Sun City Computer Club

Cyber Security SIG

July 21, 2022

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??

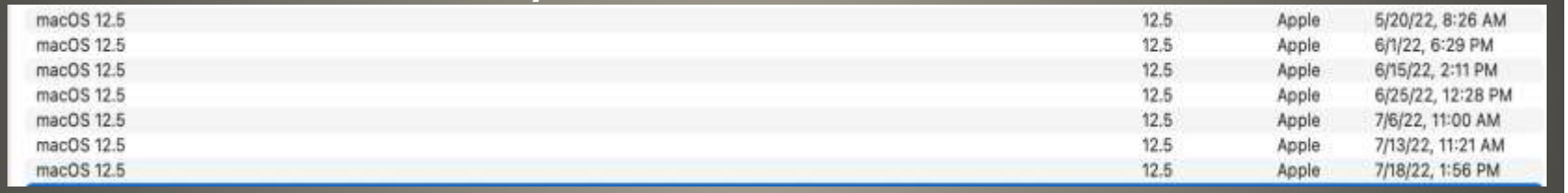
Presenter???

Updates

- macOS Monterey

macOS 11.0	11.0	Apple	10/29/20, 3:33 AM
macOS 11.4	11.4	Apple	5/24/21, 2:44 PM
macOS 11.5	11.5	Apple	7/22/21, 9:39 AM
macOS 11.5.1	11.5.1	Apple	7/26/21, 2:22 PM
macOS 11.5.2	11.5.2	Apple	8/11/21, 6:51 PM
macOS 11.6	11.6	Apple	9/14/21, 9:40 AM
macOS 12.0.1	12.0.1	Apple	10/25/21, 1:32 PM
macOS 12.1	12.1	Apple	12/13/21, 4:05 PM
macOS 12.2	12.2	Apple	1/26/22, 1:08 PM
macOS 12.2.1	12.2.1	Apple	2/11/22, 1:15 AM
macOS 12.3	12.3	Apple	3/14/22, 4:37 PM
macOS 12.3.1	12.3.1	Apple	4/1/22, 9:46 AM
macOS 12.4	12.4	Apple	5/16/22, 3:15 PM
macOS 12.5	12.5	Apple	7/20/22, 7:19 PM

- macOS Ventura Beta 13.0 (22A52951)
- macOS Monterey Beta DEV



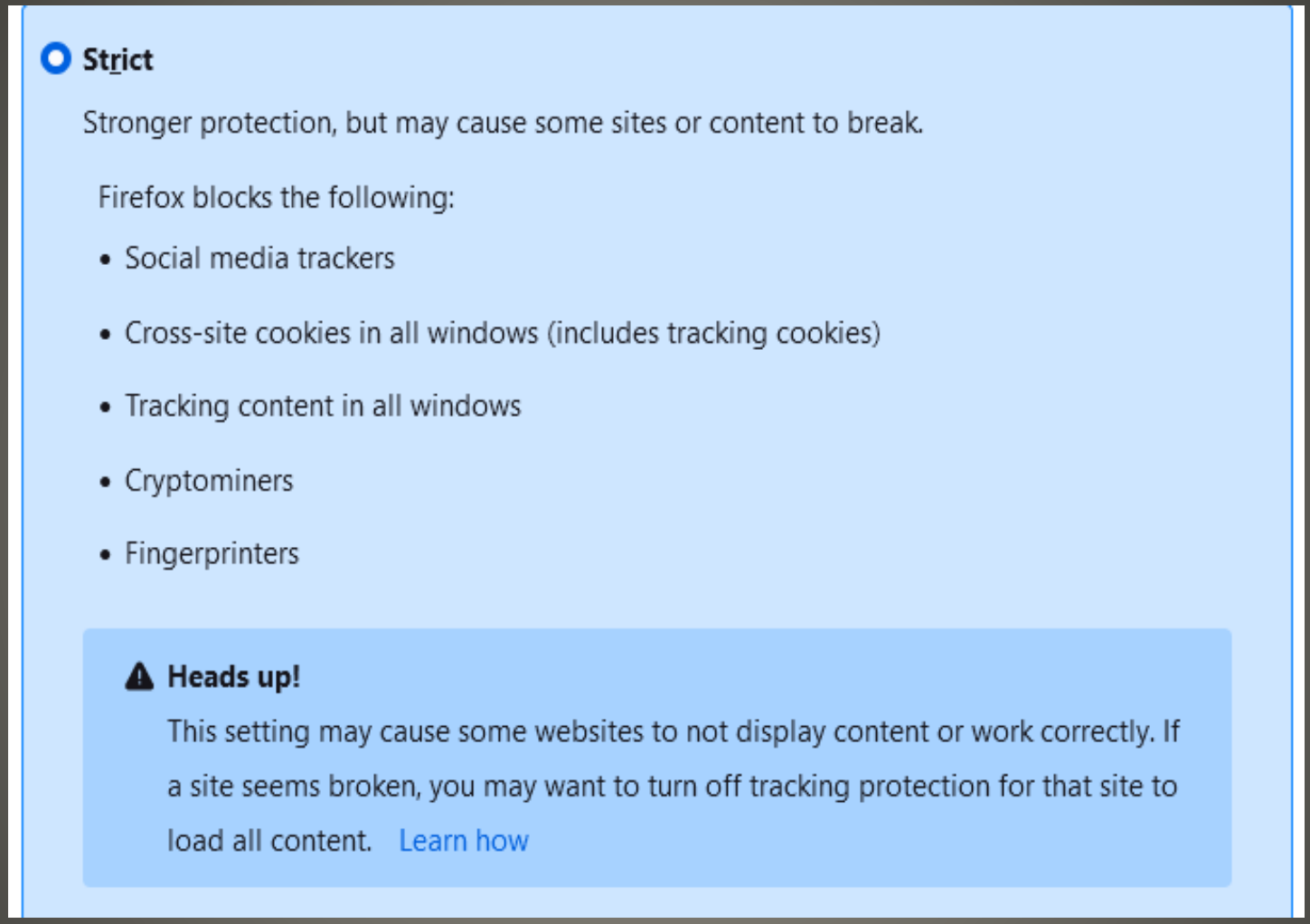
macOS 12.5	12.5	Apple	5/20/22, 8:26 AM
macOS 12.5	12.5	Apple	6/1/22, 6:29 PM
macOS 12.5	12.5	Apple	6/15/22, 2:11 PM
macOS 12.5	12.5	Apple	6/25/22, 12:28 PM
macOS 12.5	12.5	Apple	7/6/22, 11:00 AM
macOS 12.5	12.5	Apple	7/13/22, 11:21 AM
macOS 12.5	12.5	Apple	7/18/22, 1:56 PM

- macOS Big Sur 11.6.8
- macOS Catalina 10.17.7
- iOS & iPadOS 15.6
- watchOS 9.7
- tvOS 15.6

Updates

- ChromeOS 103.0.5060.132
- Windows 10 21H2 (19044.1826)
- Windows 11 21H2 (22000.778)
- Windows 11 Dev 22H2 (25163.1000)
- Windows 11 Rel 22H2 (22622.436)
- Edge 103.0.1264.62
- Chrome 103.0.5060.136
- Opera 89.0.4447.51
- Firefox 102.0.1
- Brave 1.41.100
- Vivaldi 5.3.2679.68

Remember these slides?



Firefox Query Parameter Stripping

Firefox Query Parameter Stripping

- https://www.engadget.com/example.html?fbclid=aa7-V4yb6Yfit_9_Pd

- Facebook and others
- Changes with user's interaction
- Other sites use the same technique

Olytics: oly_enc_id=, oly_anon_id=
Drip: __s=
Vero: vero_id=
HubSpot: _hsenc=Marketo: mkt_tok=
Facebook: fbclid=, mc_eid=

But for how long?

privacy.query_stripping.enabled.pbmode false

- Next?

Now Facebook encrypts URL

- Google blurs Supreme Court Justice's homes
- <Confirms these ARE those homes>

sigh

- 8kun[.]top
- TheDonald[.]win

- Report to new sole ISP provider
- Now moved

Outages during January 6 Hearings

- California to manufacture insulin
- Arizona law prohibit recording within 8 feet of law enforcement

  Misdemeanor & verbal warning
- Cruise losing control again

Current Issues

Current Issues

- China researchers claim
  Mind Reading AI measure party loyalty
- Musk *Neuralink*
- Experian
  Multiple users report account takeover
  New email address, new security questions, new PIN
  Also, new accounts created with stolen IDentities
  No MFA
  Some protections via browser cookies
- Iran provide Russia with hundreds of drones
- BMW Heated Seats $18/mo.
- California school districts data breaches
  700,000+ Posted OnLine
- Smart thermostats save or harm electrical grid?

Current Issues

- OpenSSL version 3.0.4 serious vulnerability
  OpenSSL version 3.0.5 fixed
- Yubico donated 30,000 Yubikeys to Ukraine
- Apple Lockdown mode $2M bounty

Rolling Pwn

- Honda keyless entry system vulnerability
- Play it forward - jam the first code
- Unlock & start - but not drive
- ReSynch vulnerability

- Tesla Bluetooth replay

Current Issues

- Ring provided video to law enforcement
  11 times (so far 2022) without
  warrant or consent
- MFA bypass via phishing Office 365 users
  Remember browser cookies – sensitive sites
- Lenovo laptops firmware release
  UEFI - check Lenovo site
- macOS app sandbox escape flaw
  Found and reported by Microsoft
  Fixed by Apple Catalina, Big Sur & Monterey
- Adobe patches Acrobat, Reader & Photoshop

Current Issues

- Chrome OS Flex
- 988 Suicide hotline 16-July-2022
  1-800-273-TALK
- Windows NFS vulnerability
  SYSTEM arbitrary code execution
- Former CIA employee convicted
  All counts WikiLeaks 2016 hung jury 2020
  Vault 7
- Congress asking FTC investigate
  "take enforcement actions"
  "problematic actors in consumer VPN industry"
  "deceptive advertising and data collection practices"
  Consumer Reports report

Current Issues

- Hubble 2GB solid state disk drive
- JWST 68GB solid state disk drive

- You?

- ClearView AI sued by Greece 20€
- Ransomware indexing stolen information
- App advertising launch DDoS attacks against Russia
  Actually identify and track Ukrainians
- Cloud servers in UK outages due to heat

Phone star codes

- Helpful <-> Harmful
- *69
  trace the last number to call your phone
  Phone number and Time
  Block
  Call back
- *57
  harassment
  Info passed to Law Enforcement
  Follow up with law enforcement
- Extra charges may apply

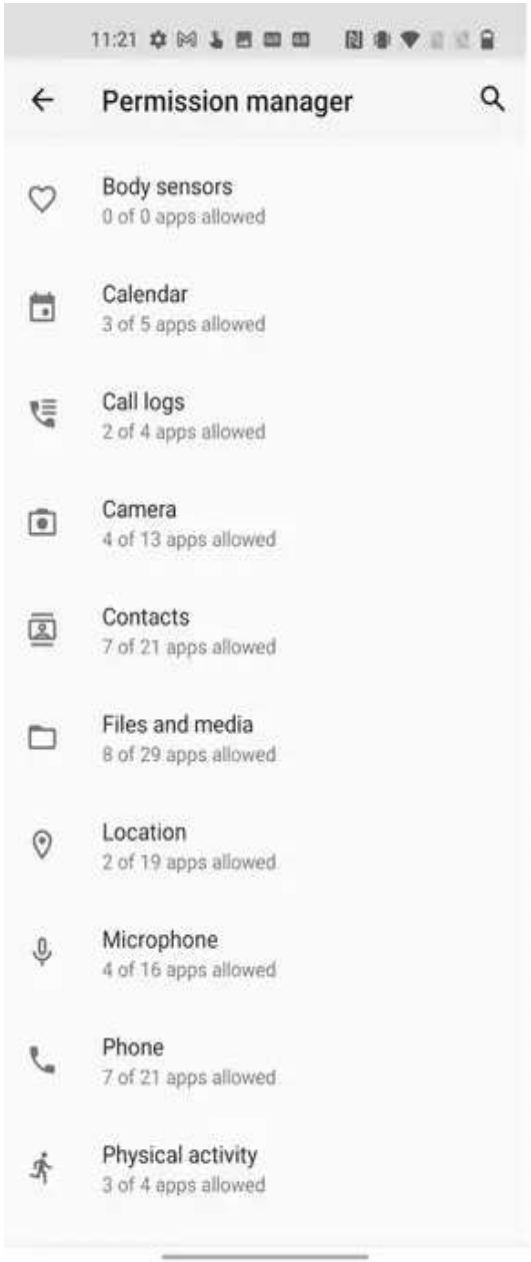
- Android 12 Privacy Dashboard
- Permission Manager

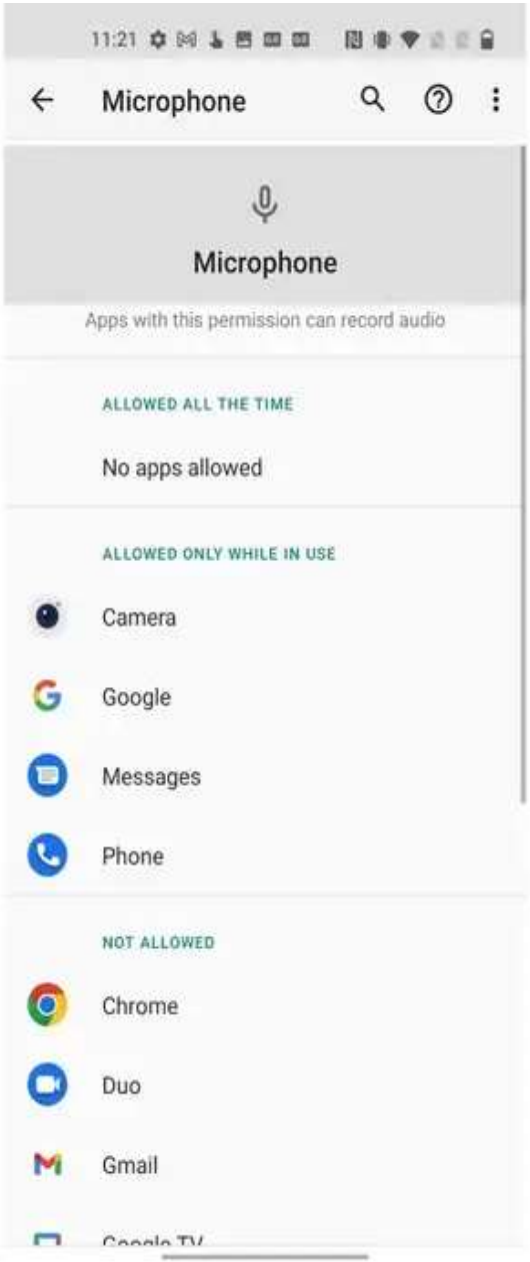
Android reputation shift

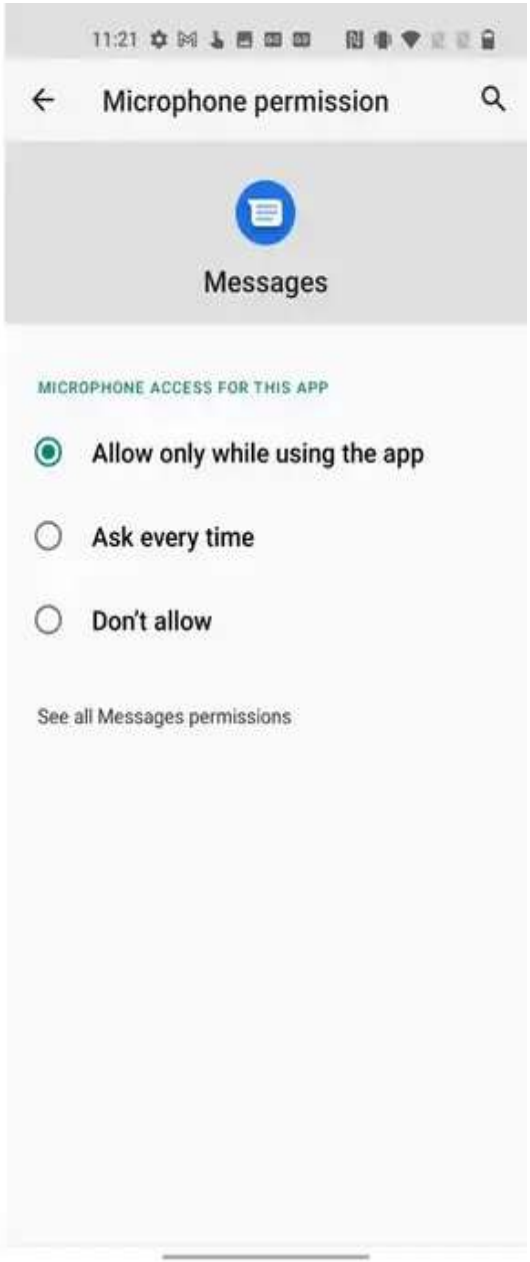
- User control

  call logs, camera(s), microphone, location, contacts, files, physical activity, …

Android Reputation Shift


11:21
Permission manager
Body sensors
0 of 0 apps allowed
Calendar
3 of 5 apps allowed
Call logs
2 of 4 apps allowed
Camera
4 of 13 apps allowed
Contacts
7 of 21 apps allowed
Files and media
8 of 29 apps allowed
Location
2 of 19 apps allowed
Microphone
4 of 16 apps allowed
Phone
7 of 21 apps allowed
Physical activity
3 of 4 apps allowed


11:21
Microphone
Microphone
Apps with this permission can record audio
ALLOWED ALL THE TIME
No apps allowed
ALLOWED ONLY WHILE IN USE
Camera
Google
Messages
Phone
NOT ALLOWED
Chrome
Duo
Gmail

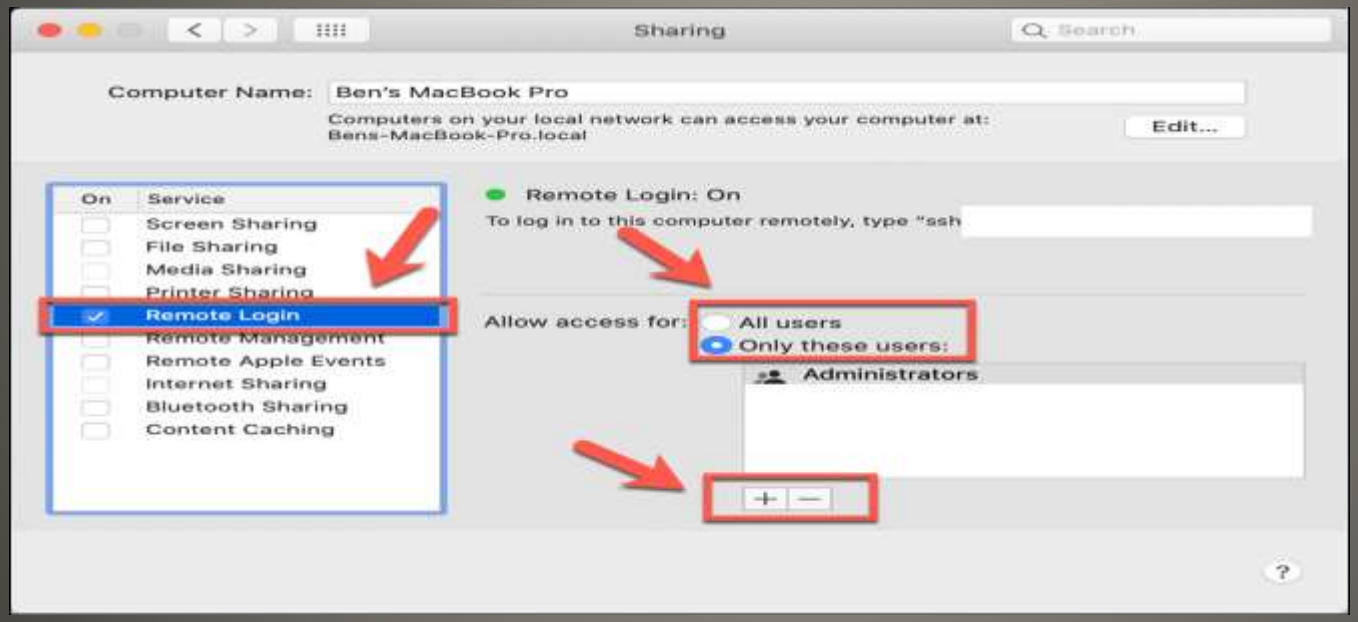

11:21
Microphone permission
Messages
MICROPHONE ACCESS FOR THIS APP
Allow only while using the app
Ask every time
Don't allow
See all Messages permissions

- Fine tune permissions
  - Share only while app is running
  - Temporary access
  - Approximate location

REVIEW APPS AND THEIR PERMISSIONS

Android Reputation Shift

- Disabled by default
- Enable when needed Disable when not
- SSH and SFTP



Enable SSH on Mac

- sudo systemsetup -setremotelogin on
- sudo systemsetup -setremotelogin off

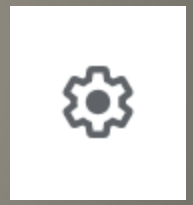
- sudo systemsetup -getremotelogin

Enable SSH on Mac

App control Google Drive

- Apps use Google Drive
- Helpful <-> Harmful
- WhatsApp Google Drive
  Yeahbut Your access Your charges
- Periodic audit
- Chrome drive.google.com
  Your Google account(s)
  Settings cog
  Settings > Manage Apps

  Disconnect from Drive



Current Issues

- Critical vulnerabilities in GPS tracker
- Pig butchering scams epidemic


IBM
IBM
Polaroid
Polaroid
CS
135 12

- 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