Sun City Computer Club

MUG MAC Users Group

April 24, 2024
3:00pm

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

- Wake Words

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

- SIG Leader replacement
- # Take over
- Inclusion Zoom & Recording
- Summers are Important Apple

- Apple Users Group
- # Leader(s)???
- iDevices in MUG   no one wants that

Presenter???

Computer Club Vimeo Library

- May 7, 2024 9am Central
- Live Stream   Apple.com   YouTube
- Apple Pencil
- Magic Keyboard
- New iPad Pro?
- New iPad Air?

let loose.

You're invited to watch a special Apple Event.
Tune in at apple.com.

May 7, 2024
7:00 a.m. PT

Apple "Let Loose" Event

- iOS 17.5
- iPadOS 17.5
- WatchOS 10.5

- Note: Beta tester Privacy Policy

Beta 3

- Updates for added features
- Updates for fixed bugs
- Updates for AI & AI improvements

Apple Store

- Upside Down Charging fix?
- Tilting
- Rotating

Magic Mouse

- Ability to update iDevices in their boxes
- iPadOS 18 with calculator App?
- Apple Pencil 3?

Current Issues

- Atomic Stealer
- Arc Browser Google sponsored link
- Use Control-Click bypass Gatekeeper
- Update System Settings
- Used Account password
- Now uses Keychain & Keychain data

- Meethub

- Control-click AVOID!!

Mac Info Stealer Apps

- GTA 6 Mac macOS stealer
  Right click - Open

1 STEP

RIGHT CLICK

2 STEP

CLICK 'OPEN'

A helper tool is needed to manage your games.
Origin is trying to install a new helper tool.

Enter your password to allow this.

User Name:

Password:

Cancel   Install Helper
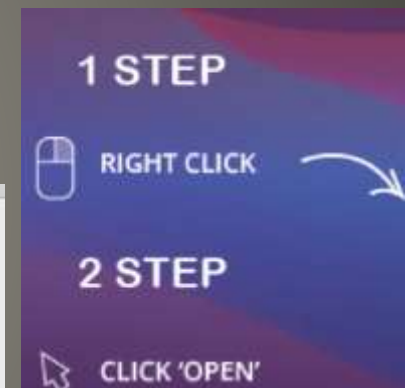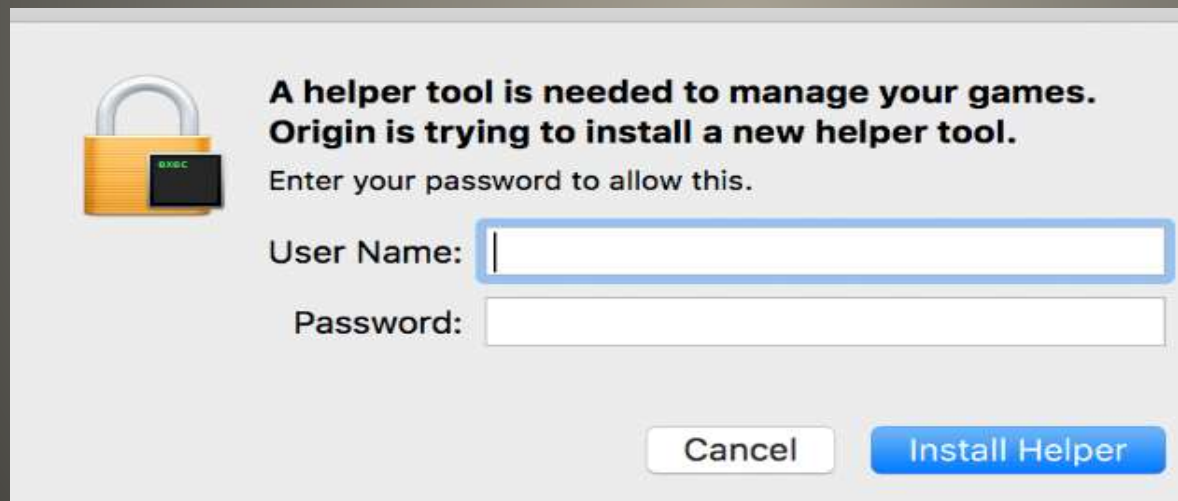
Current Issues

macOS Stealer Apps

iWork iPad Shortcuts

- **Pages**
  - On iPad, press and hold the Command key on a connected keyboard to select noncontiguous words, sentences, or paragraphs using a trackpad or mouse
  - Streamlined in-app notifications inform you when a person joins a collaborative document for the first time
  - Preserve file format and full quality when adding HEIC photos taken on iPhone or iPad
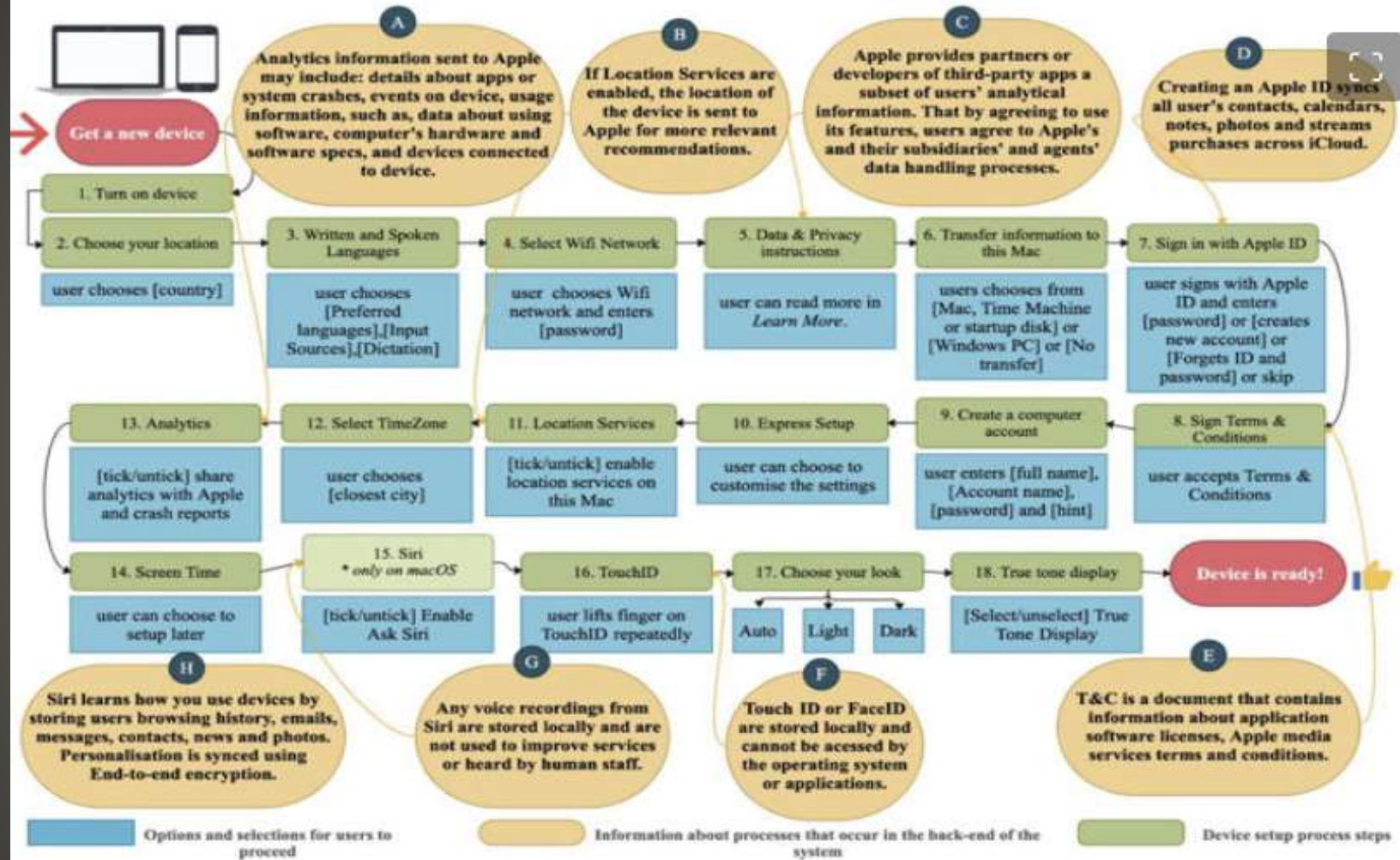 - Additional stability and performance improvements
- **Keynote**
  - Add a new look to your slides with the Dynamic Color, Minimalist Light, and Minimalist Dark themes
  - Streamlined in-app notifications inform you when a person joins a collaborative presentation for the first time
  - Preserve file format and full quality when adding HEIC photos taken on iPhone or iPad
  - On iPad, press and hold the Command key on a connected keyboard to select noncontiguous words, sentences, or paragraphs using a trackpad or mouse
  - Improved compatibility for slide transitions when importing and exporting Microsoft PowerPoint files
  - Additional stability and performance improvements
- **Numbers**
  - Streamlined in-app notifications inform you when a person joins a collaborative spreadsheet for the first time
  - Preserve file format and full quality when adding HEIC photos taken on iPhone or iPad
  - On iPad, press and hold the Command key on a connected keyboard to select noncontiguous words, sentences, or paragraphs using a trackpad or mouse
  - Additional stability and performance improvements

iWork iPad Shortcuts

A — Analytics information sent to Apple may include: details about apps or system crashes, events on device, usage information, such as, data about using software, computer's hardware and software specs, and devices connected to device.

B — If Location Services are enabled, the location of the device is sent to Apple for more relevant recommendations.

C — Apple provides partners or developers of third-party apps a subset of users' analytical information. That by agreeing to use its features, users agree to Apple's and their subsidiaries' and agents' data handling processes.

D — Creating an Apple ID syncs all user's contacts, calendars, notes, photos and streams purchases across iCloud.

Get a new device

1. Turn on device

2. Choose your location — user chooses [country]

3. Written and Spoken Languages — user chooses [Preferred languages],[Input Sources],[Dictation]

4. Select Wifi Network — user chooses Wifi network and enters [password]

5. Data & Privacy instructions — user can read more in *Learn More.*

6. Transfer information to this Mac — users chooses from [Mac, Time Machine or startup disk] or [Windows PC] or [No transfer]

7. Sign in with Apple ID — user signs with Apple ID and enters [password] or [creates new account] or [Forgets ID and password] or skip

13. Analytics — [tick/untick] share analytics with Apple and crash reports

12. Select TimeZone — user chooses [closest city]

11. Location Services — [tick/untick] enable location services on this Mac

10. Express Setup — user can choose to customise the settings

9. Create a computer account — user enters [full name], [Account name], [password] and [hint]

8. Sign Terms & Conditions — user accepts Terms & Conditions

14. Screen Time — user can choose to setup later

15. Siri * only on macOS — [tick/untick] Enable Ask Siri

16. TouchID — user lifts finger on TouchID repeatedly

17. Choose your look — Auto | Light | Dark

18. True tone display — [Select/unselect] True Tone Display

Device is ready!

H — Siri learns how you use devices by storing users browsing history, emails, messages, contacts, news and photos. Personalisation is synced using End-to-end encryption.

G — Any voice recordings from Siri are stored locally and are not used to improve services or heard by human staff.

F — Touch ID or FaceID are stored locally and cannot be acessed by the operating system or applications.

E — T&C is a document that contains information about application software licenses, Apple media services terms and conditions.

Options and selections for users to proceed

Information about processes that occur in the back-end of the system

Device setup process steps

Privacy. That's iPhone

- Aalto University Study
- [Privacy of Default Apps in Apple's Mobile Ecosystem](#)

Apple Data Privacy

- Anti-stalking utility
  Find My

"This item isn't certified on the Apple Find My network. You can disable this item and stop it from sharing its location with the owner. To do this, follow the instructions provided on a website by the manufacturer of this item."

- MDM

  Beta version can be enforced

- Web distribution
  Iff EU

iOS 17.5 Beta features

- AI-focused M4 chips
  MacBook Pro then others
- iPads   iPad Pro iPad Air
- iPhone 16

Apple Rumor

- Turn Off
- Yeahbut Screen has other ideas
- Hold Digital Crown and Side button

Apple Watch Ghost Touch

- 6.1-inch OLED display with notch
- 138.4 x 67.3 x 7.3 mm -> 147.7 x 71.5 x 7.7 mm
- Touch ID with Home button -> Face ID
- Faster A17?
- USB-C

iPhone SE 4

- $200 8GB -> 16GB
- YeahBut AI?

Macs with 8GB RAM

- Customize Lock Screen
  iPadOS 17
  https://www.xda-developers.com/how-to-customize-lock-screen-ios/?
- Stage Manager
  https://www.xda-developers.com/how-to-use-stage-manager-macos/?
- Three-dot Menu

Floating menu: Full Screen   Split View   Slide Over

iPad Tips

Split View
NOT ALL APPS SUPPORT
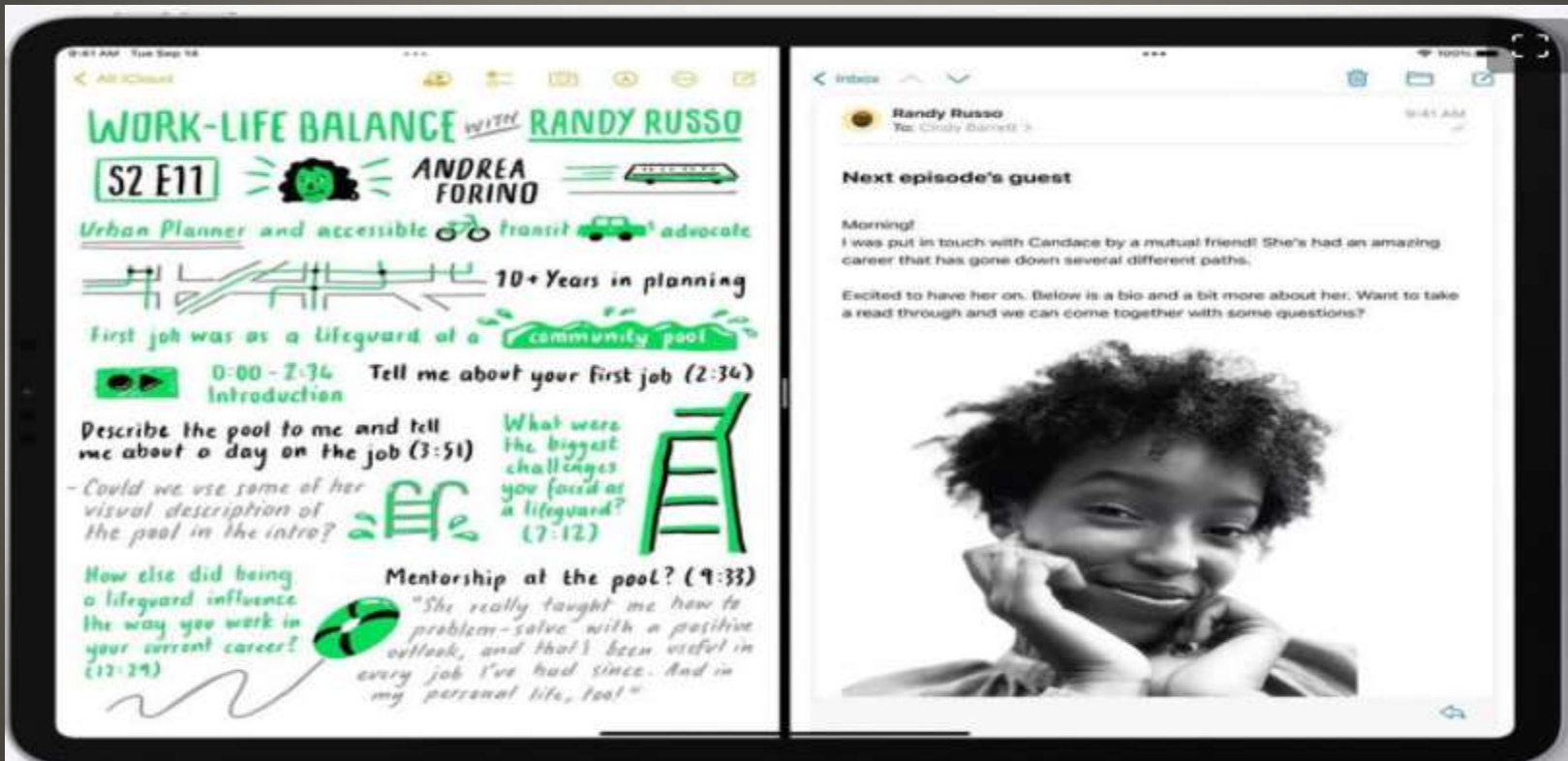
iPad Tips

Slide Over
Multiple Supported Apps over main background window
Swipe to edge to hide
Center Window

iPad Tips

- The Shelf
  Multiple Pages of App near bottom of screen

iPad Tips

- Picture-in-Picture
  Watch videos
  Access Main Screen   Position as desired
  Swipe to side to hide
  Drag Gray arrow icon to have video reappear
  Use Pinch gesture to resize video
- Quick Note
   Swipe up bottom left
- Keyboard Shortcuts
  Attached keyboard
- Virtual Keyboard
  Pinch to shrink
  Drag with gray bar
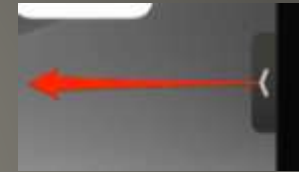
iPad Tips

- Focus Modes

https://www.xda-developers.com/focus-ios-15-macos-monterey/?
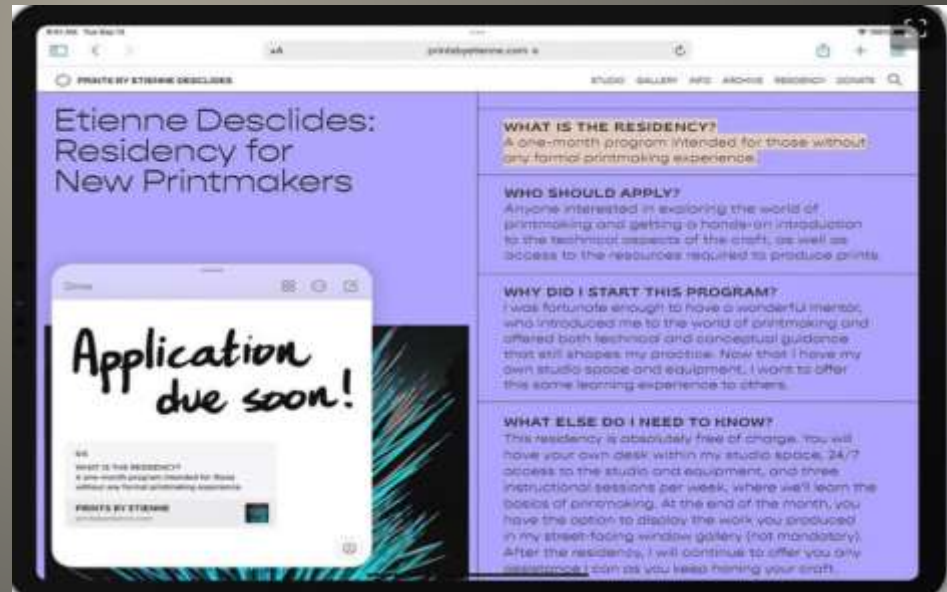
- Code your own apps
  Swift Playgrounds
  Apple Developer
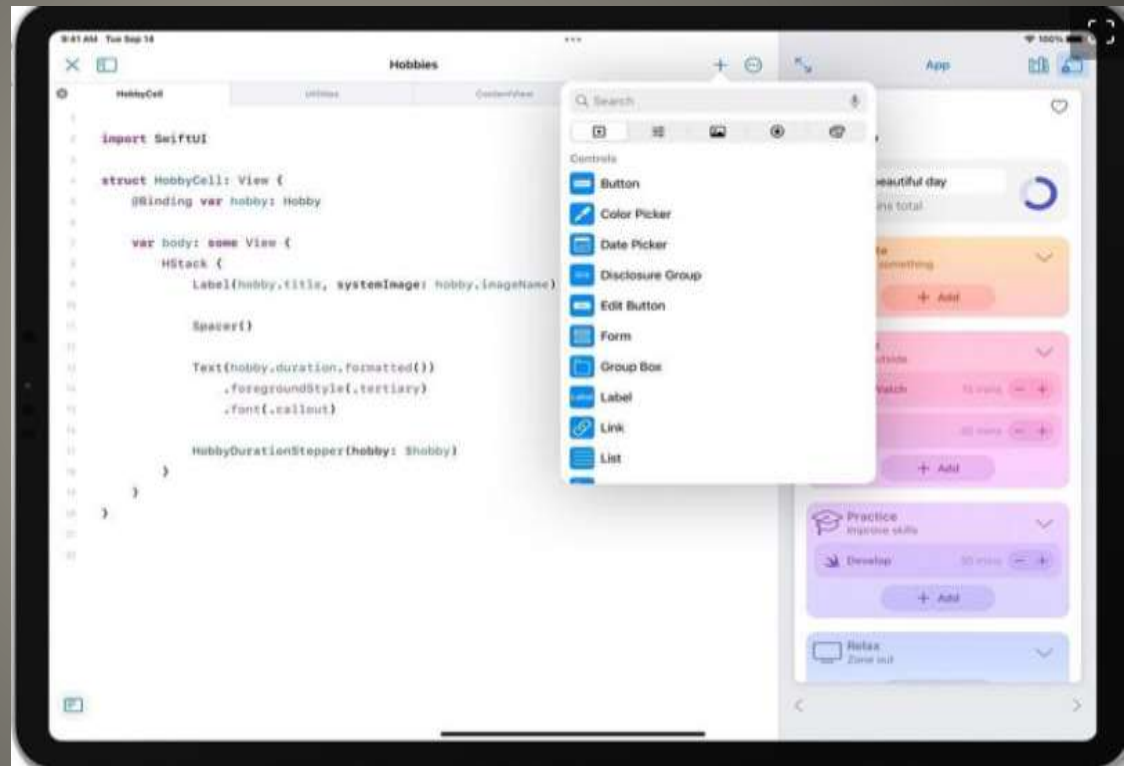
iPad Tips

- Handoff and Continuity   Wi-Fi & Bluetooth
- Sidecar Side display with pencil
- Universal Control

https://www.xda-developers.com/how-to-use-universal-control/?

iPad Tips   Apple Eco System Mac

- XProtect – scan for known malware Remediate
- Block malware Gatekeeper, Notarization
- Prevent launch or execution

- YeahBut "You have a virus!" Probably not   Application Notification Masquerading as System Alert updates-mac.com   "Allow Notifications"
- Browser   Settings > Websites

macOS

- Reset Password
- Allow Don't Allow
- Push bombing
- Don't Allow as you should
- Allow – just quit!!   NO PLEASE NO
- Follow up Phone call – NOT Apple Support

Apple 2FA Bombing

- 28-character alphanumeric code
- Good
   Strong key
   Only you have it
   Timely account recovery
   Nevermind On Off New
- Bad
   Loss is a real loss
   Disable account recovery
   Inconvenient

AppleID Recovery Key

- "Apple detected that you are being targeted by a mercenary spyware attack that is trying to remotely compromise the iPhone associated with your Apple ID," read the notification. "This attack is likely targeting you specifically because of who you are or what you do. Although it's never possible to achieve absolute certainty when detecting such attacks, Apple has high confidence in this warning — please take it seriously."

iPhone Spyware

- Blackberry says:
- LightSpy "sophisticated iOS implant"
- Lockdown Mode

iPhone Spyware

- Most message attachments will not work
- WEB browsing becomes restricted
- Facetime from new contacts will not work
- Restricted access to accessories
- Certain applications will not run
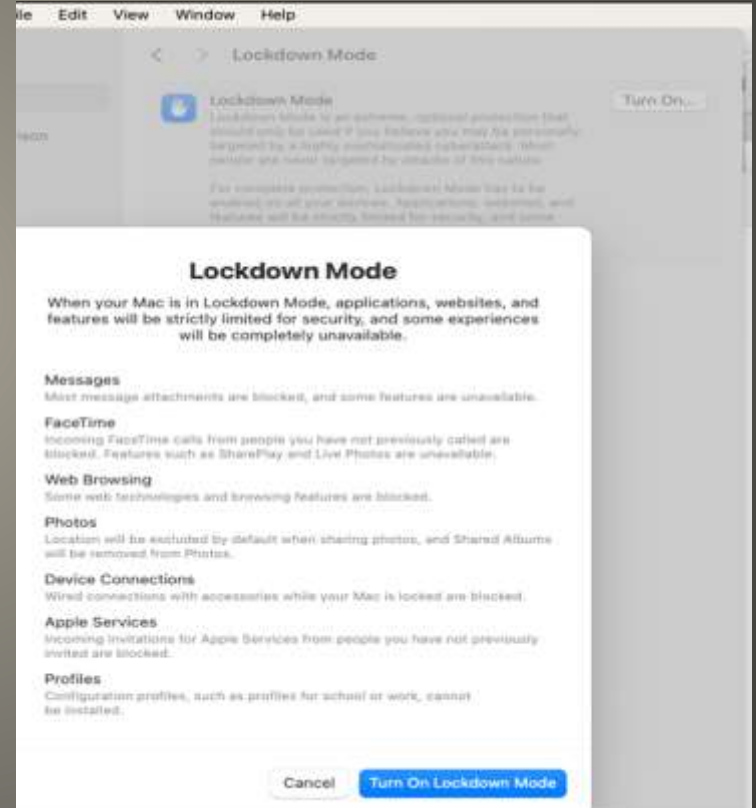
macOS Security Lockdown Mode

- Lockdown Mode
- Apple Mail
  Mail Privacy Protection
  Masking IP address
  Loading content in background
  Hide My Email
- Gatekeeper & SIP
- Sandbox for apps
- FileVault encryption
- Linux base

macOS Security

- Anti-virus => Security Suites
- XProtect signature based
   0-day signatures
   Delay in XProtect data
   XProtect data blocked/altered
- Gatekeeper
   Application signing
   Developer's signing certificate compromised
   User able to bypass Gatekeeper
- User Social engineering
   Click through warnings
   "Follow directions"
- Browser protections

Macs need Anti-virus?

- Resources needed
- Resources used
- Anti-virus can "see" data you can not
- Helpful <-> Harmful
- Rosetta 2 Apple silicon run Intel based code
- Apple silicon Secure Boot vs Intel EFI
- Recovery mode
- Device Firmware Update Mode (DFU)

Macs need Anti-Virus?

- Recovery Mode
  Most Apple devices
  Uses bootloader
  Connect to Mac Install iOS/iPadOS
- Device Firmware Update
  Secret handshake
  Corrupt boot loader
- Mac T2 security chip
  Restore using another Mac

Wait, Recovery Mode   DFU?

- Was Mac only
- Apple App Store protections not 100%
- Files loaded from Internet warning
- Files loaded from Internet setting
- Apps can infect post-install
- Discounted Tax return software
- Be Aware

Apps   Sideloading

- System Integrity Protection (SIP)
- Normal SIP bypass
   Restart in Recovery Mode
   Setup
   Restart   i.e. physical access
- Migration Assistant
- Add exception to SIP exclusion list
- Apple macOS updates
   Ventura 13.4, Monterey 12.6.6, Big Sur 11.7.7

Migraine

- System Settings Trackpad
  App Exposé Open windows for that app
- System Settings > Accessibility > Pointer Control > Trackpad
  Use Trackpad for dragging With Drag Lock
  Drag & Drop past trackpad limits
- Laptop battery
  Screen Saver 20 -> 5
  Battery *Slightly dim the display on battery*
- Dark Room to Bright Sunlight
  Settings > Displays > Automatically adjust brightness
  Settings > Displays > Night Shift
  True Tone enabled
  ProMotion from Refresh Rate dropdown menu

macOS

- Default Apps
  Default web browser
  Settings > Desktop & Dock > Widgets
  Default email

  Mail > Settings > General > Default email reader
  Any file > Right click > Get Info button
  Browser Extensions
  Consent-O-Matic   automatically opt-out ??
  FileVault On   Settings > Privacy & Security
  Privacy & Security
  Analytics & Improvements Off (ON in Beta)
  Apple Advertising

macOS

- Apple has ways of tracking when you are personally targeted by cyber-criminals
- Apple Threat Notifications

"Apple threat notifications are designed to inform and assist users who may have been individually targeted by mercenary spyware attacks, likely because of who they are or what they do"

"Mercenary spyware attacks cost millions of dollars and often have a short shelf life, making them much harder to detect and prevent."

- Threat Notification at top of page when signed in on AppleID website
- Email and iMessage to address & numbers associated with AppleID
- High confidence alerts

"We strongly suggest you enlist expert help, such as the rapid-response emergency security assistance provided by the Digital Security Helpline at the nonprofit Access Now."

https://www.accessnow.org/

Apple Threat Notifications

iPhone Lockdown Mode – what changes?

Here's what Apple says happens when you activate Lockdown Mode in its official guide...

- Messages - Most message attachment types are blocked, other than certain images, video, and audio. Some features, such as links and link previews, are unavailable.

- Web browsing - Certain complex web technologies are blocked, which might cause some websites to load more slowly or not operate correctly. In addition, web fonts might not be displayed, and images might be replaced with a missing image icon.

- FaceTime - Incoming FaceTime calls are blocked unless you have previously called that person or contact. Features such as SharePlay and Live Photos are unavailable.

- Apple services - Incoming invitations for Apple services, such as invitations to manage a home in the Home app, are blocked unless you have previously invited that person. Game Center is also disabled.

- Photos - When you share photos, location information is excluded. Shared albums are removed from the Photos app, and new Shared Album invitations are blocked. You can still view these shared albums on other devices that don't have Lockdown Mode enabled.

- Device connections - To connect your iPhone or iPad to an accessory or another computer, the device needs to be unlocked. To connect your Mac laptop with Apple silicon to an accessory, your Mac needs to be unlocked and you need to provide explicit approval.

- Wireless connectivity - Your device won't automatically join non-secure Wi-Fi networks and will disconnect from a non-secure Wi-Fi network when you turn on Lockdown Mode. 2G cellular support is turned off.

- Configuration profiles - Configuration profiles can't be installed, and the device can't be enrolled in Mobile Device Management or device supervision while in Lockdown Mode. ■

The Following Slide from MUG January 24, 2024

- Reboot Daily: According to research from Amnesty International and Citizen Lab, Pegasus often relies on zero-click 0-days with no persistence. Regular daily reboots can help clean the device, making it necessary for attackers to repeatedly reinfect, thereby increasing the chances of detection over time.
- Lockdown Mode: There has been several public reports on the success of Apple's newly added lockdown mode in blocking iOS malware infection.
- Disable iMessage and Facetime: iMessage, enabled by default, is an attractive exploitation vector. Disabling it reduces the risk of falling victim to zero-click chains. The same advice applies to Facetime, another potential vector for exploitation.
- Keep Device Updated: Install the latest iOS patches promptly, as many iOS exploit kits target already patched vulnerabilities. Swift updates are crucial for staying ahead of some nation-state attackers who may exploit delayed updates.
- Exercise Caution with Links: Avoid clicking on links received in messages, as Pegasus customers may resort to 1-click exploits delivered through SMS, other messengers, or email.
- Check Backups and Sysdiags Regularly: Processing encrypted backups and Sysdiagnose archives using MVT and Kaspersky's tools can help in detecting iOS malware.

iOS spyware mitigations

- Exclude specific apps and/or websites

**Activate Lockdown Mode
On Other Devices**

Lockdown on macOS

- Delayed   now May?
- 10.9"
- 12.9"
- Air and Pro versions
- M2 chip
- Front camera moved to side bezel

2024 iPad Air ?

- Apple AI Reference Resolution as Language Modeling (ReALM)

  Radically enhance how voice assistants understand/respond

  Understand pronouns & indirect references in conversation

  Parsing on-screen entities & locations

  Tune LLM for reference resolution tasks

  Users with disabilities

  Integrates text and visual information

Siri

- Advanced Camera
- Extra storage
- "If your subject is a person, dog, or cat, iPhone 15 lets you quickly capture the shot and turn it into a portrait later."
- Movie

   Action mode, Cinematic mode, …
- USB-C charging
- Dynamic Island

New iPhone envy?

- News+ game Quartiles
- Expanded sideloading
- Palestinian Flag emoji fix
- Notes app with Tip
- Apple Books Reading Goals

iOS 17.5 Beta 2

- On device LLM
- Ajax ?

iOS 18

- Probably M4
- Neural engine

M3 Mac mini

- Dock is not Taskbar
  Taskbar icons, time & date, search, & stuff
  Dock Pinned App icons,   Launchpad
- Different keys keyboard
  Alt -> Option
  Enter -> Return
  Backspace -> Delete
  Control   same but different
  Ctrl + C   Copy   Command + C
- Names

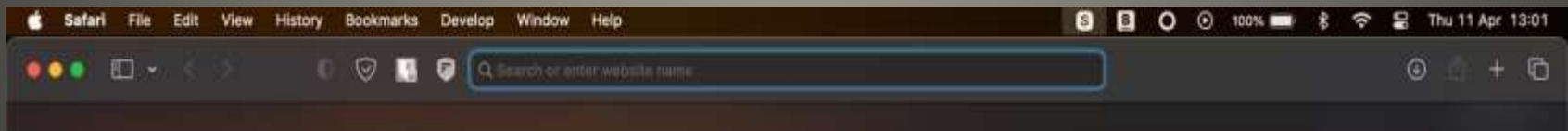| Windows	Mac
Control Panel	System Settings
Ctrl+Alt+Delete	Command+Option+Escape
File Explorer	Finder
Recycle Bin	Trash
Shortcut icon	Alias

Windows macOS

- Edge <-> Safari
- Task Manager > Activity Monitor
- Outlook -> Mail
- Notepad -> TextEdit
- Word > Pages
- Excel > Numbers
- [window buttons: _ ☐ X]   Red – Close   Yellow – Minimize   Green – Maximize

- Search Bar > Spotlight
- Task Bar > Menu Bar

Windows macOS

- None of us are as experienced as all of us
- Awareness, Preparedness, Understanding
- Participate
- Topic Suggestions
- Questions: scccMUG@gmail.com

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

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

- Questions, suggestions, comments?

SCCCMUG@gmail.com