Sun City Computer Club

Cyber Security SIG

December 15, 2022

Questions, Comments, Suggestions welcomed at any time

Even Now

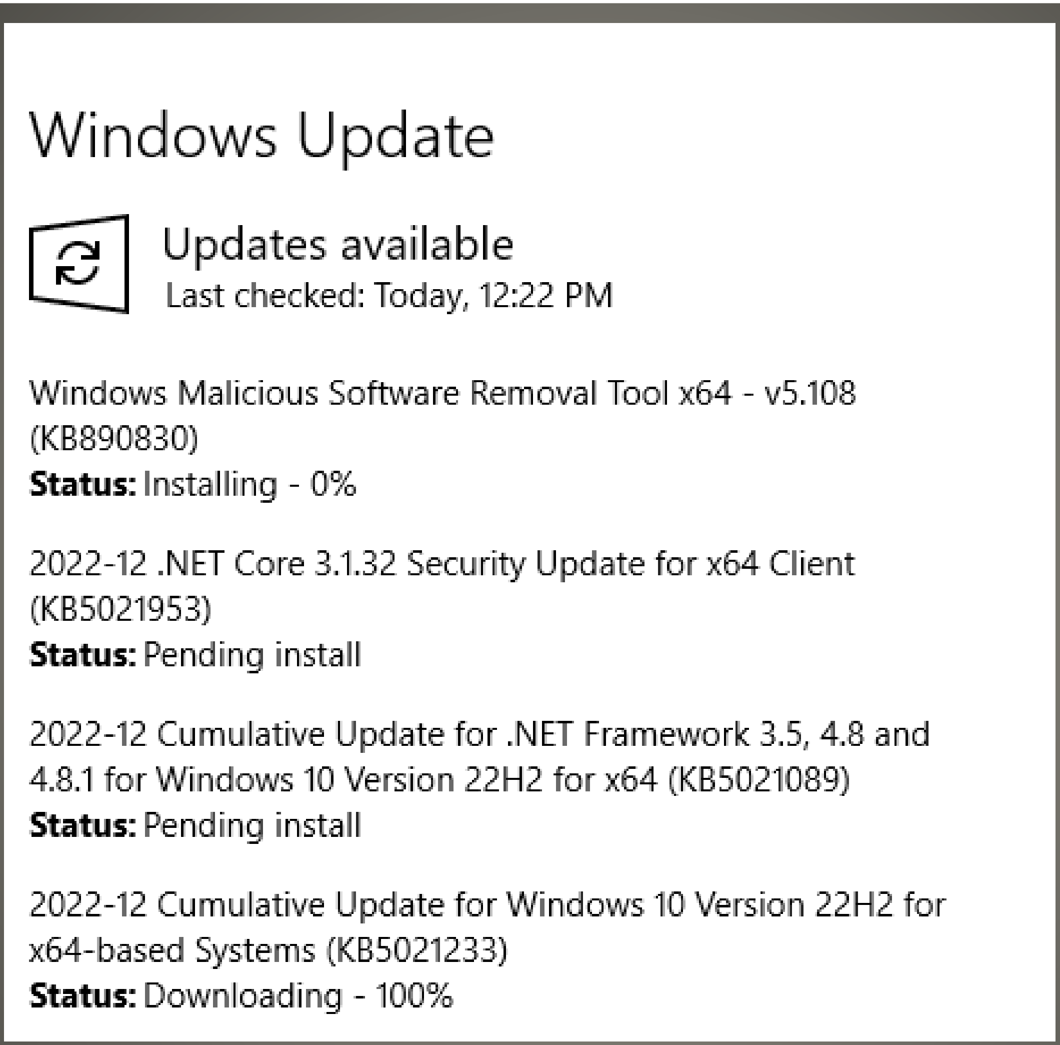
- Audio recording of this session as MP4 file
- Audio recording available at link shown above

Audio Recording In Progress

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

Updates

- ChromeOS 108.0.5359.111
- Any VMs



Windows Update

Updates available

Last checked: Today, 12:22 PM

Windows Malicious Software Removal Tool x64 - v5.108 (KB890830)

Status: Installing - 0%

2022-12 .NET Core 3.1.32 Security Update for x64 Client (KB5021953)

Status: Pending install

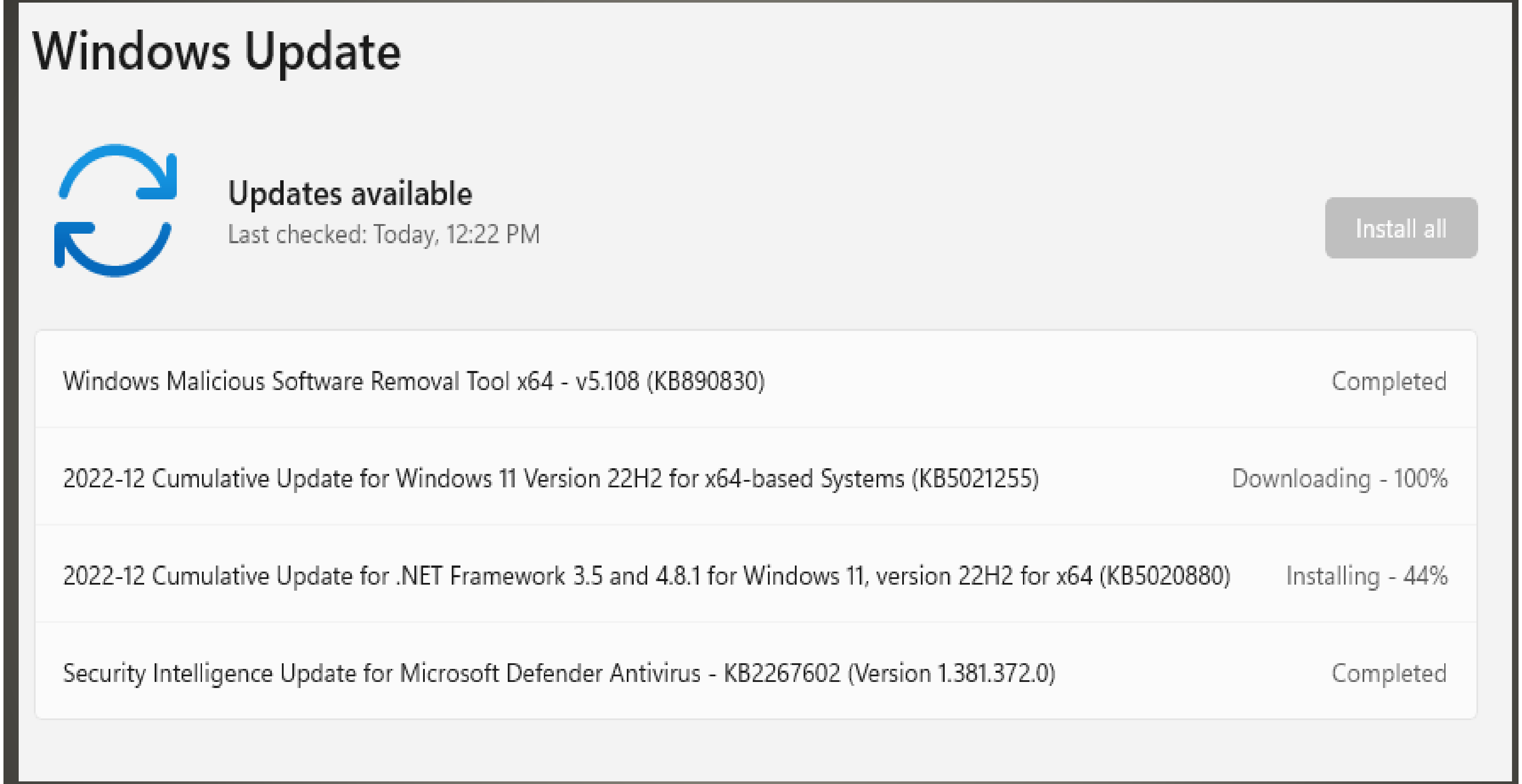
2022-12 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 for x64 (KB5021089)

Status: Pending install

2022-12 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems (KB5021233)

Status: Downloading - 100%

Windows Update Windows 10



Windows Update

Updates available

Last checked: Today, 12:22 PM

Windows Malicious Software Removal Tool x64 - v5.108 (KB890830)	Completed
2022-12 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems (KB5021255)	Downloading - 100%
2022-12 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 22H2 for x64 (KB5020880)	Installing - 44%
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.381.372.0)	Completed

Windows Update Windows 11

Windows Update Schedule B

- 74 Vulnerabilities
- 7 Critical
- 1 Previously Disclosed
- 1 Actively exploited

Windows Update

- Windows 8.1 end of support Jan 10, 2023

- Apple has released security updates to address vulnerabilities in multiple products. An attacker could exploit some of these vulnerabilities to take control of an affected device.

- iCloud for Windows 14.1
- Safari 16.2
- macOS Monterey 12.6.2
- macOS Big Sur 11.7.2
- tvOS 16.2
- watchOS 9.2
- iOS 15.7.2 and iPadOS 15.7.2
- iOS 16.2 and iPadOS 16.2
- macOS Ventura 13.1

Apple Updates Everything

Updates

- Browser Updates
- App Updates Microsoft Store Apple Store

Holiday Scams

- PayPal
  Now Amazon (NOT REALLY)
  AnyDesk

Aikido

- Anti-Virus
- Security Suites
- End Point Protection
- Delete (really delete) protected malware
- Wiper
- Microsoft Defender
- Defender for Endpoint
- SentinelOne EDR
- TrendMicro Apex One
- Avast Antivirus
- AVG Antivirus

- Palo Alto
- XDR
- Cylance
- CrowdStrike
- McAfee
- BitDefender

Aikido safer

- Hive Social
  Twitter alternative
  HUGE growth
  Even LARGER vulnerability issues
  Client data exposed
  Servers taken down 2-Dec-2022
- 7 bullet theory North Carolina power substation
  And more
- Restaurant Facebook sites hacked
  Attacker create ads for other sites
- US Cyber Safety Review Board
  "Please tell us how"
  Lapsus$ Uber, Microsoft, Okta, Samsung, …
  16–21-year-old
- Android manufacturer's encryption keys stolen
  Over-the-Air updates   Samsung & LG

Current Issues

- Catfishing

Catfishing is a term for a person who pretends to be someone else online.

- Sirius XM vulnerability

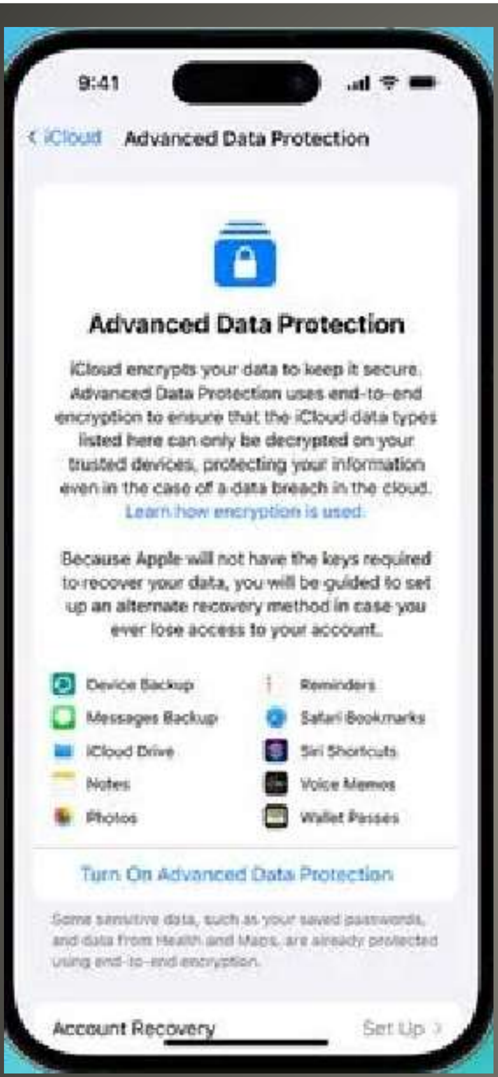
Connected vehicle services

Earlier this year, we were able to remotely unlock, start, locate, flash, and honk any remotely connected Honda, Nissan, Infiniti, and Acura vehicles, completely unauthorized, knowing only the VIN number of the car.

- Apple plan to scan for CSAM
- Apple Enhanced iCloud Encryption

Current Issues

Apple Enhanced iCloud Encryption



< iCloud Advanced Data Protection

Advanced Data Protection

iCloud encrypts your data to keep it secure. Advanced Data Protection uses end-to-end encryption to ensure that the iCloud data types listed here can only be decrypted on your trusted devices, protecting your information even in the case of a data breach in the cloud. Learn how encryption is used.

Because Apple will not have the keys required to recover your data, you will be guided to set up an alternate recovery method in case you ever lose access to your account.

- Device Backup
- Messages Backup
- iCloud Drive
- Notes
- Photos
- Reminders
- Safari Bookmarks
- Siri Shortcuts
- Voice Memos
- Wallet Passes

Turn On Advanced Data Protection

Some sensitive data, such as your saved passwords, and data from Health and Maps, are already protected using end-to-end encryption.

Account Recovery Set Up >

- Device Backup
- Messages Backup
- iCloud Drive
- Notes
- Photos
- Reminders
- Safari Bookmarks
- Siri Shortcuts
- Voice Memos
- Wallet Passes

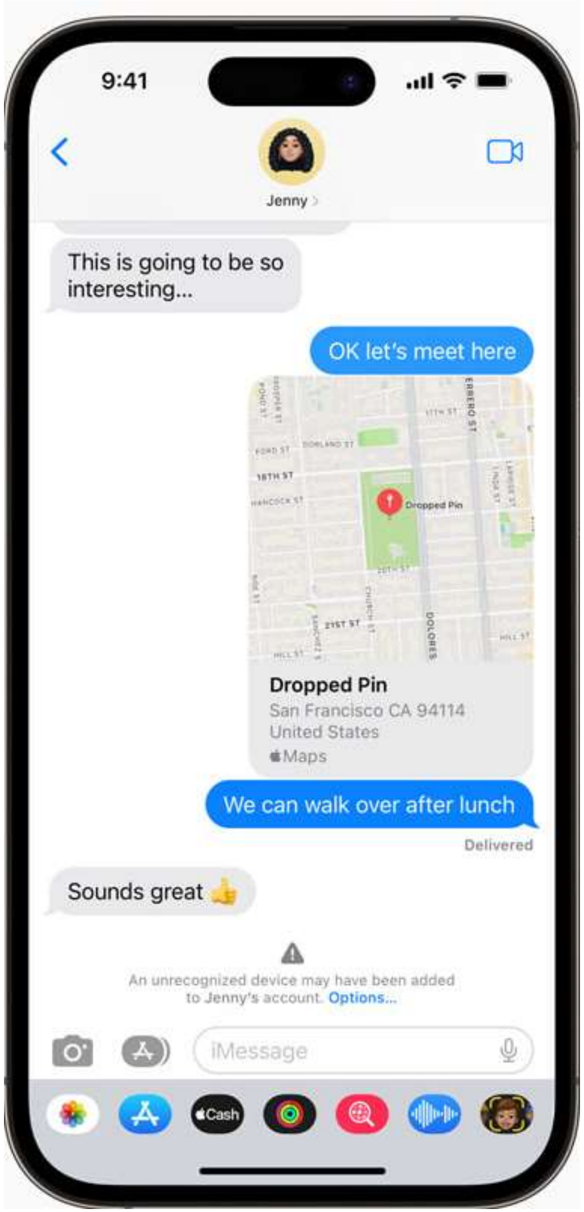
Apple Enhanced iCloud Encryption

- End-to-End encryption
- Encryption double edged sword
- No one else

  Not Apple, Not Law Enforcement
- Encrypt iCloud backups already
- EFF et al “yea”
- FBI “Hey”

- iMessage Contact Key Verification
- Security Keys for Apple ID
- Lockdown Mode

Other Apple privacy initiatives



This is going to be so interesting...

OK let's meet here

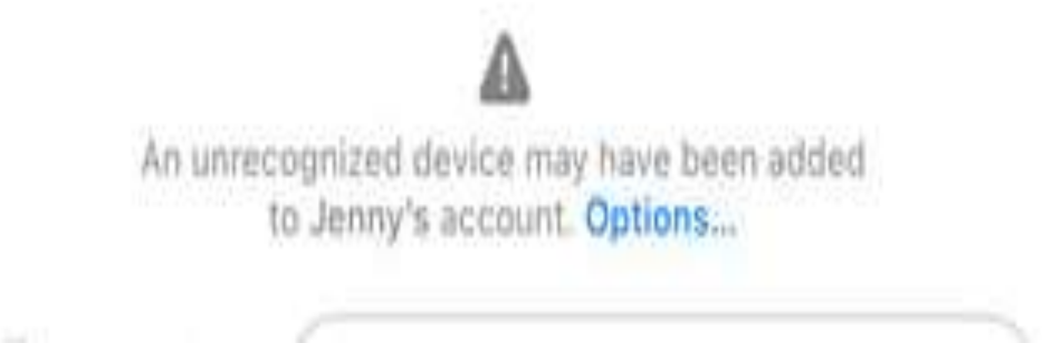
Dropped Pin
San Francisco CA 94114
United States
Maps

We can walk over after lunch

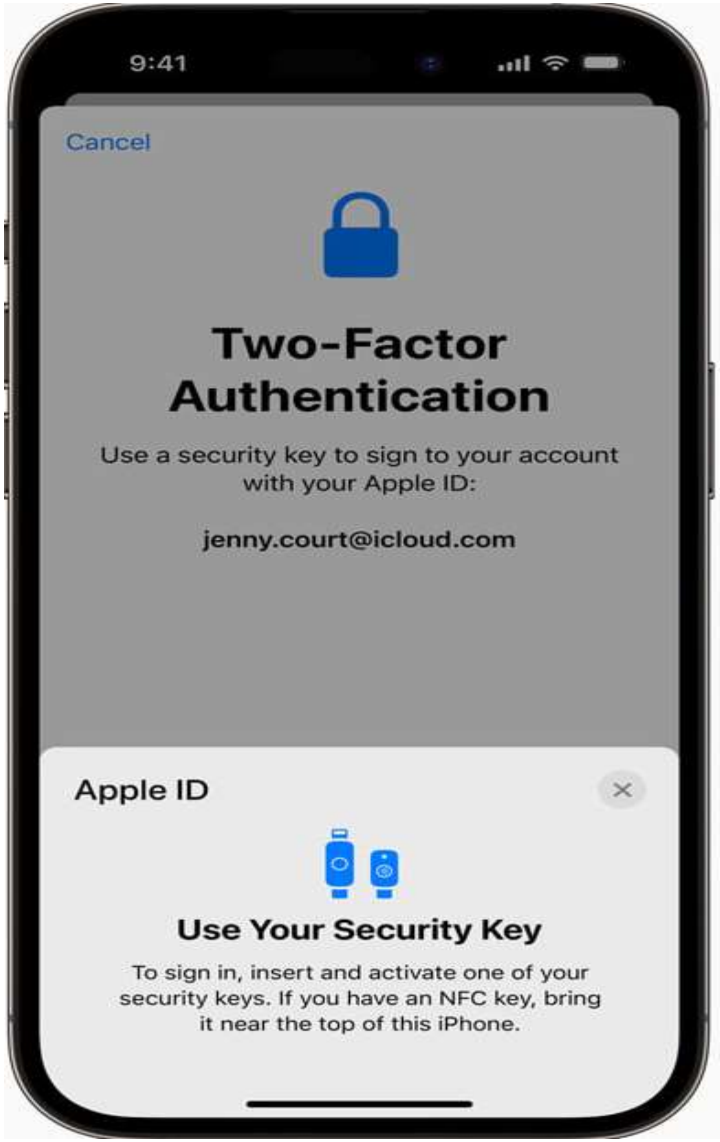
Delivered

Sounds great 👍

An unrecognized device may have been added to Jenny's account. Options...



An unrecognized device may have been added to Jenny's account. Options...



Two-Factor Authentication

Use a security key to sign to your account with your Apple ID:

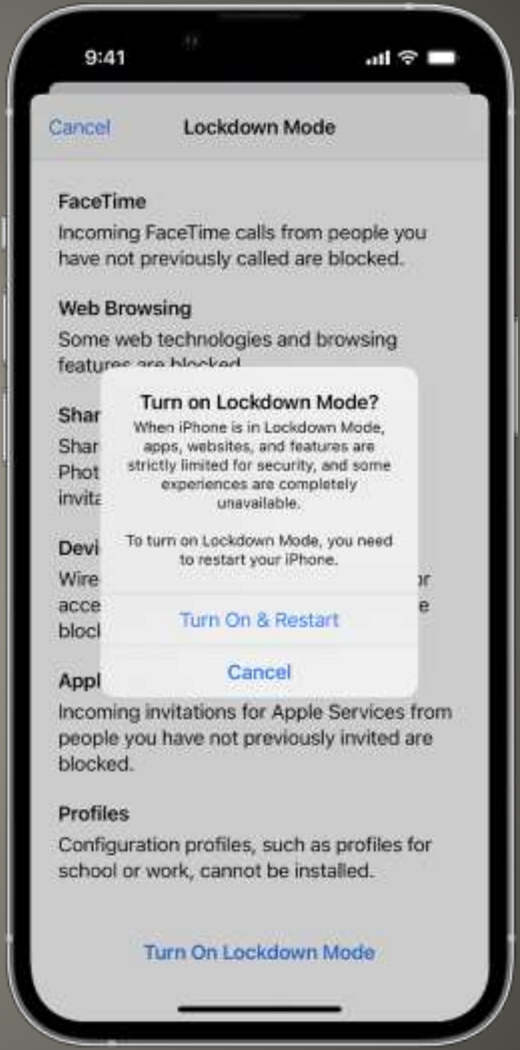
jenny.court@icloud.com

Apple ID

Use Your Security Key

To sign in, insert and activate one of your security keys. If you have an NFC key, bring it near the top of this iPhone.

Lockdown Mode



9:41

Cancel

Lockdown Mode

FaceTime

Incoming FaceTime calls from people you have not previously called are blocked.

Web Browsing

Some web technologies and browsing features are blocked.

Shar

Shar

Phot

invita

Devi

Wire r

acce e

bloc

Turn on Lockdown Mode?

When iPhone is in Lockdown Mode, apps, websites, and features are strictly limited for security, and some experiences are completely unavailable.

To turn on Lockdown Mode, you need to restart your iPhone.

Turn On & Restart

Cancel

Appl

Incoming invitations for Apple Services from people you have not previously invited are blocked.

Profiles

Configuration profiles, such as profiles for school or work, cannot be installed.

Turn On Lockdown Mode

- How Lockdown Mode protects your device
- When Lockdown Mode is enabled, some apps and features will function differently, including:
- 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.
- 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.
- Shared Albums - 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. When you turn off Lockdown Mode, you need to turn Shared Albums on again in your device settings.
- 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 explicit approval provided.
- 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.
- Phone calls and plain text messages continue to work while Lockdown Mode is enabled. Emergency features, such as SOS emergency calls, are not affected.

Lockdown Mode

- You and only you
- Not Apple Not LE Not government …
- Lose the key not you either
- Credential theft someone else not you
- Info valued and vital to heirs
- NOT On by default
- ALL Devices under an Apple ID need 16.2

  Move older devices to another or new ID
- Chose one or both recovery methods

  Recovery Contact Recovery key

Advanced Data Protection Cautions

- Recovery Contact
  - Trusted person in contacts lists with Apple device & Apple ID
  - Message to that recovery contact
  - Recovery contact accepts
  - They can help you with recovery access
  - Unable to unlock on their own
- Recovery Key
  - 28-character key
  - Verify the key
  - GUARD that key
- Enable Advanced Data Protection

Advanced Data Protection Cautions

Advanced Data Protection Cautions

- Web access from iCloud DISABLED
- No One   remember NO ONE
- Data already protected
  - Passwords and Keychain
  - Health data
  - Home data
  - Messages in iCloud (but not iCloud backups)
  - Payment information
  - Apple Card transactions
  - Apple Maps (details such as favorites and search history)
  - QuickType Keyboard learned vocabulary
  - Safari (details such as history, tab groups, and iCloud tabs)
  - Screen Time
  - Siri information (details such as settings and personalization)
  - Wi-Fi passwords
  - W1 and H1 Bluetooth keys
  - Memojions already enabled

Advanced Data Protection Cautions

- Advanced Data Protection Options
  - iCloud backup
  - iCloud Drive
  - Photos, including photos in a Shared Library, if everyone in the Shared Library has Advanced Data Protection enabled
  - Notes
  - Reminders
  - Safari Bookmarks
  - Siri Shortcuts
  - Voice Memos
  - Wallet passes

- No Protections
- iCloud Mail
- Contacts
- Calendars
- Photos stored in Shared Albums and any file shared with “Anyone with a link”
- Any document shared for iWork collaboration
- Any third-party app data that doesn’t employ its own end-to-end encryption (though if the backups of those apps are stored in iCloud Backup, they will be end-to-end encrypted, and if an app stores data in iCloud Drive, it should be end-to-end encrypted, as well)
- Some metadata and usage information (details such as the names of your devices, the sizes of files, and more, which is notable because recent reports suggest that Apple isn’t entirely transparent about the data it collects)

Advanced Data Protection Cautions

- iCloud

  Recommended by Apple again and again

  Revenue for Apple

  Multiple

  1-2-3 Backup

  Encrypt backup then backup the backup

  Need to be logged in with AppleID

  No Power   No Internet

  Account taken over

Advanced Data Protection Cautions

- Cybersecurity Advisories for Cybersecurity and Infrastructure Security Agency
- CISA Phishing Infographic
- https://www.cisa.gov/sites/default/files/publications/phishing-infographic-508c.pdf

- GPS location, speed, turn-by-turn navigation, maintenance, crash detection,

Samsung presentation

Potential sale of 15 Billion auto records to US government – Vice

VIN

Infotainmainment info call logs

MyHyundai MyGenesis

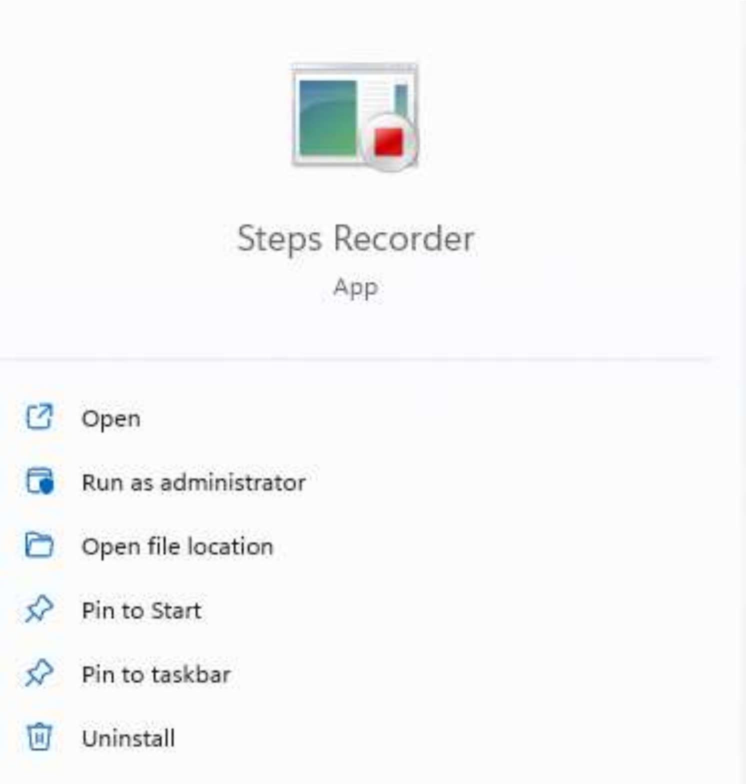
OnStar

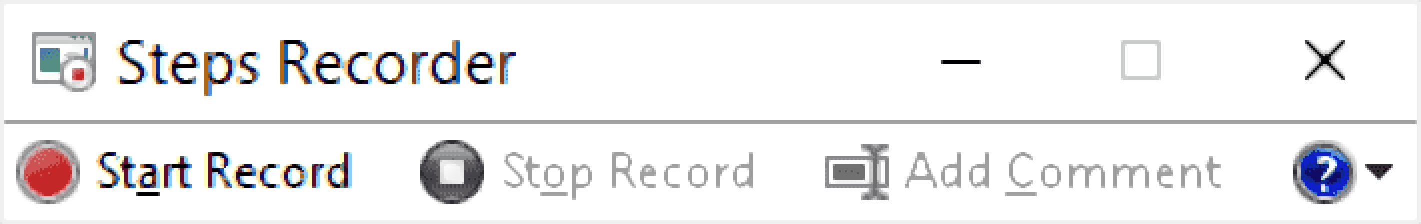
Jeep Cherokee hacked with someone at wheel

Sirius XM

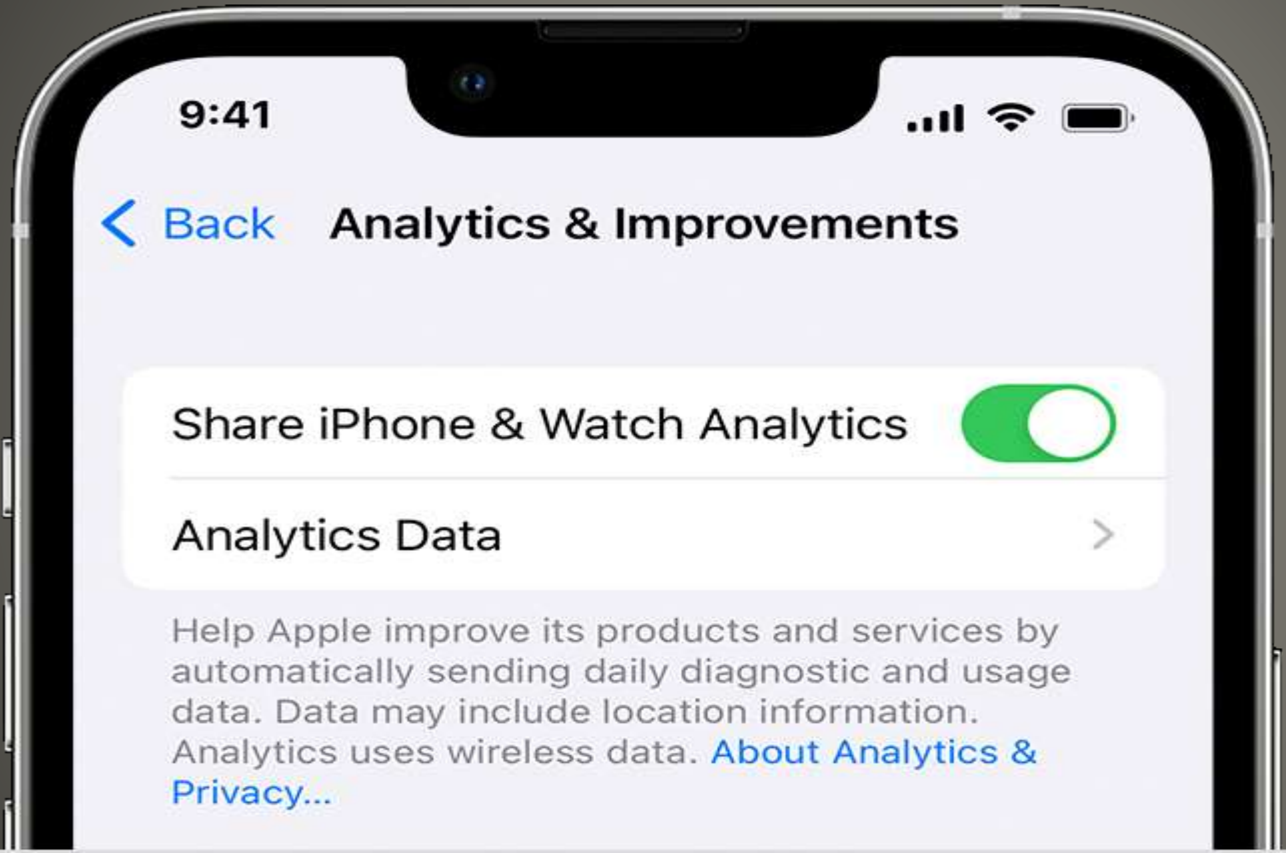
- All Windows versions?
- Troubleshooting tool
- Start > Steps Recorder

Windows step recorder


Steps Recorder
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar
Uninstall


Steps Recorder
Start Record
Stop Record
Add Comment

- Apple iPhone Analytics privacy setting



Share iPhone & Watch Analytics ●

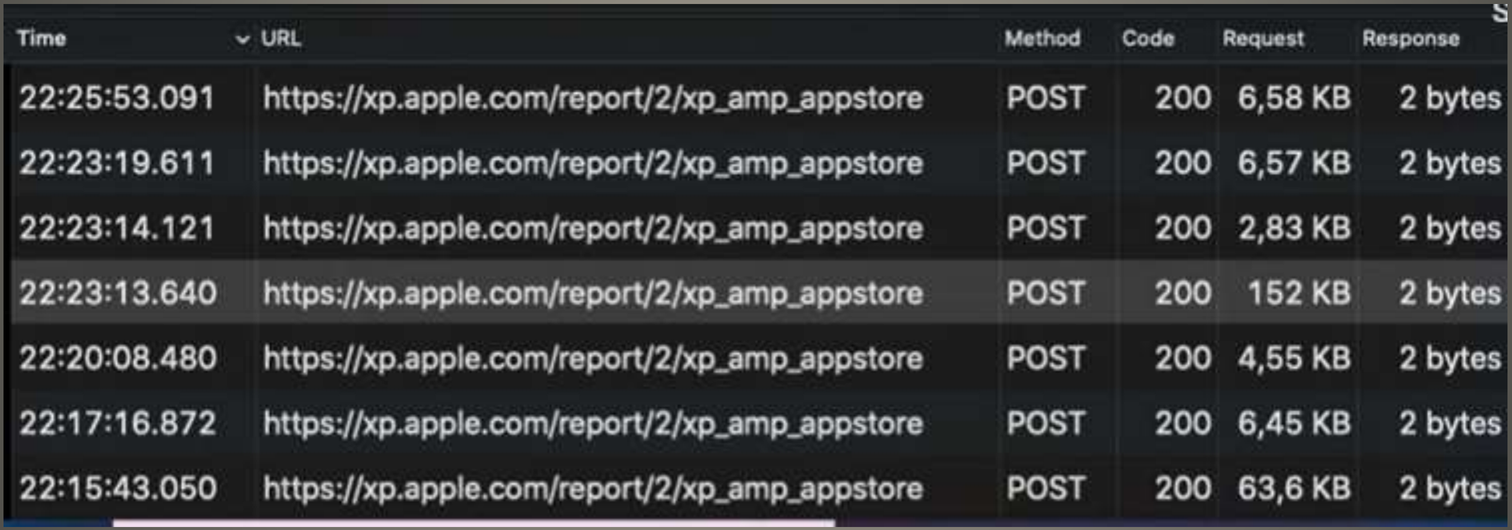
Analytics Data >

Help Apple improve its products and services by automatically sending daily diagnostic and usage data. Data may include location information. Analytics uses wireless data. About Analytics & Privacy...

Privacy

Apple App store

- App search, ads viewed, how long, etc.
- IDs   unique IDs
- Device details, storage, language



Time	URL	Method	Code	Request	Response
22:25:53.091	https://xp.apple.com/report/2/xp_amp_appstore	POST	200	6,58 KB	2 bytes
22:23:19.611	https://xp.apple.com/report/2/xp_amp_appstore	POST	200	6,57 KB	2 bytes
22:23:14.121	https://xp.apple.com/report/2/xp_amp_appstore	POST	200	2,83 KB	2 bytes
22:23:13.640	https://xp.apple.com/report/2/xp_amp_appstore	POST	200	152 KB	2 bytes
22:20:08.480	https://xp.apple.com/report/2/xp_amp_appstore	POST	200	4,55 KB	2 bytes
22:17:16.872	https://xp.apple.com/report/2/xp_amp_appstore	POST	200	6,45 KB	2 bytes
22:15:43.050	https://xp.apple.com/report/2/xp_amp_appstore	POST	200	63,6 KB	2 bytes

Bypass VPN when using Apple Services

- Health
- Wallet
- Apple Music
- Apple TV
- Books
- iTunes
- Stocks

- Settings > Privacy & security > Location Services > Significant Locations

- Helpful <-> Harmful

Significant Locations

- Apps ask for tracking permission
- Prevents apps seeing IDFA

  Identifier for Advertisers

  Apple’s IDFA   Not their tracking Identifier

App Tracking Transparency

Others

- Wi-Fi MAC Address
- Ability to associate with other data
- MAC addresses are unique

  MOSTLY

- End-to-end encryption
- UNLESS a recipient is not an iPhone user
- Other messaging services to use Other encryptions

iMessage

- App store

Ads

Siri

- On-Device speech recognition
- Audio never (almost) never leaves device
- HOWEVER transcripts always do

Apple does not sell customer data

- BUT it can and does use customer data for Apple products

- ChromeOS 108.0.5359.75

  New Features

  Virtual Desk Save and/or close

  on-screen keyboard

  Critical Files   - Trash
- ChromeOS Chrome OS ChromeOS Flex

  Chrome OS previous name of ChromeOS

  ChromeOS only supported on

  Chromebook, Chromeboxes, Chromebases

  ChromeOS Flex devices PC, MAC, etc

ChromeOS

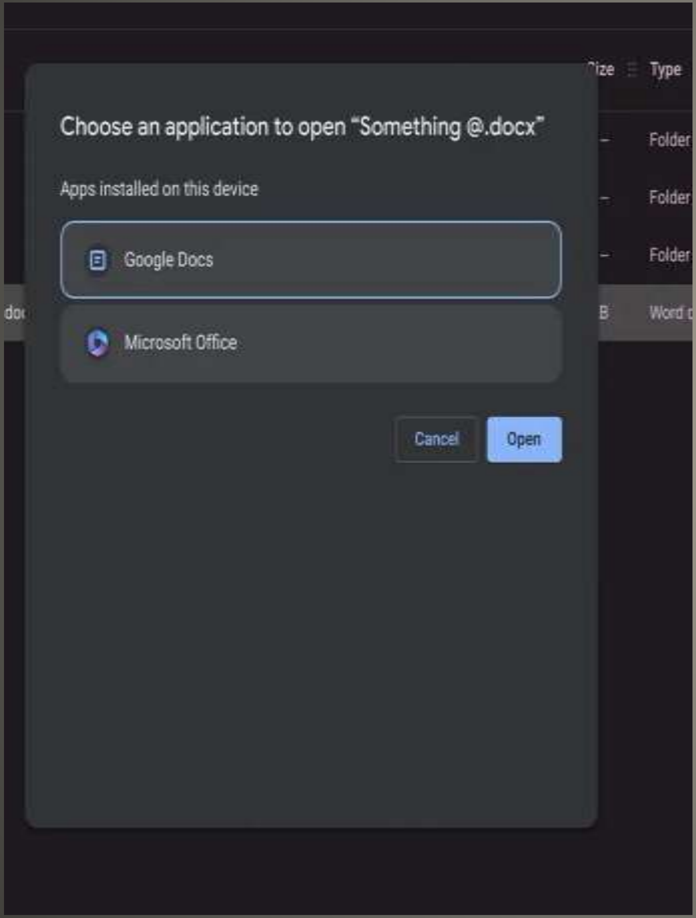
ChromeOS

- Verified boot & Google Security chip
- ChromeOS Flex support for UEFI
  Prevent ChromeOS Flex booting other OS
  With Secure Boot enabled
- Manage & auto update firmware
- TPM and full disk encryption
- ChromeOS Flex - no support Google Play
  no support Android apps
  no support Parallels Windows VM
  Varied support for Linux Development

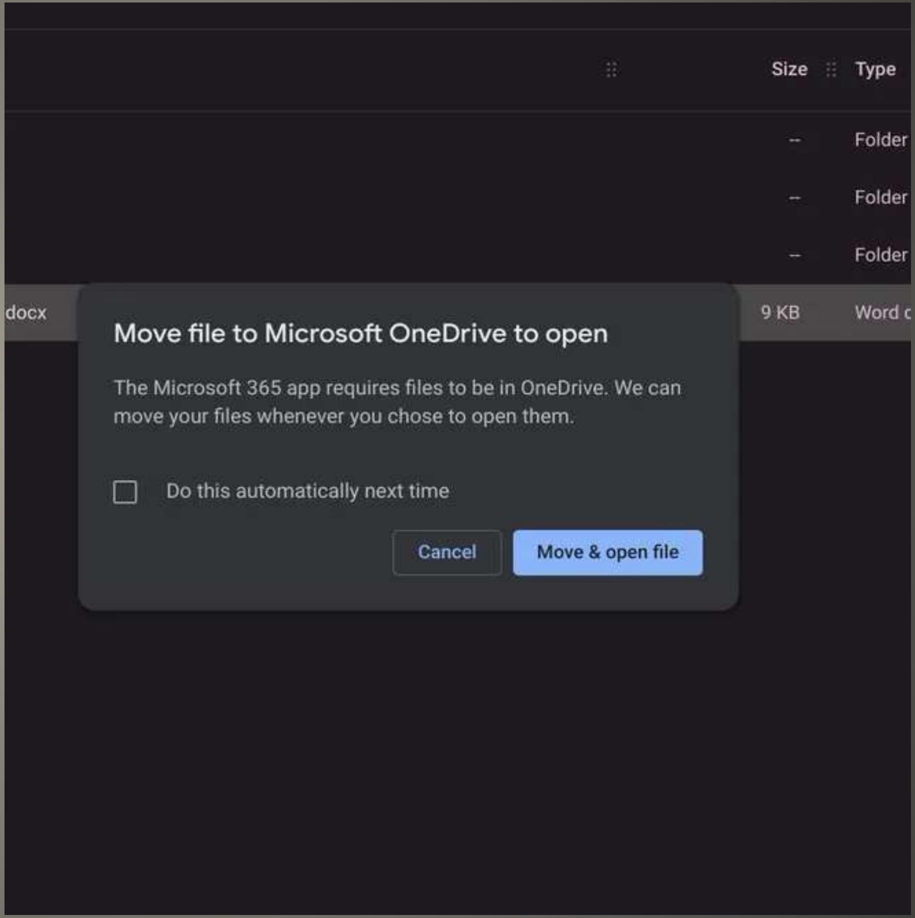
- Support for limited architectures & models
  - Intel or AMD
  - No ARM
  - Check certifications
- Different keyboard layouts, shortcuts
- Limited or no support
  - CD, DVD, biometrics, Thunderbolt, etc.
- Speed & Performance
- No zero-touch enrollment

ChromeOS Flex

- Native edit office files on Chromebook


Choose an application to open “Something @.docx”

Apps installed on this device


Move file to Microsoft OneDrive to open

The Microsoft 365 app requires files to be in OneDrive. We can move your files whenever you chose to open them.

☐ Do this automatically next time

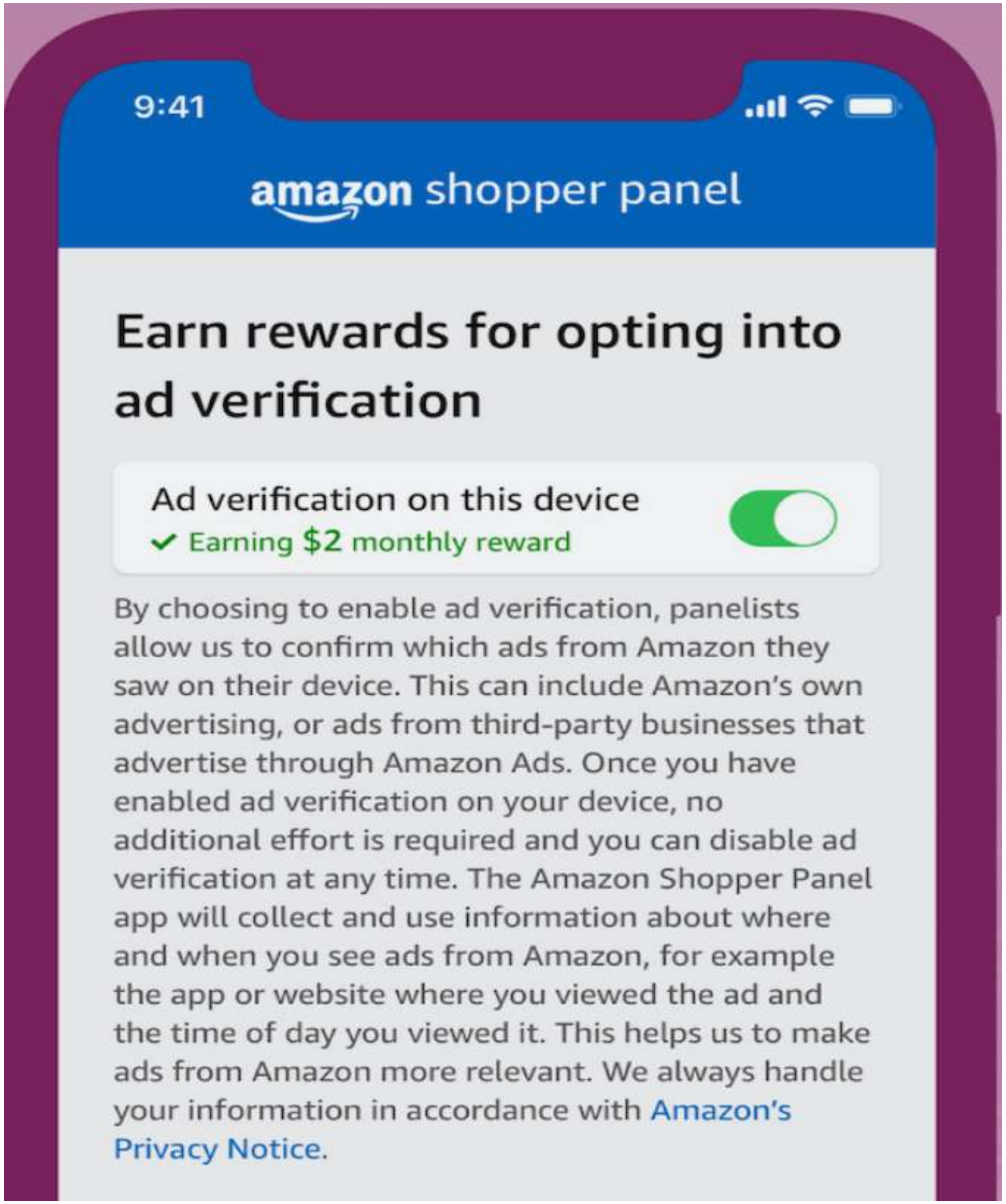
ChromeOS

- 1Passwpord
- Bitwarden
- DuckDuckGo support macOS browser
- PayPal

Passkeys

Amazon Ad Verification Program

- Google & Facebook tried
- Amazon Shopper Panel
- Opt-in $2/mo



Earn rewards for opting into ad verification

Ad verification on this device

✓ Earning $2 monthly reward

By choosing to enable ad verification, panelists allow us to confirm which ads from Amazon they saw on their device. This can include Amazon's own advertising, or ads from third-party businesses that advertise through Amazon Ads. Once you have enabled ad verification on your device, no additional effort is required and you can disable ad verification at any time. The Amazon Shopper Panel app will collect and use information about where and when you see ads from Amazon, for example the app or website where you viewed the ad and the time of day you viewed it. This helps us to make ads from Amazon more relevant. We always handle your information in accordance with Amazon's Privacy Notice.

- Improvement to GPT-3
- Chat with AI
- *Chat with AI*

  Written opinion piece for *The Guardian*

  Exam responses with full marks

  Coding challenges in obscure programming languages

  Writes limericks

  Refuse lawlessness

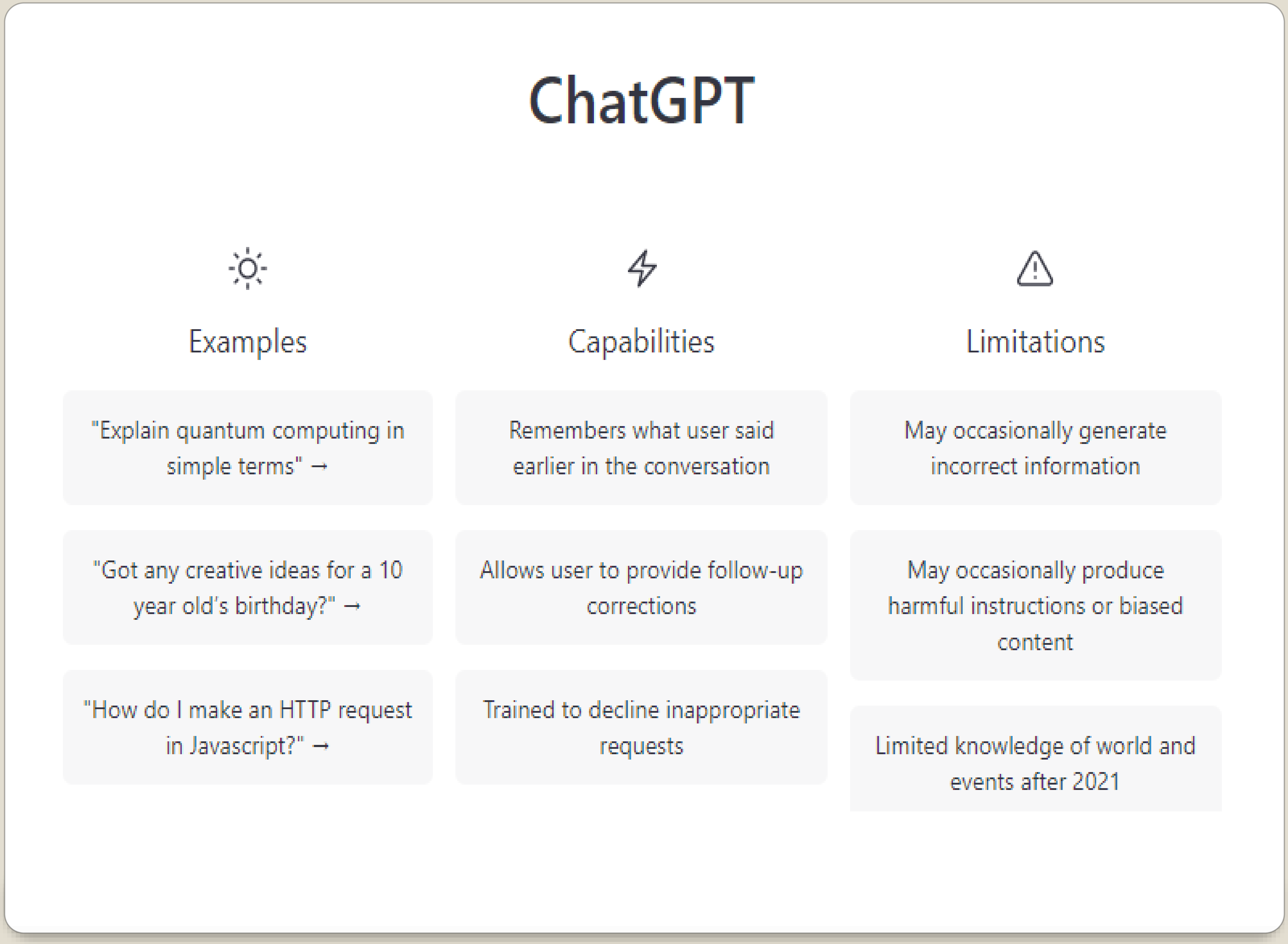
ChatGPT

- Lower costs

  Refunds, deals, disputes, etc.

  DoNotPay
- Diet Plan including meal planning, shopping lists, etc.
- Create bedtime stories, essays, research, etc.
- Create programming codes in many programming languages – Caution
- chat.openai.com

ChatGPT

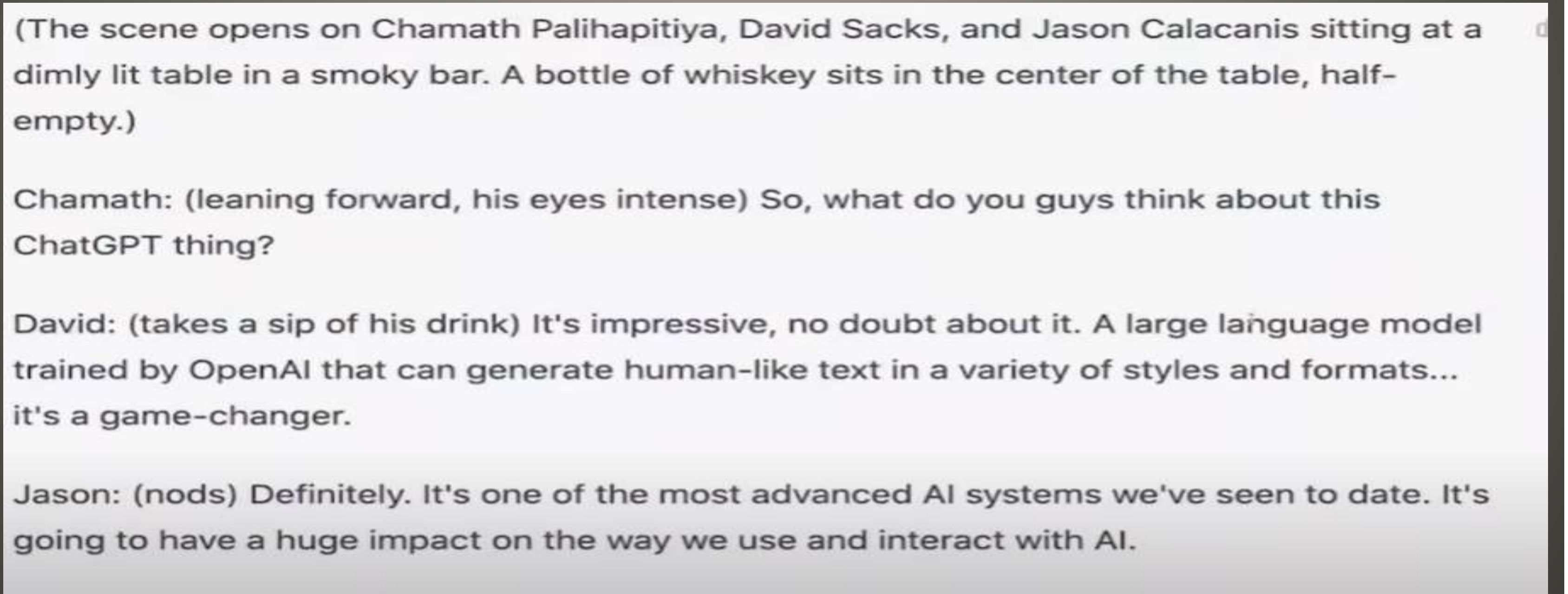


ChatGPT

Examples	Capabilities	Limitations
"Explain quantum computing in simple terms" →	Remembers what user said earlier in the conversation	May occasionally generate incorrect information
"Got any creative ideas for a 10 year old's birthday?" →	Allows user to provide follow-up corrections	May occasionally produce harmful instructions or biased content
"How do I make an HTTP request in Javascript?" →	Trained to decline inappropriate requests	Limited knowledge of world and events after 2021

- Write movie script with two characters describing AI with the style of Quinton Tarantino.

  PG dialog staging …



(The scene opens on Chamath Palihapitiya, David Sacks, and Jason Calacanis sitting at a dimly lit table in a smoky bar. A bottle of whiskey sits in the center of the table, half-empty.)

Chamath: (leaning forward, his eyes intense) So, what do you guys think about this ChatGPT thing?

David: (takes a sip of his drink) It's impressive, no doubt about it. A large language model trained by OpenAI that can generate human-like text in a variety of styles and formats... it's a game-changer.

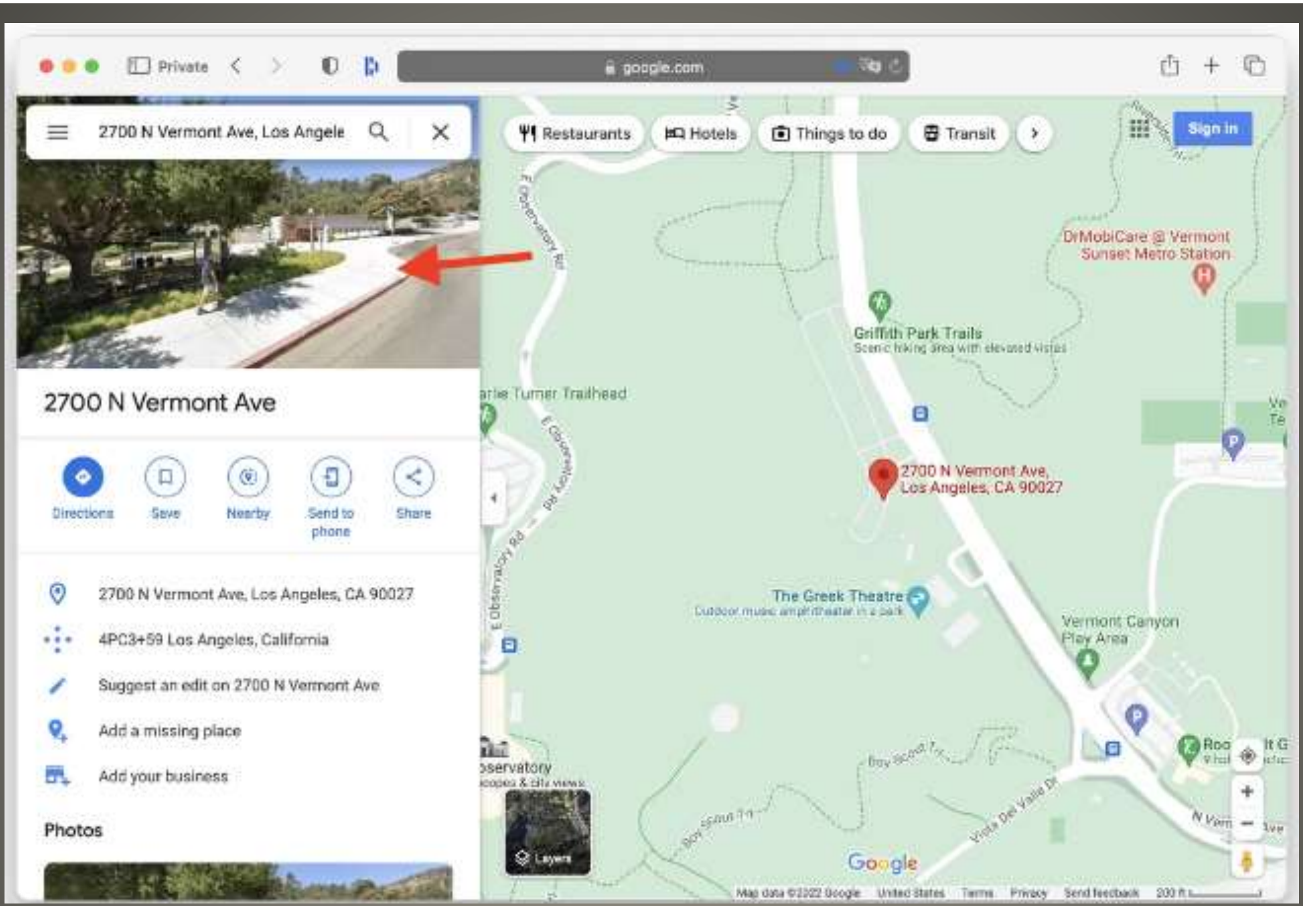
Jason: (nods) Definitely. It's one of the most advanced AI systems we've seen to date. It's going to have a huge impact on the way we use and interact with AI.

Example

- “Tell me why this JavaScript code generates an error”

- Only since 2021
- True & False

Example



Private
google.com
Restaurants
Hotels
Things to do
Transit
Sign in
DrMobiCare @ Vermont Sunset Metro Station
Griffith Park Trails
Scenic hiking area with elevated vistas
2700 N Vermont Ave, Los Angeles, CA 90027
The Greek Theatre
Outdoor music amphitheater in a park
Vermont Canyon Play Area
E Observatory Rd
Boy Scout Trl
Vista Del Valle Dr
Layers
Google
Map data ©2022 Google United States Terms Privacy Send feedback 200 ft
Directions
Save
Nearby
Send to phone
Share
Photos

2700 N Vermont Ave, Los Angele

2700 N Vermont Ave

2700 N Vermont Ave, Los Angeles, CA 90027

4PC3+59 Los Angeles, California

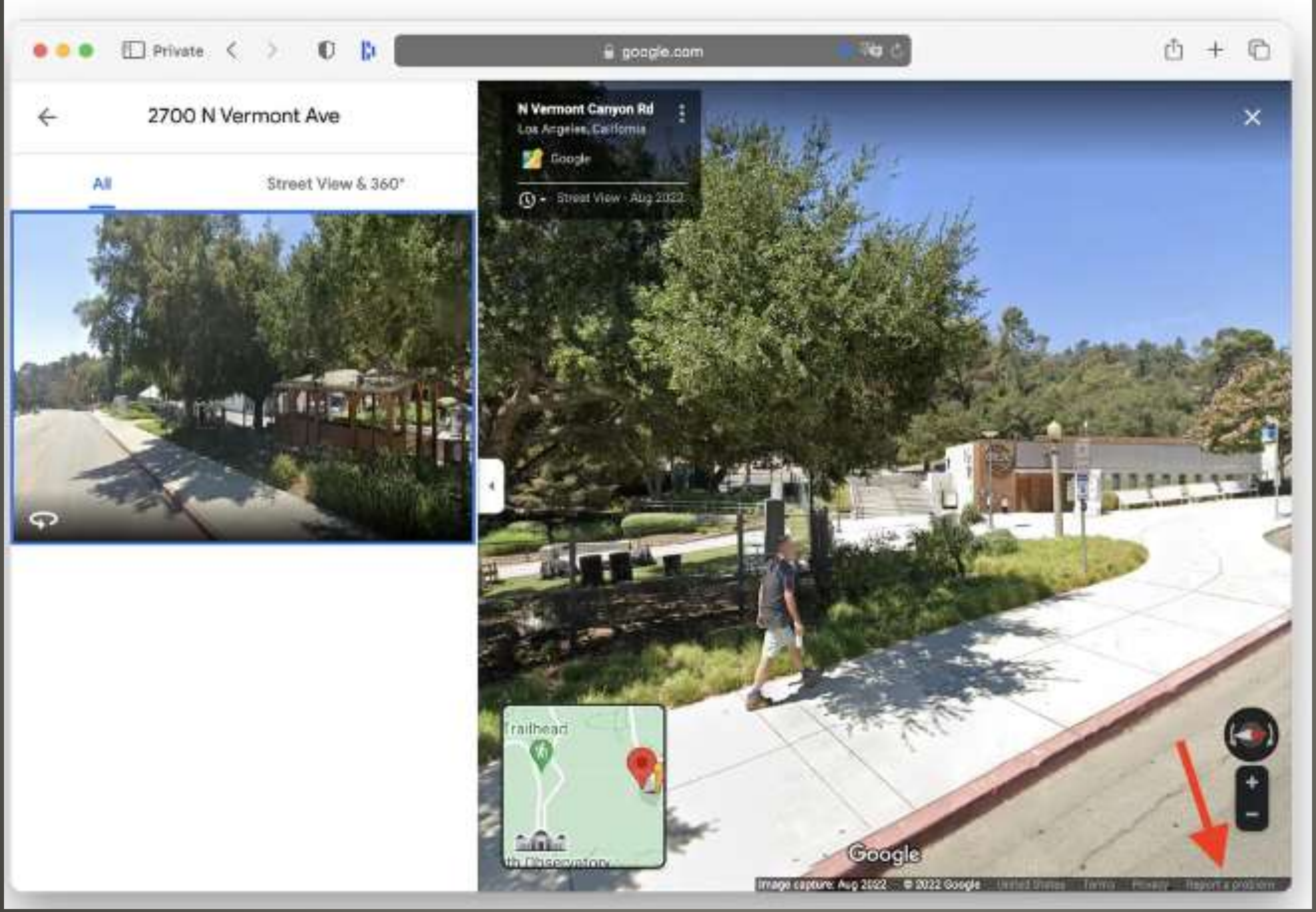
Suggest an edit on 2700 N Vermont Ave

Add a missing place

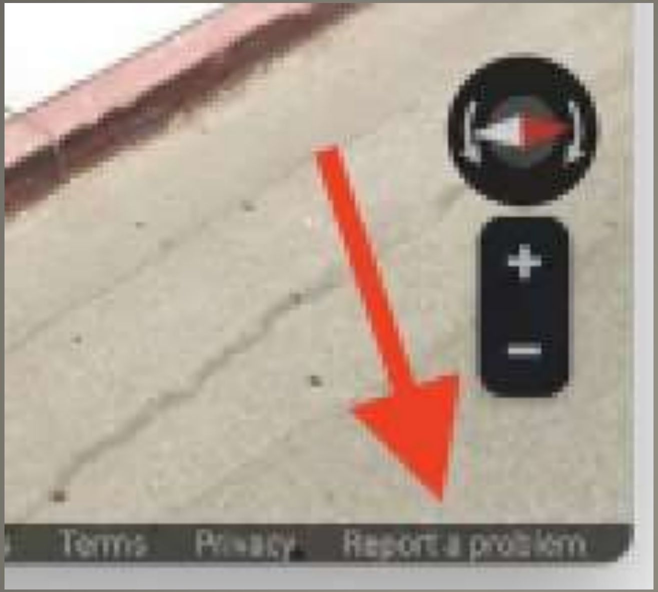
Add your business

Blur home in Google maps street view

- Report a Problem

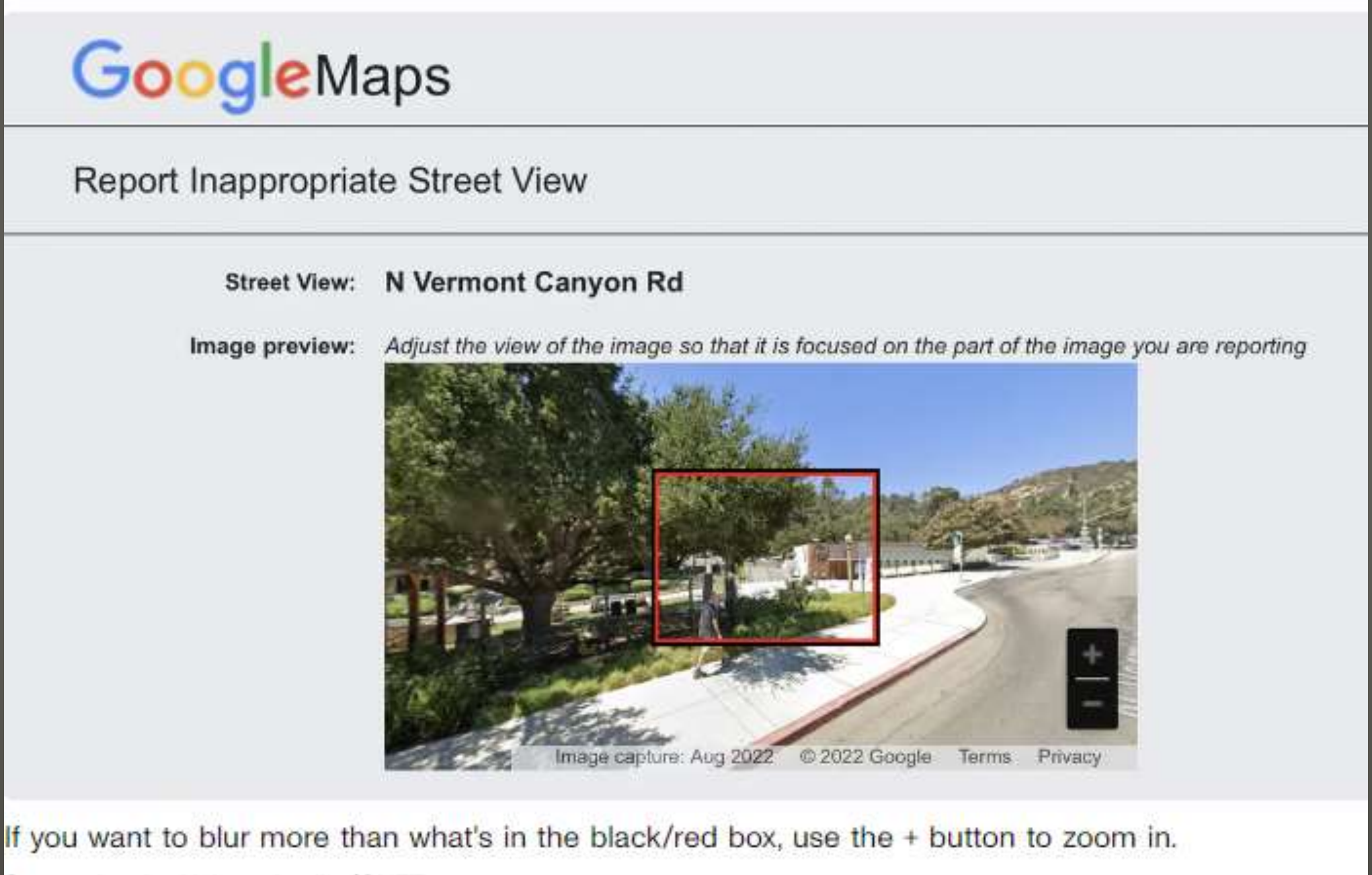


Blur home in Google maps street view



Report a problem

- Choose What to blur



Report Inappropriate Street View

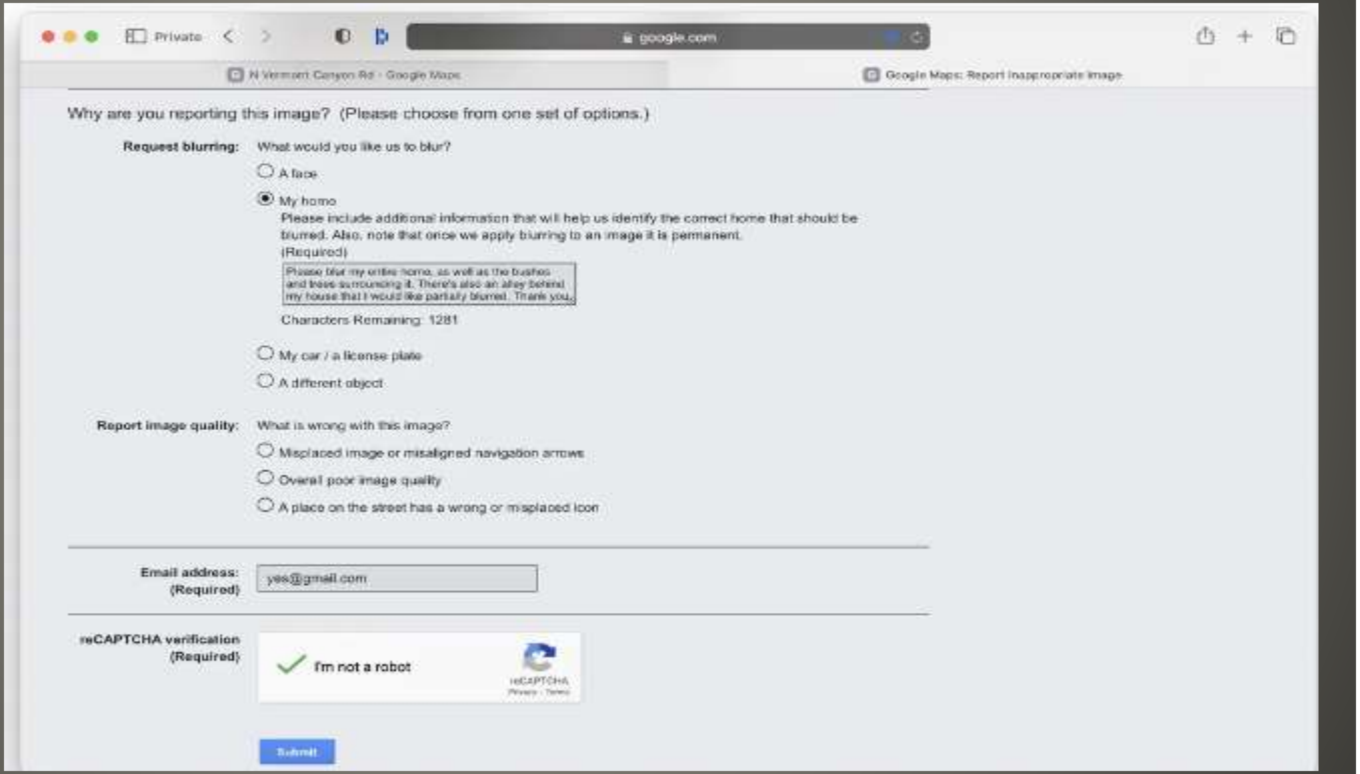
Street View: N Vermont Canyon Rd

Image preview: *Adjust the view of the image so that it is focused on the part of the image you are reporting*

If you want to blur more than what's in the black/red box, use the + button to zoom in.

Blur home in Google maps street view

- Why?
- Face, Home, Car, License plate, other
- Email


Private
google.com
N Vermont Canyon Rd - Google Maps
Google Maps: Report Inappropriate Image

Why are you reporting this image? (Please choose from one set of options.)

Request blurring: What would you like us to blur?

○ A face

● My home

Please include additional information that will help us identify the correct home that should be blurred. Also, note that once we apply blurring to an image it is permanent.
(Required)

Please blur my entire home, as well as the bushes and trees surrounding it. There's also an alley behind my house that I would like partially blurred. Thank you.

Characters Remaining: 1281

○ My car / a license plate

○ A different object

Report image quality: What is wrong with this image?

○ Misplaced image or misaligned navigation arrows

○ Overall poor image quality

○ A place on the street has a wrong or misplaced icon

Email address: (Required) yes@gmail.com

reCAPTCHA verification (Required)

✓ I'm not a robot

Blur home in Google maps street view

Blur home in Google maps street view

- Submit
- Clarification
- Wait
- Once blurred …
- What if you buy/sale that property?

- All the photos on real estate sites

- Passkey setup
- Two keys per site per device per account
- Device authorization On device
- Device Security
- Stored on device
- Encrypted on device
- Unique per

Passkey Setup

- iPhone & iPad

  Settings > Passwords > Password Options
  Autofill Passwords
  tap iCloud & Keychain
- Mac

  System Settings
  Your Apple Account
  Select iCloud
  toggle on Password & Keychain

Passkey Setup

- NYC Metropolitan Opera cyber attack
- Official Vatican website DDoS

After Pope’s condemnation of Ukraine invasion

- South Dakota bans TikTok
  then Maryland, South Carolina, Texas
  Governor Abbott state employees’ personal devices
  Indiana AG sues TikTok
- Iran & Albania IT staff charged
- Anker Eufy IoT Security Camera
  Privacy lie
- Yet another Uber breach
  Employee & Company data
  Third party AWS cloud server

Current Issues

- Users subscribe

Phone Number, email, third party account
Content discovery using AI
Follow accounts
Like, Share, give hearts, gifts, comments
Challenges, Cringe, Reactions, etc.

Info collected:

Which video, how long, entire contents of any messages, country, IP address, type of device

With user’s permission:

Exact location, device’s contacts & connections, age, phone number, payment information

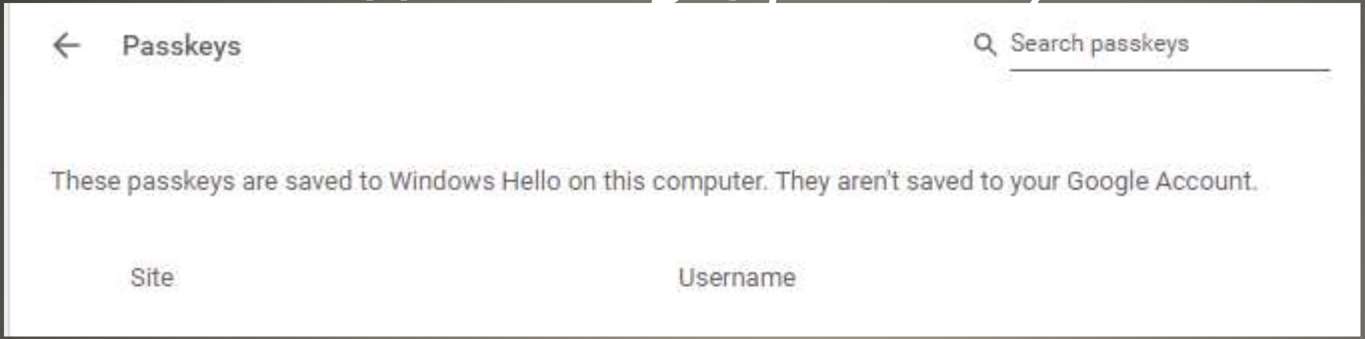
App permissions: Microphone & Camera
Thus biometric data
Data is encoded – thwart hacking?

What is TikTok?

Chrome passkeys

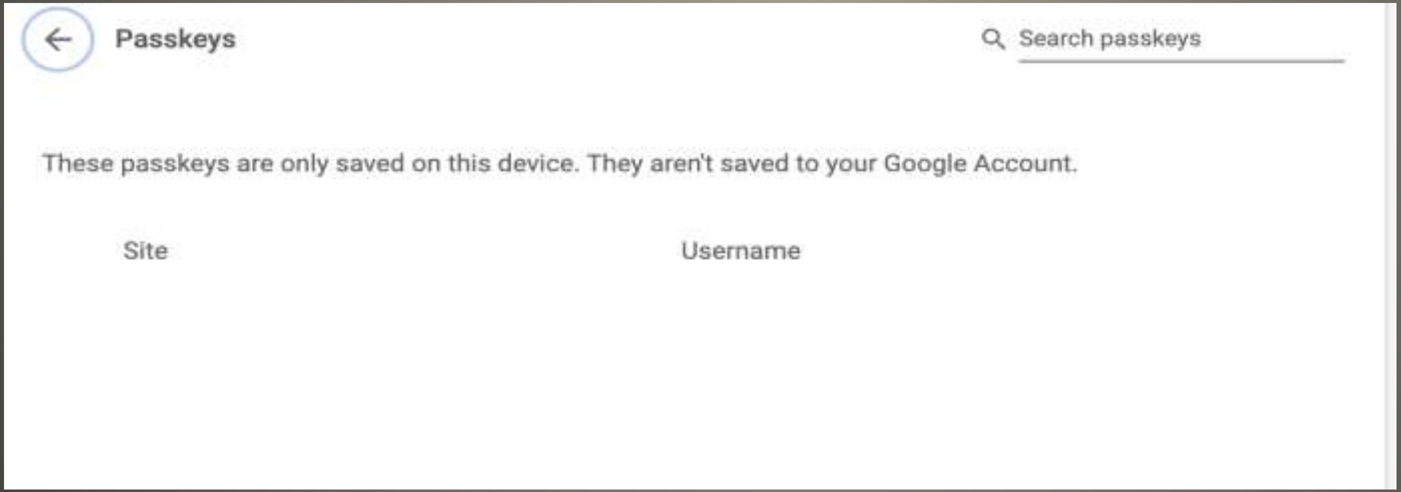
- Latest update 108.0.5359.125
  Windows 11, macOS, Android
  Android Google Password Manager
  Requires portable device
  Bluetooth for proximity
  passkeys stored in local device
  iOS Keychain
  Google Password Manager Android
  Windows 11 Windows Hello
  Not yet - ChromeOS

- *chrome://settings/passkeys*



These passkeys are saved to Windows Hello on this computer. They aren't saved to your Google Account.

Site	Username



These passkeys are only saved on this device. They aren't saved to your Google Account.

Site	Username

Chrome passkeys

Passkeys

- Passwords – phished, stolen, cracked
- Passkeys – nothing to guess, crack, stolen
- Passkey stored on device
- Access via biometrics

  FaceID, fingerprint, Windows Hello, PIN
- Asymmetric key pair device site
- Site with stored credentials -> device private key from secure key store
- 1Password passkey directory page

- Chrome needs password saving & synching
- Create new ID on supported site
- Save site as passkey?
- Mobile device screen lock as passkey?

- Visit site
- Select device to authenticate
- Bluetooth required

Android example Chrome

- Statscard

NFC Card with Cryptocurrency

- NOT Legal Advice !!
- 1099-K reporting deadline 31-Jan
- Third party payment networks
  - Venmo, PayPal
  - Part-time work
  - Side Jobs
  - Selling goods
- Was 200 transactions aggregate above $20,000
- Now $600

Federal Tax

- Medibank
  Australia’s largest medical insurer
  10 million past & present clients
  Reboot
  $15M ransom
  $35M recovery costs – so far

  Lesson, reimage to better assure

- Telegram – no SIM? No problem
  Buy & sell usernames via auction
  Fragment
- US seized 48 websites offering cyber-attack-for-hire

Current Issues

- FBI InfraGard info sharing network hacked
- Skype real-time translations Imitate your voice

Current Issues

- 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