

PRESCOTT MAC USERS GROUP

# APPLE SECURITY ALPHA TO OMEGA

1

Alpha - the beginning  
Omega - the end

## APPLE BUILT IN DEFENSES



- Malware defense structured in three layers:
  - Prevent launch or execution of malware via App store or Gatekeeper with Notarization
  - Block malware from running using Gatekeeper, Notarization and XProtect
  - Remediate malware that tries executing using XProtect
  - System Integrity Protection designed to prevent potentially malicious software from modifying protected files and folders on your Mac

2

Remember: layers are best. So, that is what Apple created for you.

Apple began to include rudimentary anti-malware protections with macOS versions with Snow Leopard in 2009. Called “XProtect,” this system service downloaded and installed new malware definitions in the background in between major macOS security updates, mostly to protect against the installation of known, in-the-wild malware.

Since then, Apple has added multiple anti-malware features to macOS, though they’re not always branded that way. Gatekeeper, app notarization, System Integrity Protection, the Signed System Volume, and access controls for hardware and software are all, one way or another, about proactively protecting system files from being tampered with and making sure that installed apps do what they say they’re doing. Another under-the-hood tool, the Malware Removal Tool (MRT), acts more like a traditional anti-malware scanner, periodically receiving definitions updates from Apple so that it could scan for and remove malware already present on your system.

## APPLE BUILT IN DEFENSES

- Gatekeeper - inhibit the distribution of malware by checking each App at the App store
- Notarization - malware scanning service for non-App store distributions for developers
- XProtect - built-in antivirus technology for signature-based detection and removal of malware
- <https://www.apple.com/macOS/security/>



3

See Apple Platform Security at <https://www.apple.com/macOS/security/> for full discussion

## APPLE BUILT IN DEFENSES

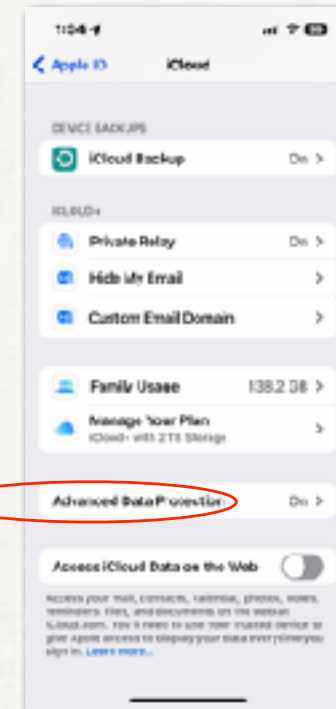
- Recovery Key - MacOS - Prevents password change without the key or another device logged into iCloud
- Download ALL Security Updates to software - MacOS & iOS
- TouchID - MacOS & iOS - Disabled after:
  - 5 incorrect attempts or
  - 48 hours of a device not being unlocked or
  - Not entering password/code to unlock for 156 hours

4

Every fingerprint is unique, so it's rare that even a small section of two separate fingerprints are alike enough to register as a match for Touch ID. The probability of this happening is 1 in 50,000 with a single, enrolled finger. And Touch ID allows only five unsuccessful fingerprint match attempts before you must enter your password. By comparison, the odds of guessing a typical 4-digit passcode are 1 in 10,000. Although some codes, like "1234," might be more easily guessed, there is no such thing as an easily guessable fingerprint pattern.

## APPLE BUILT IN DEFENSES

- Advanced Data Protection
- Requires MacOS Ventura 13.2, iOS 16.2, iPadOS 16.2 and latest software on HomePod and Apple TV
- ALL DEVICES must be up to date to turn on
- Only user's trusted devices retain access to encryption keys

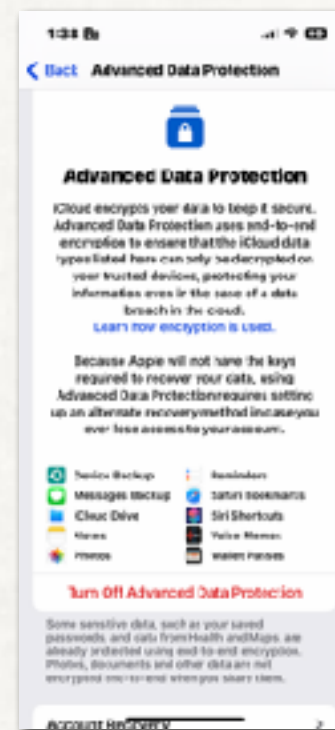


5

Trusted device: Mac, iPad, iPhone. ALL MUST BE logged into the same iCloud account. For example, I have three emails that all point to the same EXACT email address at apple abcdef@mac.com, abcdef@me.com, and abcdef@icloud.com. I MUST use the same AppleID for every device for it to work. In other words, using me.com on one, and mac.com on another DOES NOT WORK!!!

## APPLE BUILT IN DEFENSES

- Advanced Data Protection for iCloud
- End-to-end encryption for majority of iCloud data
- Mail & Contacts not encrypted
- Sets up account recovery method THAT YOU MUST REMEMBER!!



6

This new feature increases the types of data that will be end-to-end encrypted by Apple, meaning that when data is stored on iCloud, it cannot be accessed in a data breach, or by Apple itself when requested by a government or even the user. Advanced Data Protection was launched in the United States last year, but with this iOS update, it will be available to everyone globally. Some types of data already were end-to-end encrypted, like your health data, but this feature adds device backups, messages backups, iCloud Drive, notes and photos. (Your Mail and Contacts app data is not included.)

If there is a cloud breach, the criminals would not be able to access the majority of the data you have stored there. It also prevents Apple from being forced to hand over iCloud data like backups of Messages conversations when requested by governments or law enforcement, since the company has no way to access that information.

Advanced Data Protection is more of a defense against big breaches.

Make sure you are running iOS 16.3 and then go to Settings>Your account >iCloud> Advanced Data Protection. Make sure you set up Account Recovery here. It lets you add a recovery contact (a family member, for example) and get a 28-character recovery key. These will help you get access to your account if something happens. Then, go back and tap to turn on Advanced Data Protection.

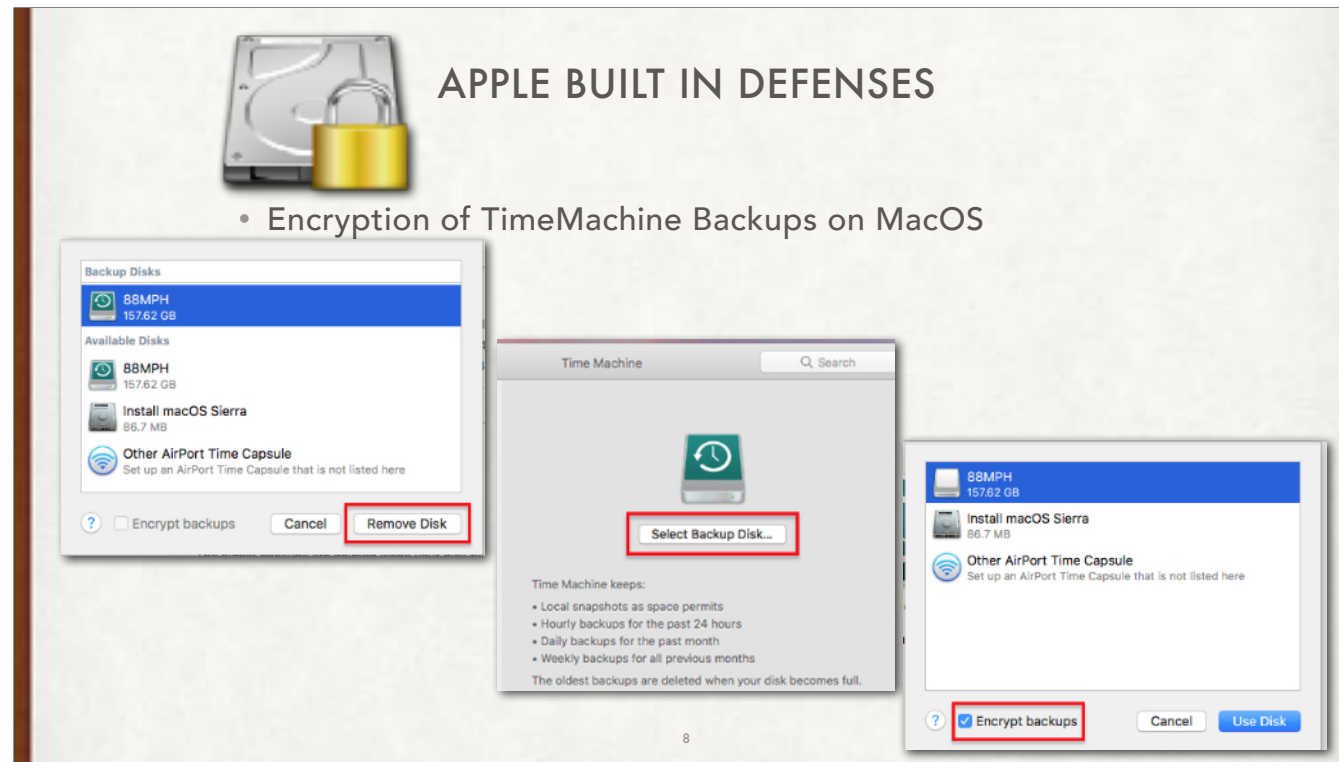
Who it's for: Everyone can turn this feature on for added peace of mind, but you should be prepared for an increased amount of responsibility. If you lose access to your devices and your recovery options, Apple has no way of accessing your data for you. However, there won't be any day-to-day differences that you notice as an iPhone user.



## APPLE BUILT IN DEFENSES

- Encryption of iOS backups on MacOS
- Encryption of TimeMachine Backups on MacOS
- Encryption of main disk using FileVault on MacOS
- Apple Pay - MacOS & iOS - merchant NEVER sees the credit card number





Go to System Settings>General>TimeMachine. Select the disk, then click “Remove Disk” (don’t worry, you data is still there!)  
Click the “Select Backup Disk”, click on your old backup disk, then check the “Encrypt Backups” option. Enter a password and a hint (required)





## APPLE BUILT IN DEFENSES

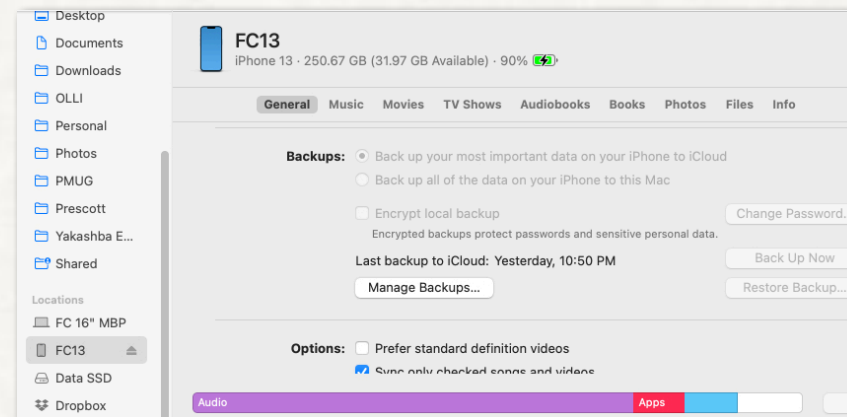
- Encryption of main disk using FileVault on MacOS - NOT RECOMMENDED!!!
- Used ONLY IF you have "Top Secret, Eyes Only" data
- System Settings>Privacy & Security, scroll to bottom





## APPLE BUILT IN DEFENSES

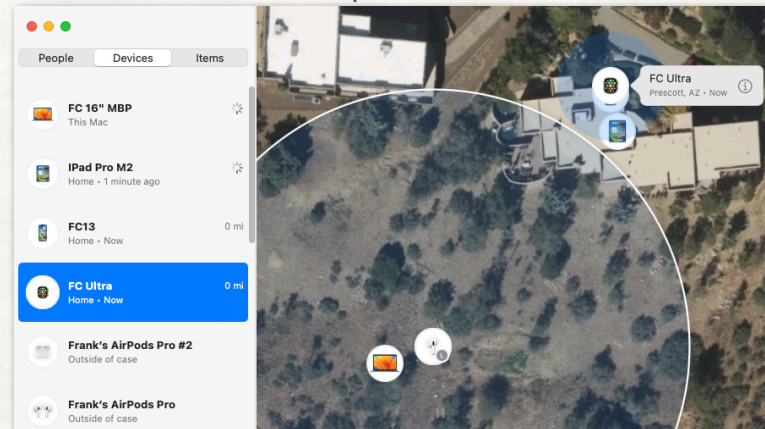
- Encryption of iOS backups on MacOS



When you select on your iPhone Settings/AppleID/iCloud Backup and turn off “Back Up This iPhone” to iCloud, then when you plug your phone into your Mac, you see it in “Locations” in the Finder Sidebar. You will be able to select “Encrypt local backup” on your Mac.

## MAC SECURITY

- Physical security of devices - Lock your home!
- Turn on "Find My" on all devices
- General location except for devices with Cellular chip



On your Mac, choose Apple menu > System Settings, then click [your name] at the top of the sidebar. If you don't see your name, click Sign in with your Apple ID to enter your Apple ID or to create one.

Click iCloud on the right.

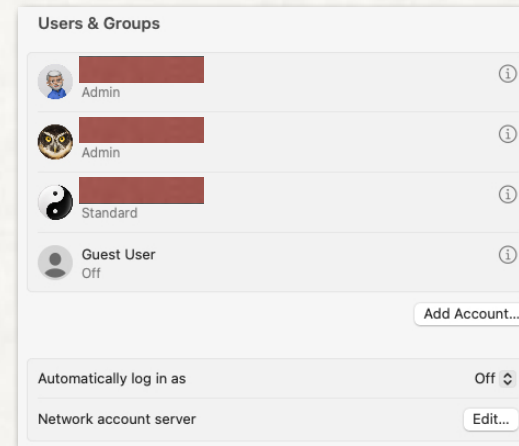
Click Find My Mac, click Turn On, then click Allow when asked to allow Find My Mac to use the location of your Mac.

Click Done.

If the Find My icon in iCloud settings has a warning badge, make sure you turned on Location Services and Find My in Privacy & Security settings.

## MAC SECURITY

- Starts with Accounts - create one Admin account, and one standard that you use - Settings>Users & Groups
- Create unique usernames and long passwords
- Turn OFF Automatic log in!



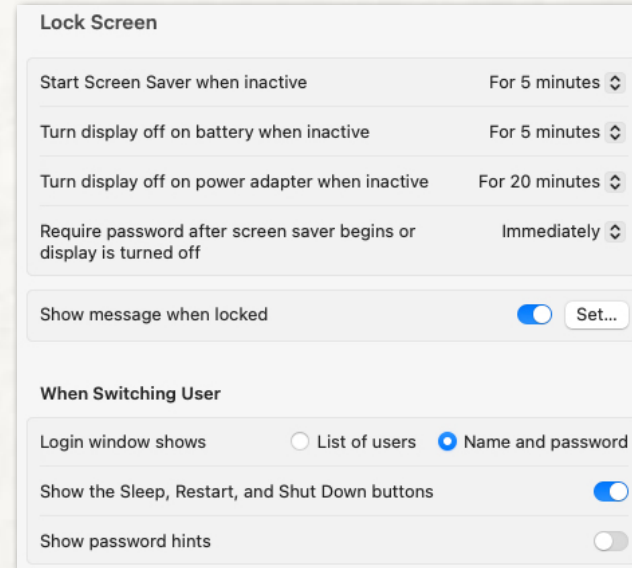
12

If the account you use regularly and are logged into has Admin privileges, then if someone steals the computer, they can change all the passwords and you will never get back in if your computer is recovered. They can also turn off Find My!!

NEVER have “Automatically log in as” On on a laptop that you carry.

## MAC SECURITY

- Turn Off automatic login: Settings>Users & Groups> Automatic login OFF
- Start Screen Saver ??
- Require Password IMMEDIATELY
- Require Name & Password on log in

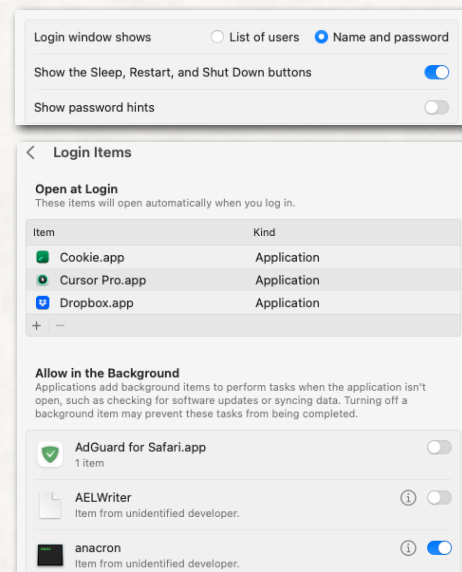


Start the screen saver very quickly: 1 minute in public places, maybe 5 minutes at home.

Require password IMMEDIATELY

You should always have to type in your user name and password. If you give them a list, then they only have to guess at one thing (password) instead of two (user name AND password)...

## MAC SECURITY



- Show Name & Password in login window: Settings>Lock Screen>Login window shows
- Regularly review Login Items Allowed in Background - Settings>General>Login Items

14

Login Items Allowed in Background - Settings>General>Login Items

Apple has “opened the kimono” as the saying goes showing ALL the login items now in Settings. DO NOT turn off unless you are positive it refers to a deleted software program!!

## MAC SECURITY

- Load & use Virus protection - Sophos recommended, but many other good ones
- Load & use Malware protection - Malwarebytes
- Upgrade computer to one with T2 Chip (Intel based computers). All M1+ computers have it for TouchID



15

Ask: who has an anti-virus, and if not, why not??

Ask: who has Malwarebytes, and if not, why not??

Ask: who has a 2018 computer or later (when T2 chip was released)

You can also use System Information to learn whether your Mac has this chip:

Press and hold the Option key while choosing Apple menu  > System Information.

In the sidebar, select either Controller or iBridge, depending on the version of macOS in use.

If you see "Apple T2 chip" on the right, your Mac has the Apple T2 Security Chip.

## MAC SECURITY

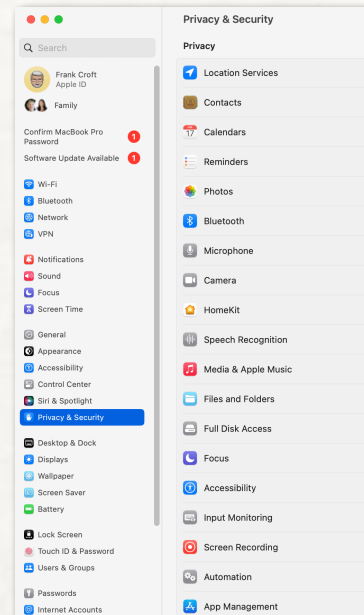
- Review Access to Mac hardware and software regularly
- Settings>Privacy and Security
- Controls access to all hardware on your computer
- Controls access to some software on your computer
- Controls access to files & folders on your computer

Access to hardware - Settings>Privacy & Security>Microphone;Camera;HomeKit;Files and Folders;Full Disk Access; et. al.

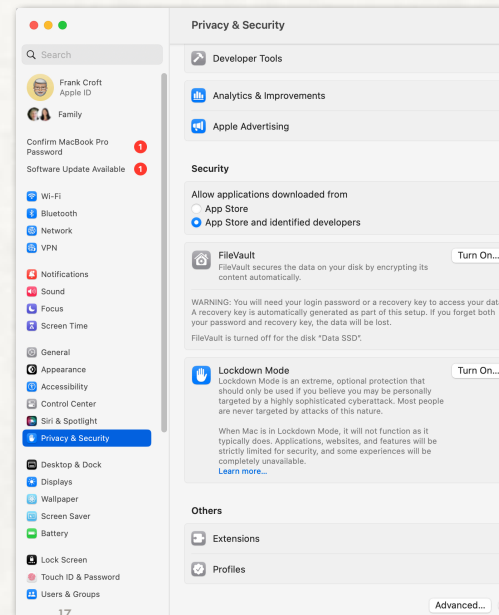


## MAC SECURITY SETTINGS> PRIVACY & SECURITY

Top Half



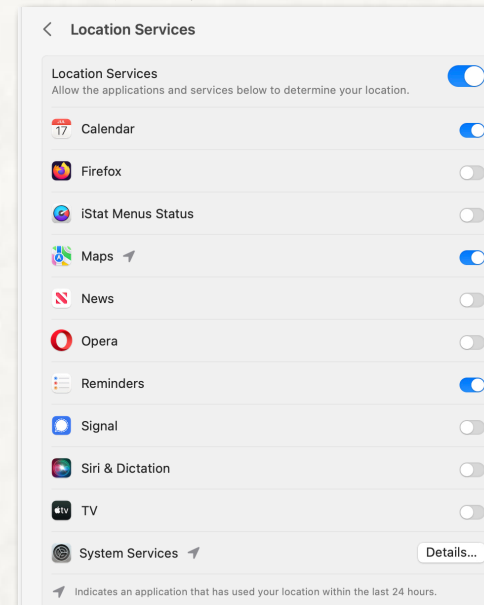
Bottom Half



Access to hardware - Settings>Privacy & Security>Location Services;Microphone;Camera;HomeKit;Files and Folders;Fill Disk Access; et. al.

## MAC SECURITY: SETTINGS> PRIVACY & SECURITY>LOCATION SERVICES

- Turn on/off using common sense
- Why does an App need your location??
- Does it need a precise or general location?

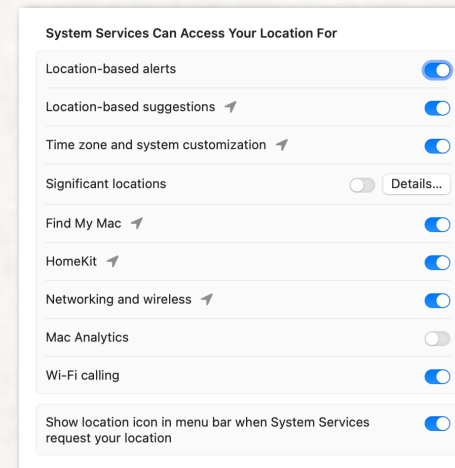


So, look at each entry, and you decide, based on how you use that app, whether it needs access to your location. For example, why does any browser need my location? Maps would in order to give me correct directions

At the bottom, note System Services and the Details button - next slide

## MAC SECURITY: SETTINGS> PRIVACY & SECURITY>LOCATION SERVICES

- System Services Details
- Pay attention to arrow icon
- Arrow indicates your location has been recently used by this app
- Many depend on movement of your Mac

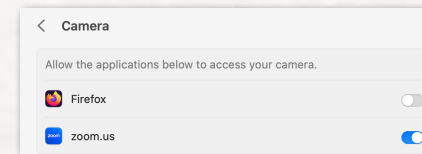
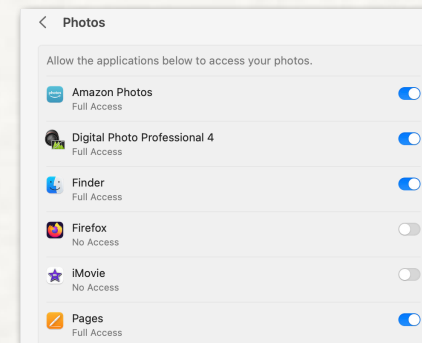


19

If you move your laptop a lot, do you want Apple to know where you have been and store it?? That is why I have Significant locations turned off!!

## MAC SECURITY: SETTINGS> PRIVACY & SECURITY

- Apps & Hardware Access - Review each one!!
- Controls Apple's "Sandboxing" - restrictions



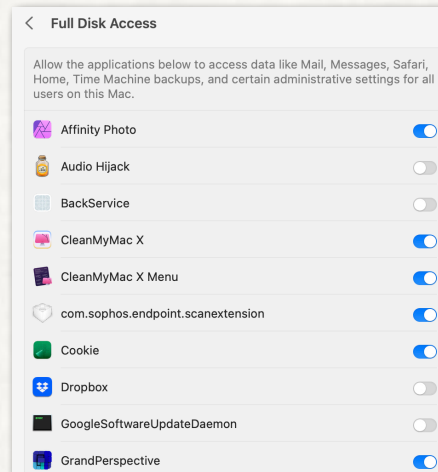
20

Firefox does not need the Microphone, but Shazam does in order to hear what is playing!!

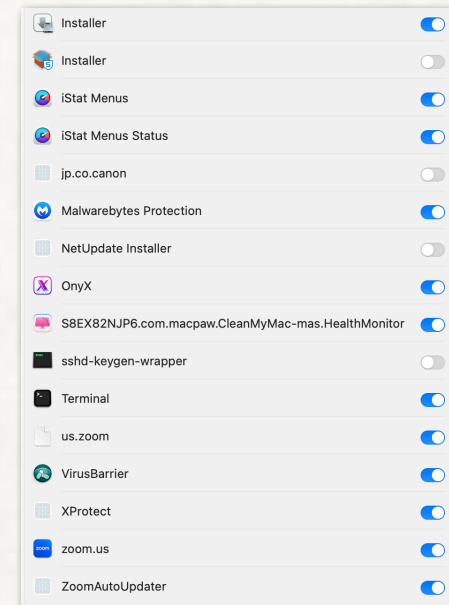
Be VERY CAREFUL about both the Microphone and Camera access!!! Many apps automatically turn on access when the app is installed to collect and sell data about you.

## MAC SECURITY: SETTINGS> PRIVACY & SECURITY

### • Full Disk Access



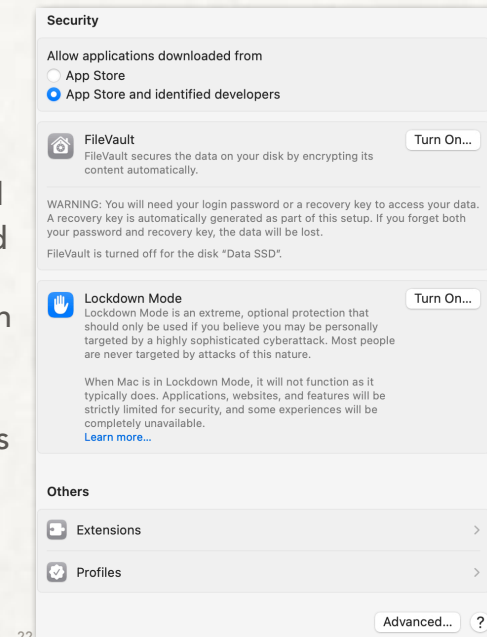
21



If you don't know if an App needs full disk access, ask someone. Join PMUG to get expert advice. If you turn off access and the App needs access, the App may not work correctly if at all

## MAC SECURITY: SETTINGS> PRIVACY & SECURITY

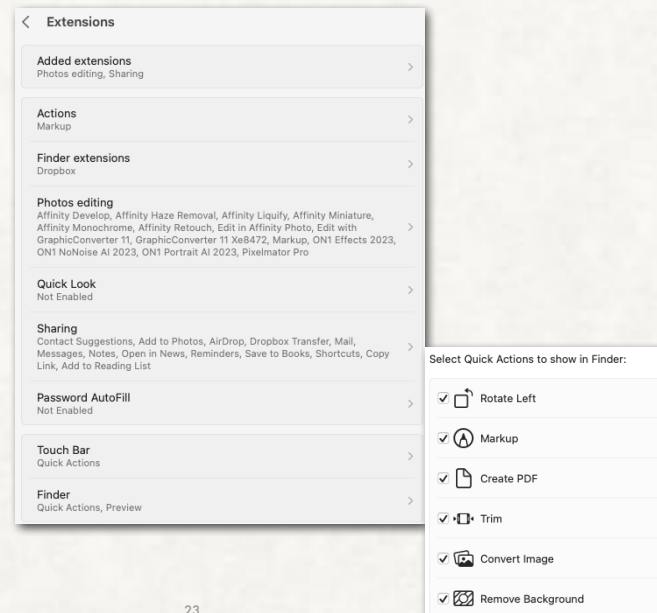
- Security - scroll to bottom
- FileVault - ONLY in special cases; NOT recommended
- Lockdown Mode - ONLY in special cases
- Ignore Extensions, Profiles and Advanced



Apple recently added an option called Lockdown Mode specifically for its most high-risk, high-profile iPhone users. It limits a variety of apps and features to minimize ways that outside attackers could compromise your device, specifically through vulnerabilities Apple itself hasn't discovered yet. Do not use this unless you have legitimate reasons to be worried about targeted attacks and your devices' security, as the setting comes with some big trade-offs. For example, it blocks many message attachments, and some websites may not work.

## MAC SECURITY: SETTINGS> PRIVACY & SECURITY

- Extensions
- Set by default
- Generally editing not needed



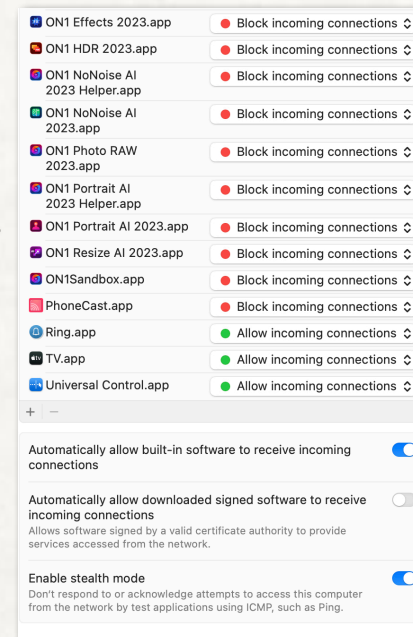
23

Use Extensions settings to enable and disable Apple and third-party extensions for your Mac, and select extensions to include in the Share menu. Extensions, such as Markup, add extra functionality to apps, the Finder, and the Touch Bar.

Generally ignore them unless you REALLY know what you need to do based on information from an App that uses them!!

## MAC SECURITY

- System Settings> Network>Firewall
- Turn on Firewall
- Click on Options and turn off “incoming connections” for unimportant Apps
- Review regularly
- Scroll to bottom and turn on first and last options



24

A firewall can protect your Mac from unwanted contact initiated by other computers when you're connected to the internet or a network. However, your Mac can still allow access through the firewall for some services and apps. For example:

If you turn on a sharing service, such as file sharing, macOS opens a specific port for the service to communicate through.

An app or service on another system can request and be given access through the firewall, or it might have a trusted certificate and therefore be allowed access.

For greater control, you can select apps and services, and specify whether they can have access through the firewall

Prevent incoming connections (Block) to nonessential services and apps. Basic internet services are a set of apps that allow your Mac to find services provided by other computers on the network. This setting prevents connections to all other sharing services.



## MAC SECURITY PASSWORDS

- System Settings>Passwords
- Password Options>AutoFill Passwords On>Allow filling from: iCloud Keychain and/or Password Manager
- Consider removing Bank, Savings, Credit Card passwords from Keychain since a stolen unlocked iPhone uses same Keychain!!
- 

1. Password	11. caseball	21. 656121
2. 123456	12. 111111	22. superman
3. 234567	13. 123456	23. qazwsx
4. 123456	14. 123456	24. 123456
5. 123456	15. 123456	25. 123456
6. 123456	16. 123456	26. 123456
7. 123456	17. 123456	27. 123456
8. 123456	18. 123456	28. 123456
9. 123456	19. 123456	29. 123456
10. dragon	20. 123456	30. 123456

A

**aaajustanotherfakewebsite.edu**  
Last modified today

User Name

joeblow@AAAJustanotherfakewebsite.edu

Password

canyouseethis123!@#

Change Password on Website

25

macOS uses keychains to help you keep track of and protect the passwords, account numbers, and other confidential information you use every day on your Mac computers and iOS and iPadOS devices.

You can use the Keychain Access app on your Mac to view and manage your keychains. When you use iCloud Keychain, you can keep your passwords and other secure information updated across your devices.

When you access a website, email account, network server, or other password-protected item, you can choose to save the password in your keychain so you don't have to remember or enter the password each time.

Can access same passwords using Finder>Applications>Utilities>Keychain Access.app - contains raw data. when you click on an account, have to check box "Show password" then enter Keychain password (usually login password for your computer)

## MAC SECURITY PASSWORDS

- Security Recommendations - Turn on “Detect Leaked Passwords
- High Priority Recommendations - Review regularly
- Other Recommendations - Review
- List of all passwords by their web site & username

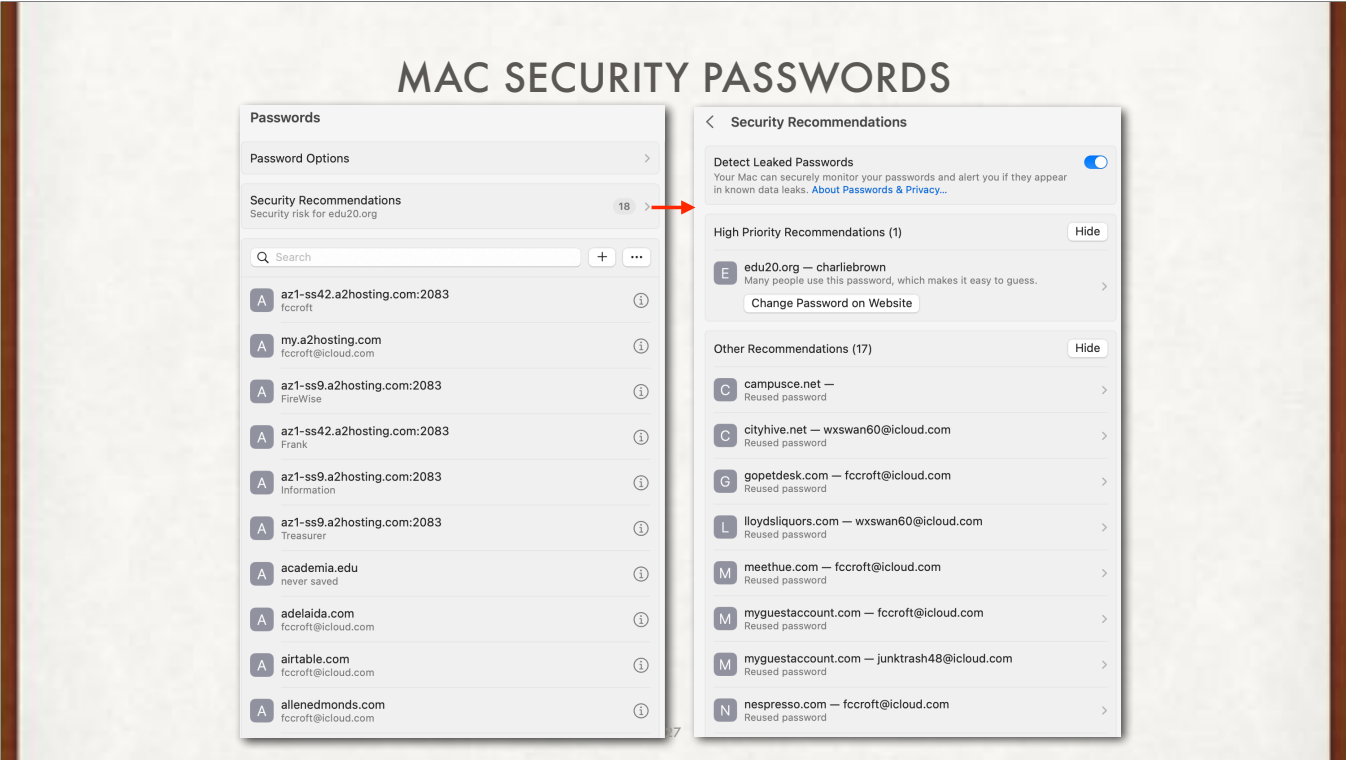
26

macOS uses keychains to help you keep track of and protect the passwords, account numbers, and other confidential information you use every day on your Mac computers and iOS and iPadOS devices.

You can use the Keychain Access app on your Mac to view and manage your keychains. When you use iCloud Keychain, you can keep your passwords and other secure information updated across your devices.

When you access a website, email account, network server, or other password-protected item, you can choose to save the password in your keychain so you don't have to remember or enter the password each time.

Can access same passwords using Finder>Applications>Utilities>Keychain Access.app - contains raw data. when you click on an account, have to check box “Show password” then enter Keychain password (usually login password for your computer)



Check for duplicates in the other recommendations since the software will not know which password to use!!

## BROWSER SECURITY

- Always have two browsers on your computer AND iPhone/iPad (Safari and Firefox/Opera)
- One browser used exclusively for your secure connections (banking, shopping, trusted sites, etc)
- Other browser accepts/stores no cookies, personal information, etc, used in Private Mode, and used to check out strange or unknown links or just surf
- Chrome and Yandex browsers should NEVER be used



28

Why stay away from Chrome? Chrome collects and stores all your searches and sites, and merges them with all the other information that Alphabet collects (Google search engine, Youtube, Fitbit, looker, Next, Waze, double-click, etc).

Why stay away from Yandex? Russian owned and operated. Ties to many of the Russian hackers.

## BROWSER SECURITY



- Use an anti-virus program that scans downloads in real time
- The more information Google/Facebook collects and sells, the higher chance of it being sold to a cracker/hacker
- They want your data so they can do the following:
  - Data ransom
  - Identity theft
  - Stealing infrastructure
  - Getting corporate information
  - Just because they can...



29

Though data breaches can be a national security threat, 86% are about money, and 55% are committed by organized criminal groups, according to Verizon's annual data breach report. Stolen data often ends up being sold online on the dark web. Buyers can purchase the data they are interested in.

Buyers use stolen data in several ways.

Open a new credit card or loan.

Change a billing address so you will no longer receive the bills.

Open new utilities accounts in your name.

Obtain a mobile phone.

Open a bank account and writing bad checks.

Use your debit card number to withdraw funds.

Obtain a new driver's license or ID.

Use your information in the event of an arrest or court action.

## BROWSER SECURITY



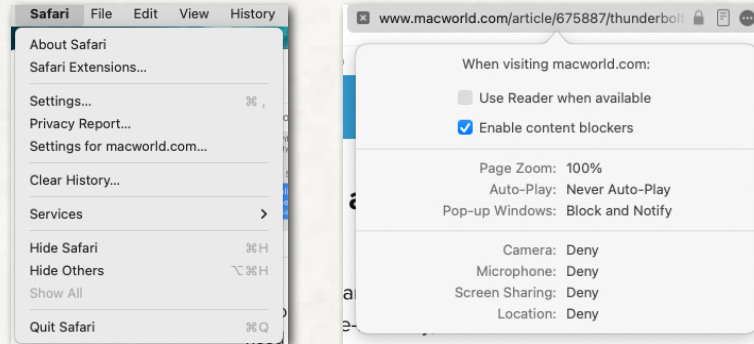
- Buyers of your stolen data can:
  - Open a new credit card or loan.
  - Change a billing address so you will no longer receive the bills.
  - Open new utilities accounts in your name.
  - Obtain a mobile phone.
  - Open a bank account and writing bad checks.
  - Use your debit card number to withdraw funds.
  - Obtain a new driver's license or ID.
  - Use your information in the event of an arrest or court action.

Identity Theft!!!

## BROWSER SECURITY



- Download “content blockers” - Safari>Safari Extensions
- Content Blockers available for most browsers
- DISTRUST ALL pop-up notifications and windows
- Customize individual web sites: Safari>Settings for ...



31

Content blocking is a feature of the browsers that allows you to block or hide all or some content in a webpage or site that you do not want to see, including images, ads, pop-ups, comments and plug-ins.

Using content blocker in a browser, you have following benefits:

Browser runs faster

Webpages load significantly quicker

By not loading unwanted content you save significant amount of mobile data.

Some harmful pop ups and script are blocked and thus it provides little privacy and security to the website visitors.

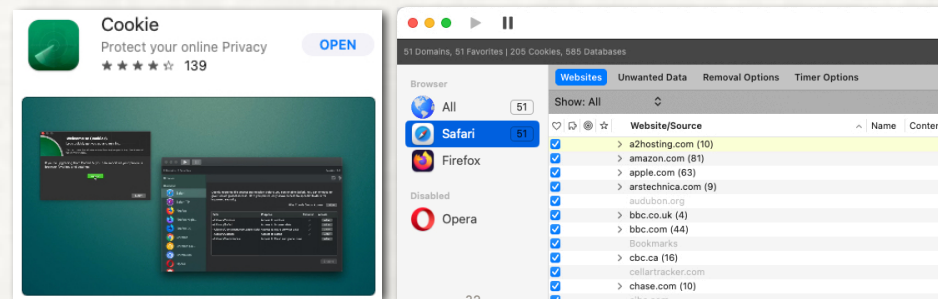
Many if not most advertisements are blocked

Many auto-running ad movies are blocked

## BROWSER SECURITY



- Be careful of accepting all cookies - use “Cookie” app from Mac App store
- Use a VPN to prevent your internet provider from collecting your web history
- Use an anonymizer search engine (DuckDuckGo)



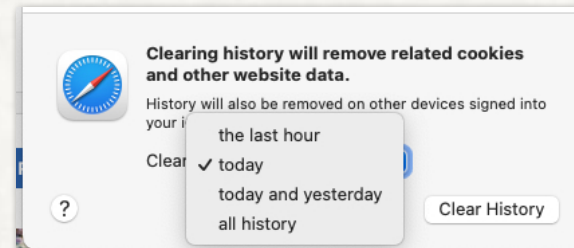
All websites that you visit store cookies in your browser without your knowledge or consent. Some are helpful, but most of them track you either once or constantly as you surf. Cookie gives you total control over all cookie storage types: HTTP cookies, Flash cookies, HTML5 databases, localStorage, IndexedDB as well as browser history and caches. Simple enough for even the most technophobic computer users, yet Cookie makes no compromises for power users. After a quick initial setup, Cookie will protect your privacy, keeping you safe from tracking and online profiling. Advanced detection and removal of spying and tracking cookie threats is included. Select favorite domains for all cookie types to completely customize your browsing experience. Setup automatic removal schedules for even better peace of mind.



## BROWSER SECURITY



- Clear your Browsing History:
  - If you are crossing international borders
  - If you are planning on using your device in an area known for its thefts
  - If you are entering a secure location
- Safari Menu>History>Clear History



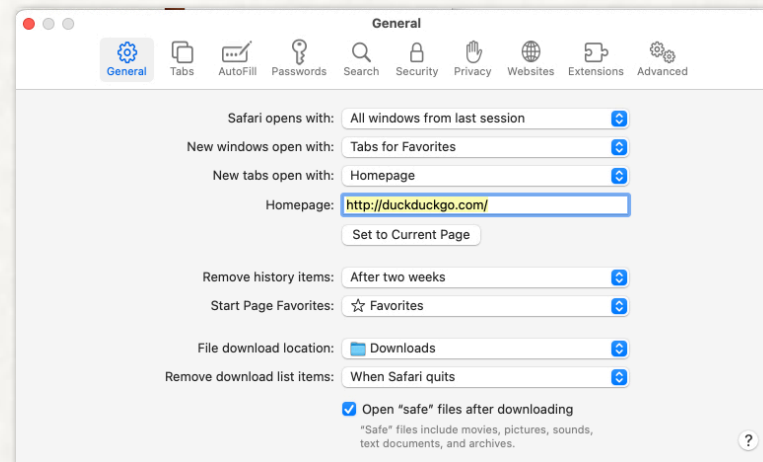
33

Browsing history can get you in trouble in “strict policing/police states” or China, Russia, Singapore. Don’t chance it!! Clear History.

## BROWSER SECURITY



- Review Safari>Settings



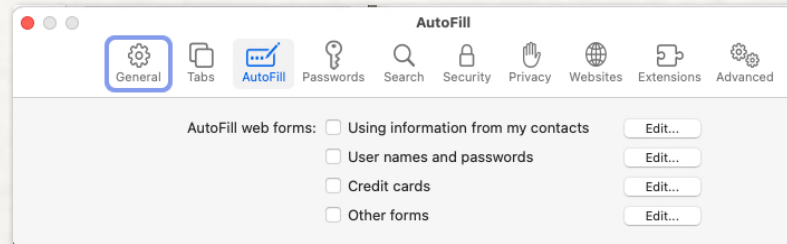
34

Lots of information here that is saved on your hard disk/SSD

## BROWSER SECURITY



- Review Safari>Settings>AutoFill
- Turn OFF all AutoFill web forms
- If thief gets your device, AutoFill will allow them to login as you!!



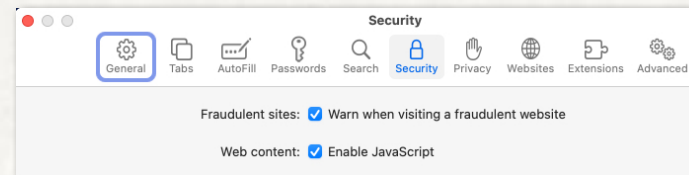
35

What if competitor got your laptop and you had automatic sign-in. Then they could go to your companies web site and your username and password would be filled in!! A burglar could get your home address, your bank, account & password, etc.

## BROWSER SECURITY



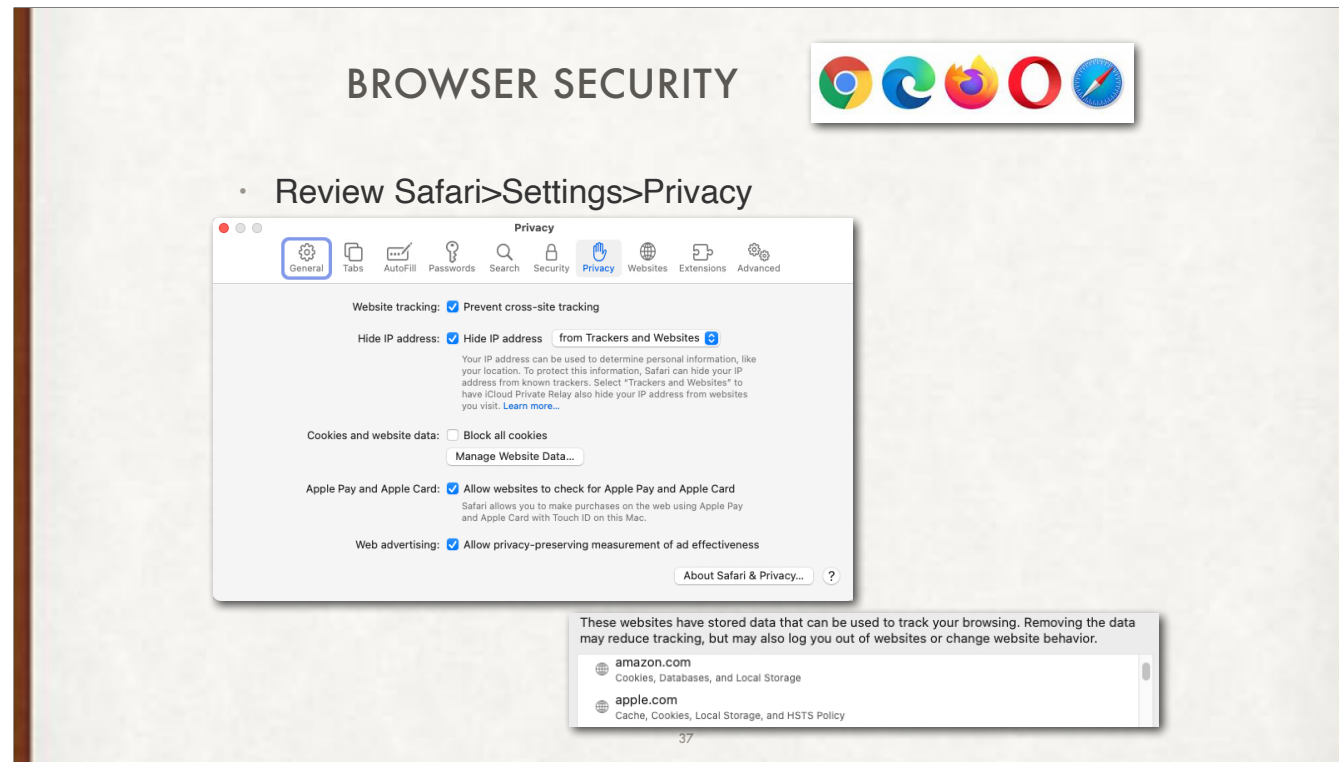
- Review Safari>Settings>Security
- Fraudulent sites should be checked!
- Web content (JavaScript) can sometimes have bugs.  
Check this if you want maximum safety, but it may stop somethings from working at a site



36

Check the first box.

The second is optional but many animations either on the web site or on your computer will not work. JavaScript is everywhere!! It sometimes has bugs which can be exploited.

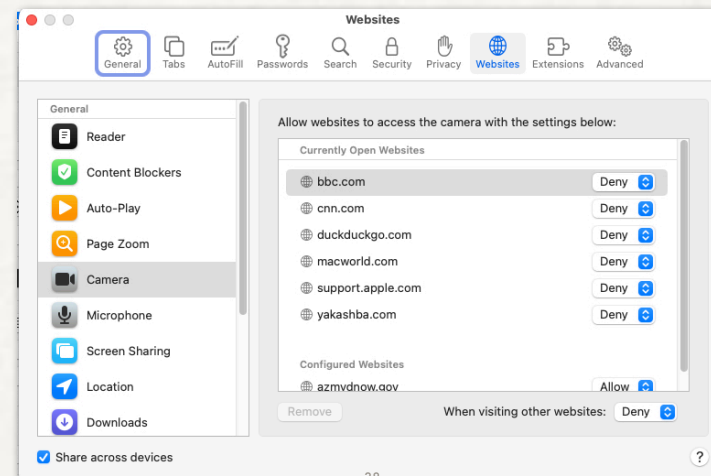


Review and remove cookies regularly (easier than once a year): Safari>Settings>Privacy>Manage Website Data

## BROWSER SECURITY



- Review Safari>Settings>Websites
- Deny use of camera, microphone & location

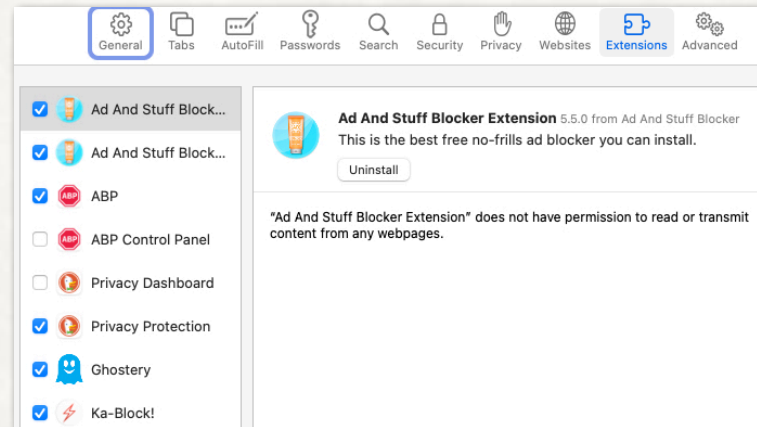


While the Camera, Microphone & Location are the most “privacy destructing/invading”, you should also review the others since some sites ask for permission to access everything!!

## BROWSER SECURITY



- Review Safari>Settings>Extensions
- Quickly and easily turn on or off or delete an extension



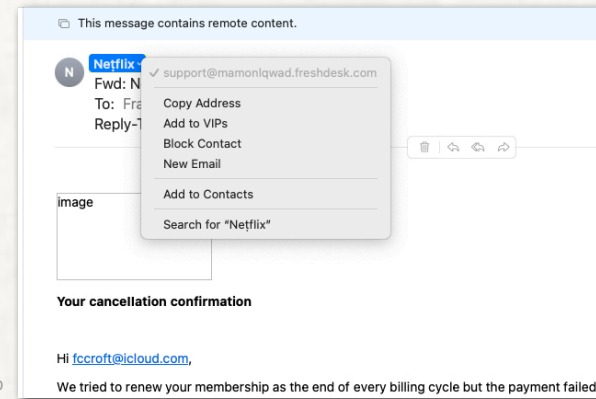
39

Extension are GREAT ways to block ads, unwanted popups, etc. You can add them to Safari by going to the Mac App store, typing in Safari Extensions, and download the ones with the most stars AND the highest number of reviews. ALWAYS be suspicious of 5 star reviews from less than 100 people (the programmer's friends)

## APPLE MAIL SECURITY

**Doug Mcknight** 6/7/23, 11:45 AM  
photographs – posted by Doug Mcknight  
On Wednesday, June 07, 2023 12:37 PM, Doug Mcknight wrote: I'm assuming you should remember them – the ladies in this image: htt...

- Be Suspicious!!
- Look for misspellings, bad grammar, strange fonts
- If you hover over a link in an email, the address it points to will be revealed - if different, DON'T click!!
- Do not open attachments, even if from an email of a person you know - many emails have been hacked & used

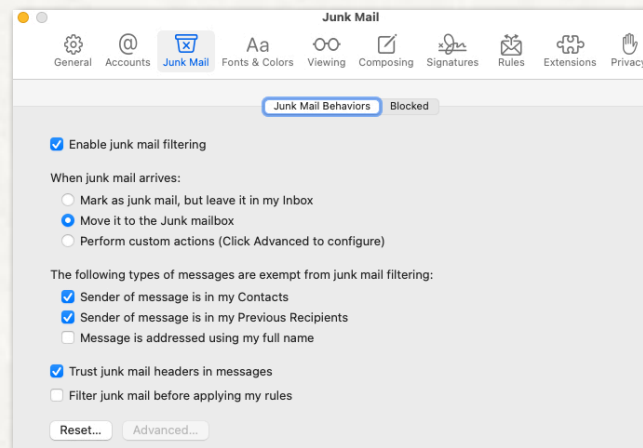


The “photograph” email has been going around for several months, and is always from “someone you know”. Their email password was hacked, their address book stolen, and is being reused by several hundred hackers, hoping for a bite.



## APPLE MAIL SECURITY - MAIL SETTINGS

- Open Mail, Click on Mail>Settings>Junk Mail
- Enable junk mail filtering and move it to Junk mailbox
- I exempt Contacts and Previous Recipients

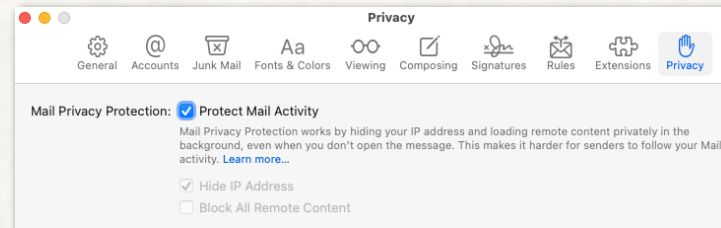


41

All email servers (Gmail, iCloud, Yahoo, etc) now scan for emails and will flag them. If they are flagged, AND you have enabled Junk mail filtering, they will go into a junk email folder. You should look at it daily, and NEVER click on an email in there unless you are sure it is real. Spammers and hackers can not embed a small program that is sent when someone clicks on their email!! If you have viewed (and not clicked) on all the emails and they are all junk, do a Edit>Select All (or Cmd A) then hit delete.

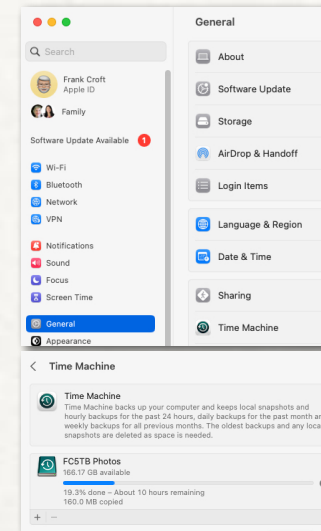
## APPLE MAIL SECURITY - MAIL SETTINGS

- Open Mail, Click on Mail>Settings>Privacy
- Protect Mail Activity very nice addition to Apple Mail!



## BACKUP YOUR COMPUTER!!

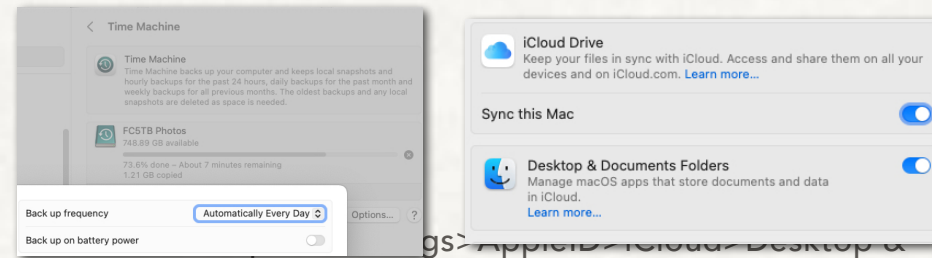
- Use Time Machine to backup your computer to local disk: Settings>General>Time Machine
- Use iCloud>iCloud Drive to backup your computer to the cloud



If you want the best protection against loss, I always back up to the web, AND to a local device. If only to the web and someone hacks your iCloud account, you could loose everything on the web. If your home burns down, you could loose the local device. That is why I do both!!

## DATA SECURITY

- Time Machine backup: Settings>General>Time Machine



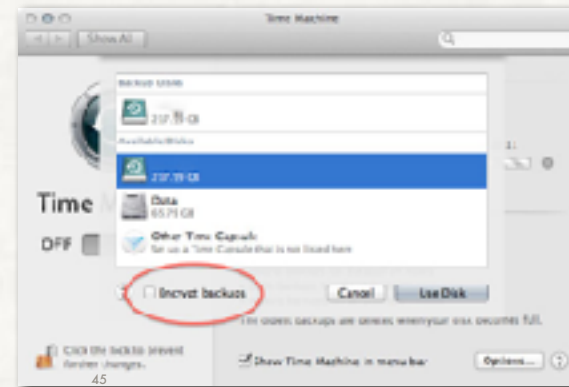
gs> AppleID>iCloud>Desktop & Documents Folders ON

- iPhone: Settings>AppleID>iCloud>iCloud Backup ON

With the two backups above (one local, one in the cloud) your data survives most catastrophes!!

## ENCRYPT YOUR BACKUP DISK

- On your Mac, click on Apple> System Settings> General> Time Machine.
- Click on “+” to add, select disk, and check Encrypt backups
- Alternately, click on Time Machine Icon in Menu bar



## ENCRYPT YOUR iOS BACKUP ON MAC

- Open **Finder** and connect your iPhone or iPad to your computer.
- Click on your device in Finder sidebar
- Select **Summary** from the options on the left or at the top in Finder.
- On the right pane, check the option that says **Encrypt local backup**.
- Finder will prompt you to set a password for encryption. Enter a password in both fields and click **Set Password**. Save this password!!!!
- Finder will start backing up your device to encrypted file