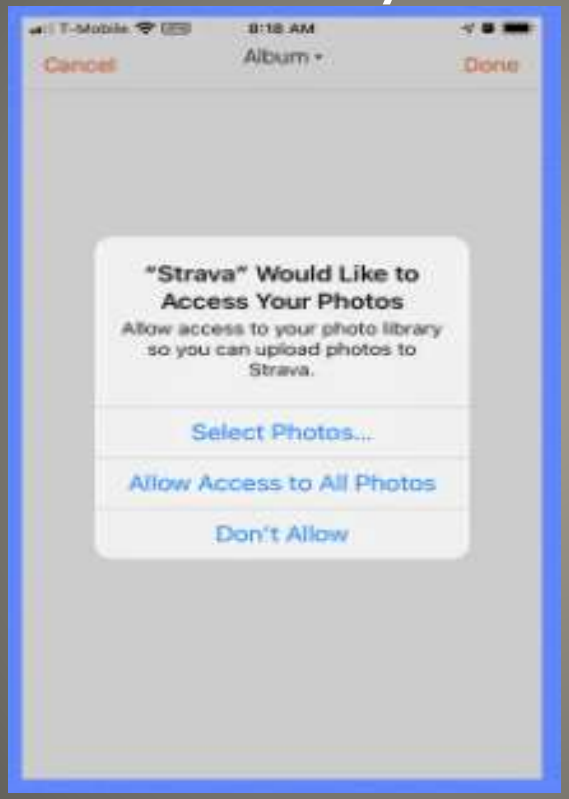


iOS 14

- Private Address
- MAC randomization Semi-randomization
- MAC filtering

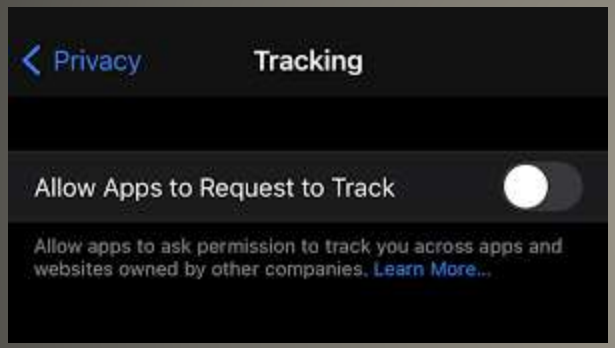
iOS 14

- Limited photo library access
- Settings > Privacy > Photos



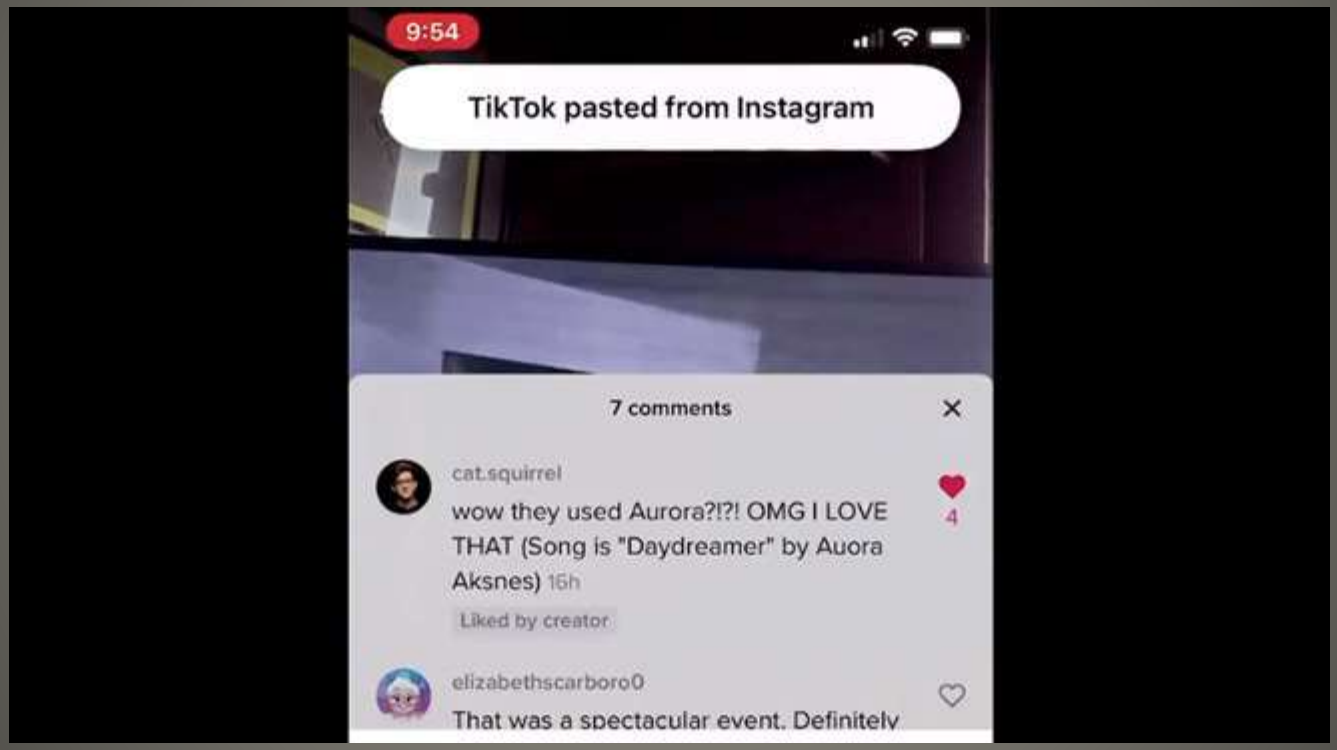
iOS 14

- Track across apps & websites
- Settings > Privacy > Tracking



iOS 14

- Clipboard monitoring
- TikTok, Starbucks, etc.



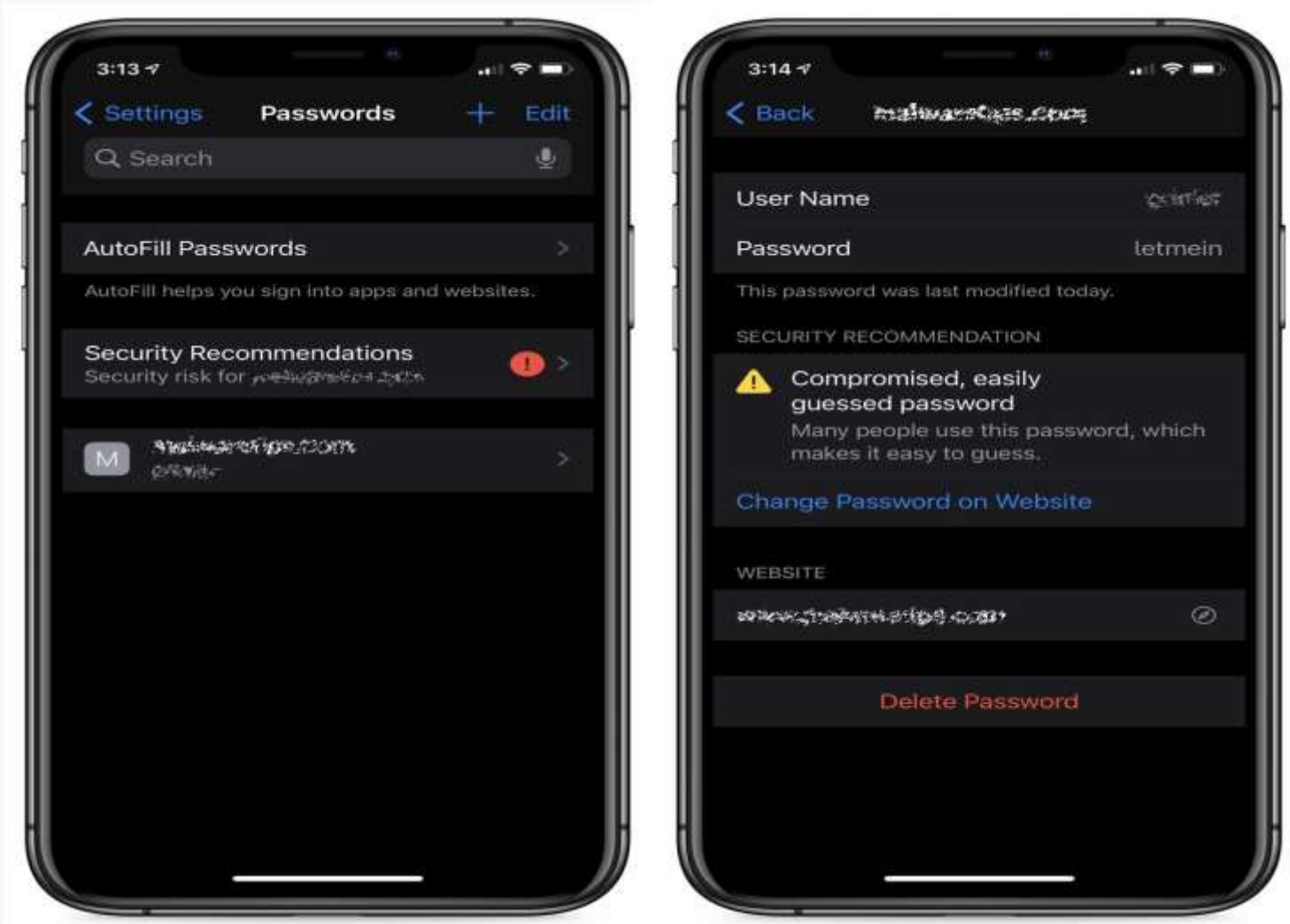
iOS 14

- Contacts autofill
- Settings > Contacts > Siri & Search

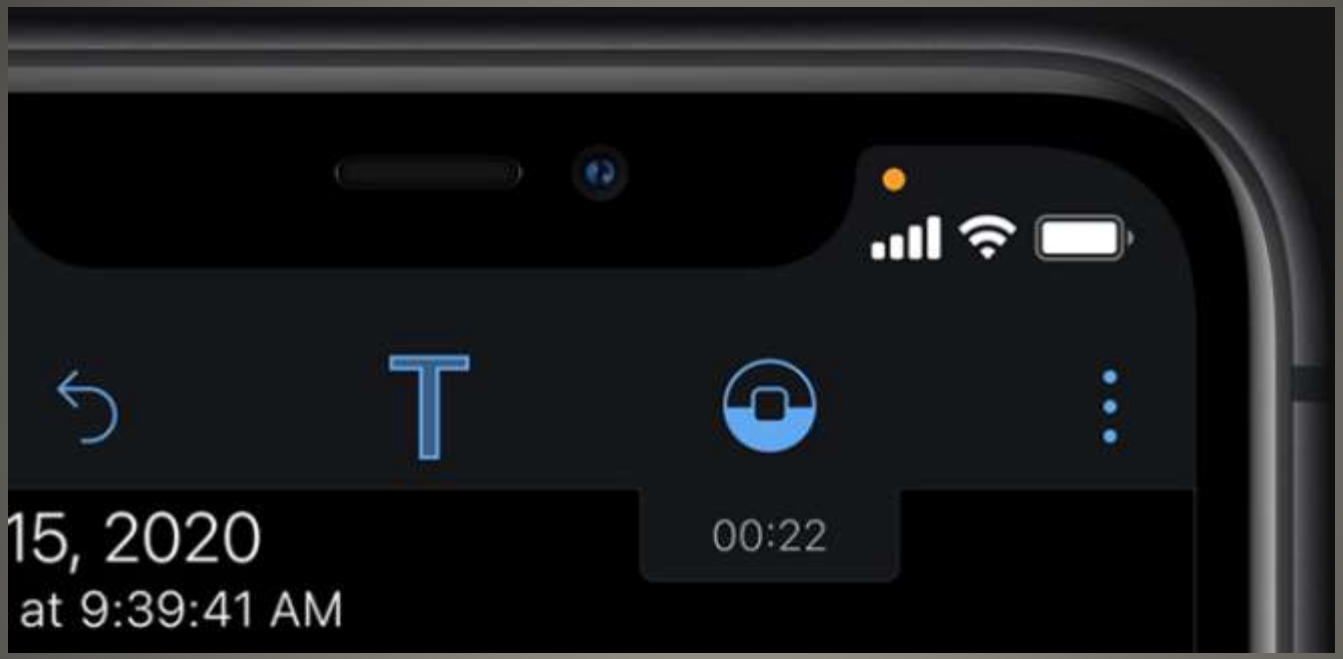
iOS 14

iOS 14

- Developers *self-report* in App Store
- Ability to change default browser
- Password monitoring & Alerts


3:13
Settings
Passwords
Edit
Search
AutoFill Passwords
AutoFill helps you sign into apps and websites.
Security Recommendations
Security risk for
M
3:14
Back
User Name
Password
letmein
This password was last modified today.
SECURITY RECOMMENDATION
Compromised, easily guessed password
Many people use this password, which makes it easy to guess.
Change Password on Website
WEBSITE
Delete Password

- Camera & Microphone indicators



iOS 14

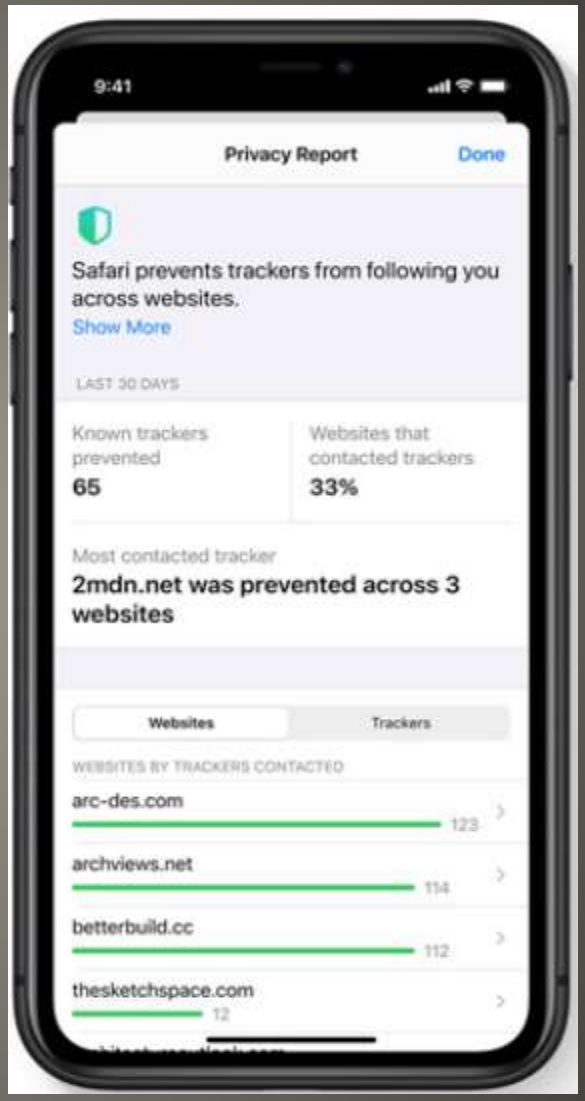
- Camera & Microphone Indicators
- Increasing use of zoom and like

iOS 14

- Red background app microphone
- Orange App microphone
- Green Camera

iOS 14 indicators

- Fastest ??
- Password alerts



iOS 14 Safari 14

iMessage EXIF data

- iDevices EXIF data
- EXchangable Image Data Format
- Date/time, location, camera settings, thumbnail, copyright, etc.
- Settings > Privacy > Location Services > Camera
- Helpful <-> Harmful
- Use iMessage directly
- Screenshot of Photo
- Audio via camera as well

Photos with EXIF data

- Native camera, Camera+, and others
- Facebook no, Photobucket yes
- One non-Apple device data stripped

- 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

QUESTIONS?