ALL THINGS SECURED

MACBOOK SECURITY GUIDE

A step-by-step guide to walk you through the most imortant security settings to change on Mac.

2026

AllThingsSecured.com/Macbook

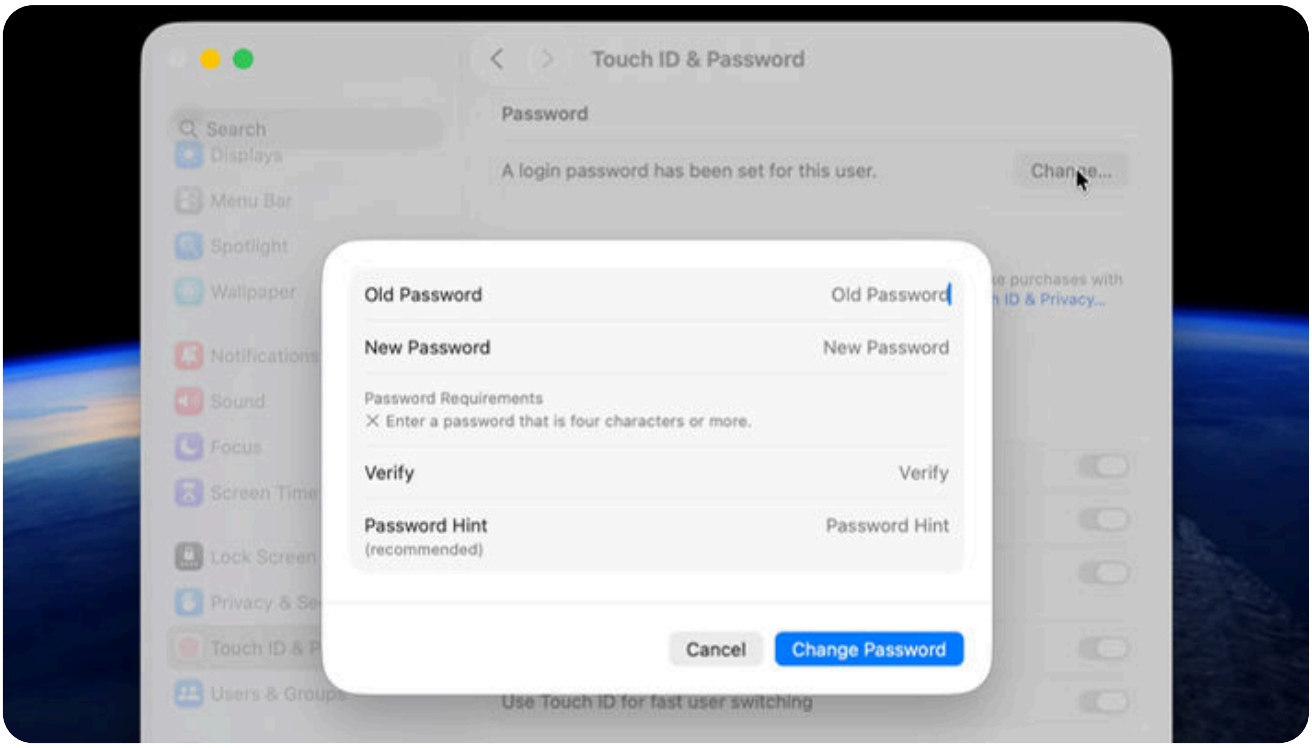
Mac Security 101

Your MacBook is one of the most powerful—and most personal—devices that you own. It holds your emails, photos, documents, browsing history, passwords, and access to countless online accounts. While Apple does a good job with security out of the box, many of the most important protections are either optional, buried in settings, or turned off by default.

This guide walks you through **specific security and privacy settings** that can dramatically reduce your risk of being hacked, tracked, impersonated, or locked out of your own data. Most of these changes take less than a minute each, require no technical background, and can be completed in about 15 minutes total.

1. Computer Password

Protect local access to your MacBook and encrypt user-level data.



RATING: Must Do!
TIME: 1 minute
DIFFICULTY: Easy

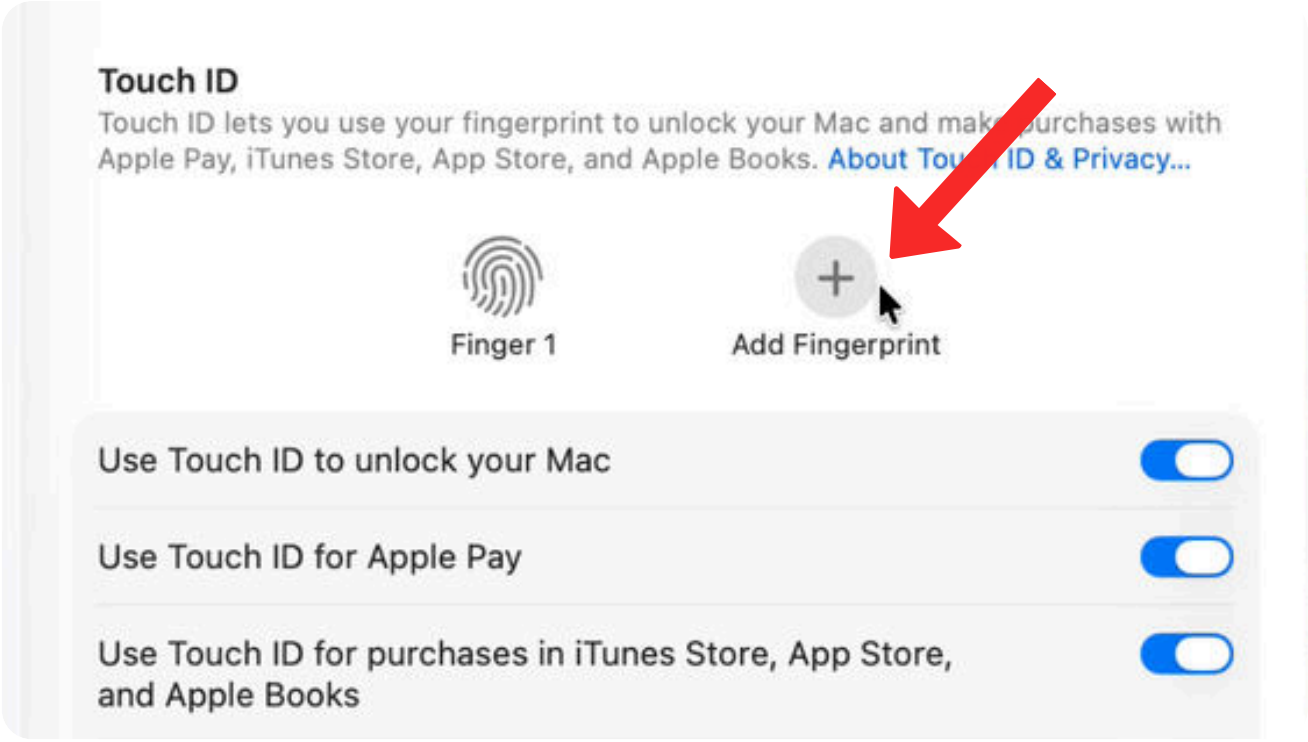
New MacBooks will require you to set a password during setup, but if you want to change this later, go to **Touch ID & Password** and then under Password clikc **Change**. You will be required to input your current password before creating a new one.

Why is this important?

Your Mac's login password is the first and most important line of defense. If someone gains physical access to your laptop, a weak password makes it trivial to access your files, emails, and saved browser sessions. A strong password significantly slows down or completely blocks unauthorized access.

2. Set Up Touch ID

Add fast, secure biometric authentication without risking privacy.



RATING: Recommended
TIME: 1 minute
DIFFICULTY: Easy

How to Access:

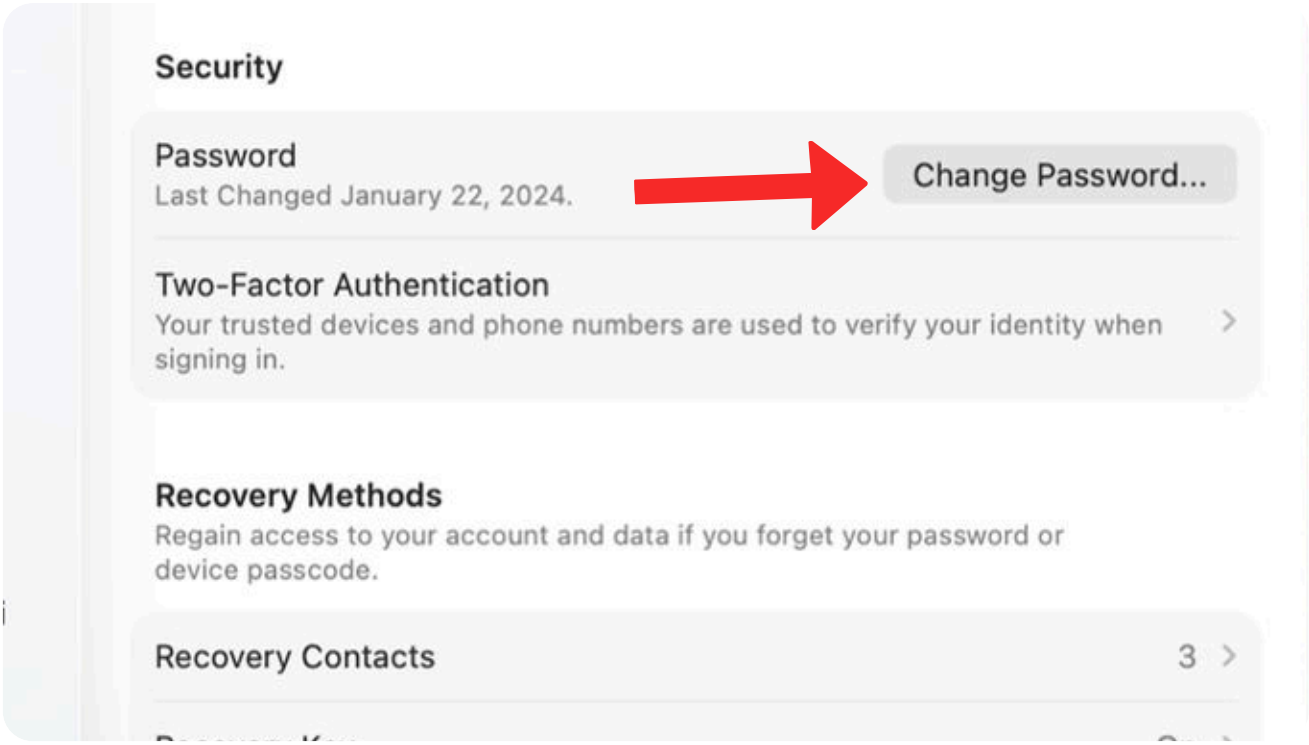
- Open **System Settings**
- Go to **Touch ID & Password**
- Add a fingerprint

Why is this important?

Touch ID allows you to unlock your Mac and approve actions quickly without typing your password in public or unsafe environments. Fingerprint data is stored in the Secure Enclave, a dedicated hardware component isolated from macOS and iCloud. This means your biometric data never leaves your device and cannot be accessed by apps or Apple itself.

3. Apple ID Password

Secure access to your Apple account, iCloud data & connected devices.



RATING: Recommended
TIME: 1 minute
DIFFICULTY: Easy

How to Access:

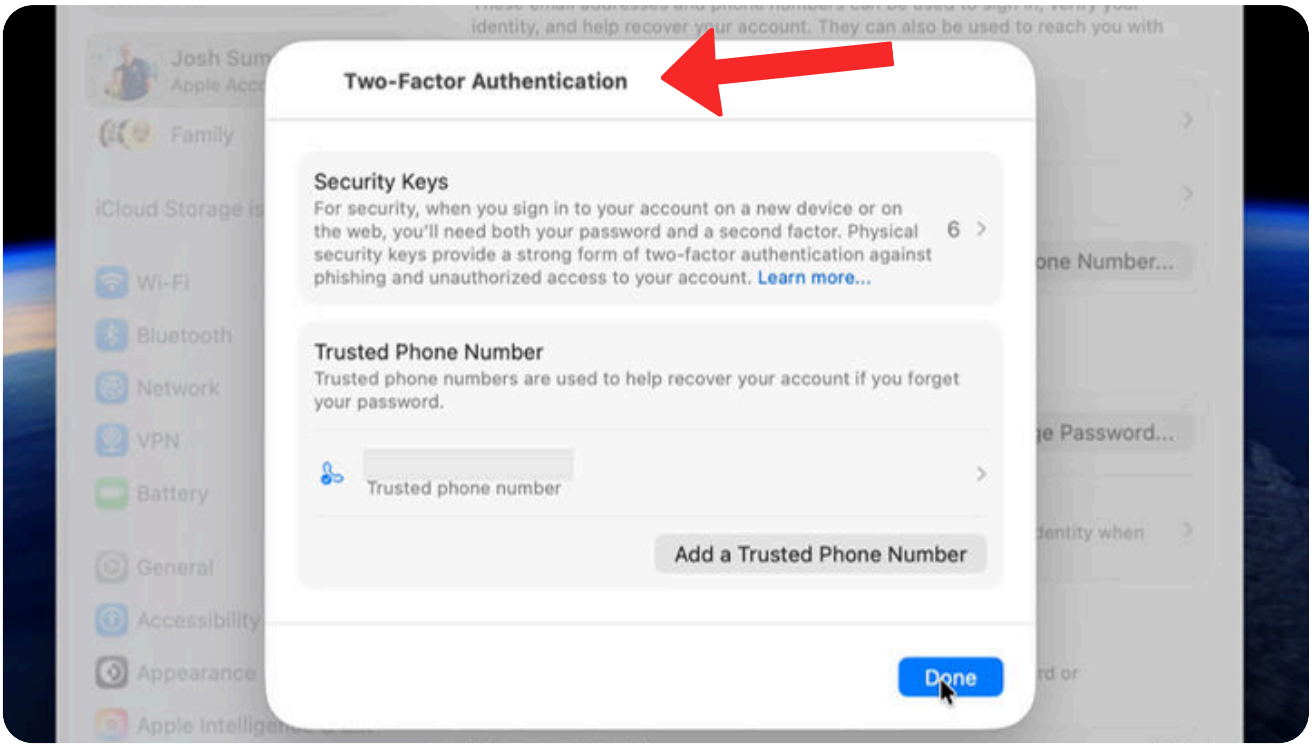
- Open **System Settings**
- Click your **Apple ID name**
- Go to **Sign-In & Security**
- Change password

Why is this important?

Your Apple ID password controls far more than just App Store purchases. It grants access to iCloud backups, photos, messages, device tracking, and account recovery features. If compromised, an attacker could lock you out of your own data. Because this password is used infrequently, it should be especially strong and unique. Never reuse it anywhere else, and store it securely in a password manager rather than relying on memory alone.

4. Apple ID 2FA

Prevent account takeovers even if your password is stolen.



RATING: Recommended

TIME: 2 minutes

DIFFICULTY: Medium

How to Access:

- Open **System Settings**
- Click your **Apple ID**
- Go to **Sign-In & Security**
- Enable **Two-Factor Authentication**

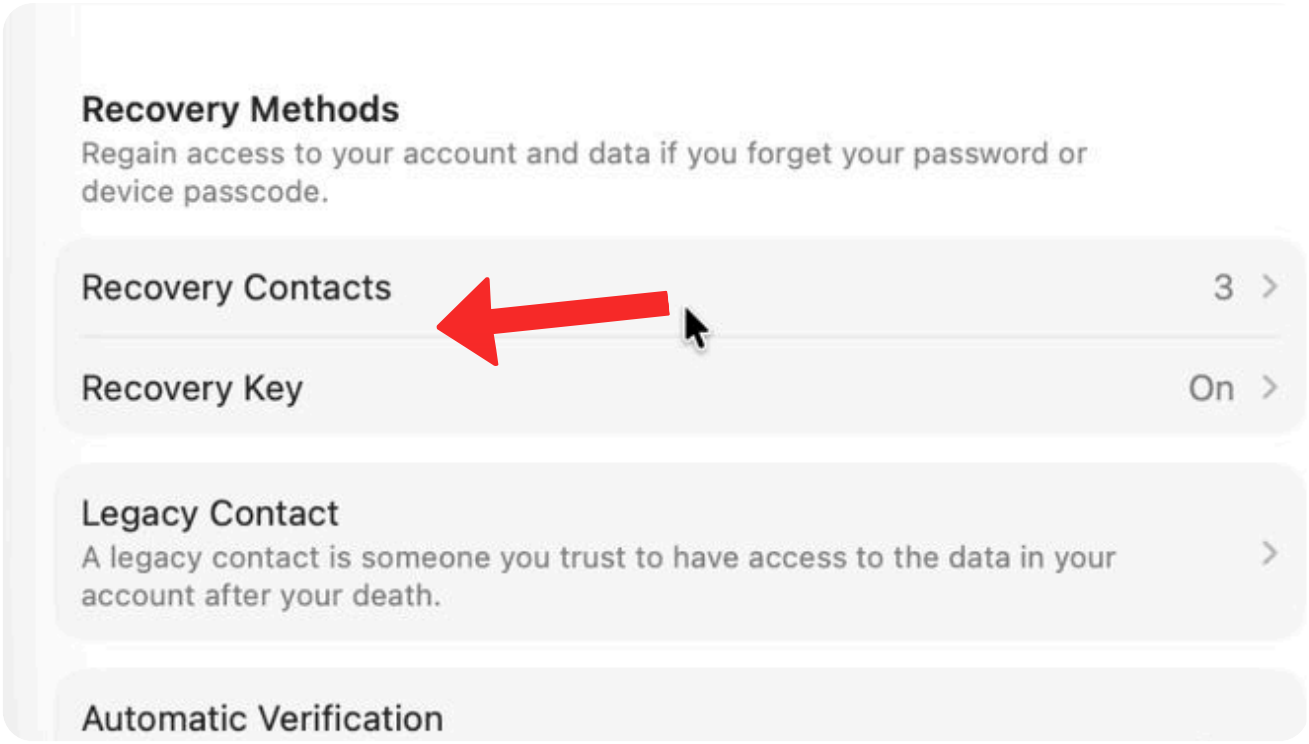
Why is this important?

Two-factor authentication (2FA) ensures that knowing your password alone is not enough to access your Apple account. This protects you against phishing, data breaches, and password reuse attacks. For maximum security, a hardware security key is ideal. At minimum, a trusted phone number should be enabled. This single setting blocks the vast majority of real-world account takeover attempts.

Watch our full Apple 2FA Tutorial on YouTube.

5. Account Recovery

Protect yourself against forgotten passwords or lost 2FA.



RATING: Recommended
TIME: 3 minutes
DIFFICULTY: Medium

How to Access:

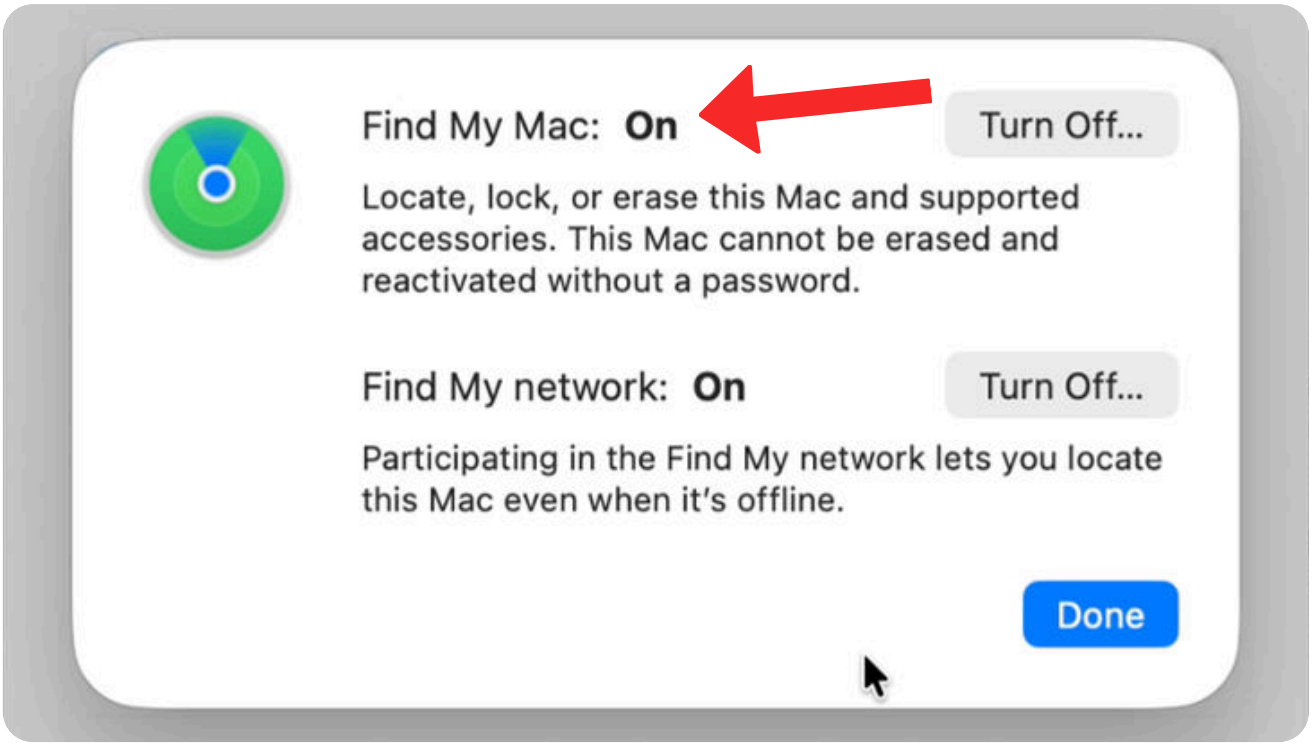
- Open **System Settings**
- Click your **Apple ID**
- Go to **Sign-In & Security**
- Click **Recovery Contacts** or **Recovery Key**

Why is this important?

A recovery contact allows a trusted person to help you regain access if you forget your password or lose your security keys. This feature is especially important if you enable stronger protections like Advanced Data Protection. Choose someone you trust completely. They cannot access your data directly, but they do play a role in account recovery, which makes this both powerful and reversible.

6. Find My Mac / Network

Allows you to locate, lock, or erase a lost or stolen MacBook.



RATING: a Good Idea
TIME: 1 minute
DIFFICULTY: Easy

How to Access:

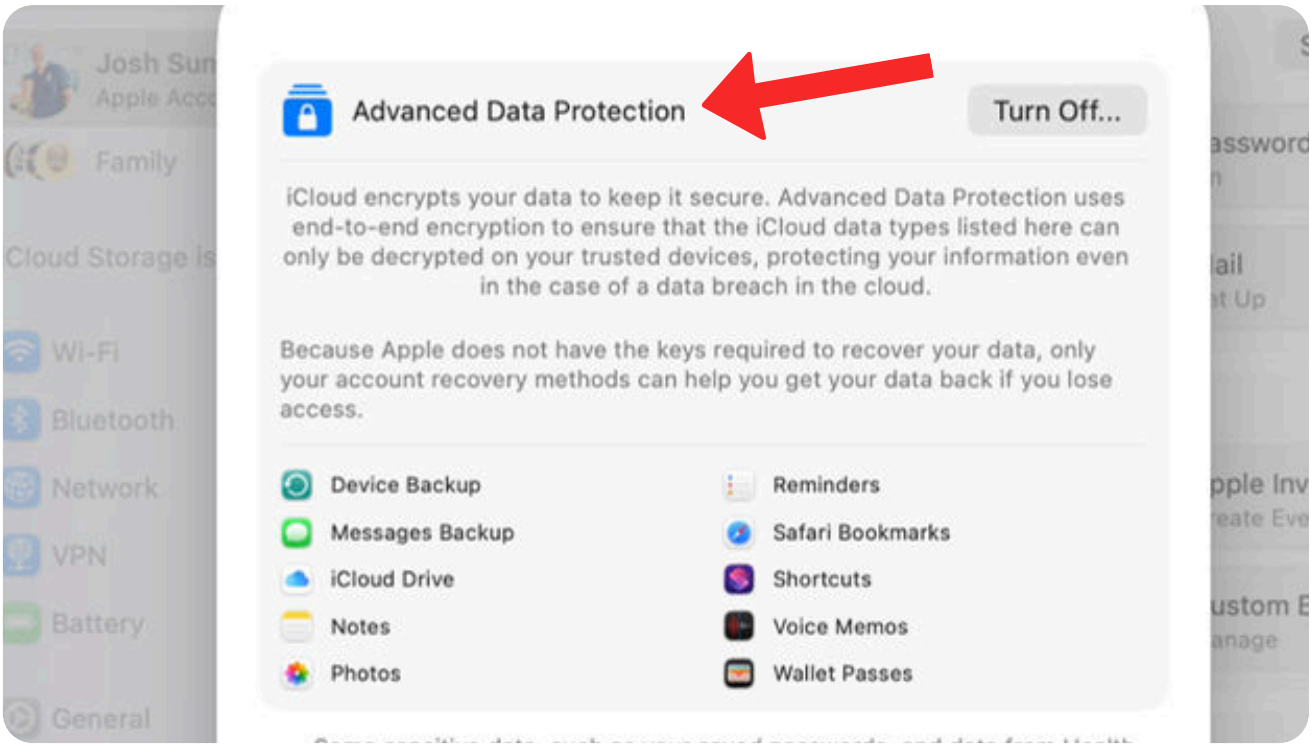
- Open your **System Settings**
- Click on your **Apple ID**
- Click **iCloud** → **See All**
- Enable **Find My Mac**

Why is this important?

Find My Mac enables remote tracking and device erasure, which is critical if your laptop is lost or stolen. This can prevent sensitive data from falling into the wrong hands. While it does involve encrypted location data, the security benefit for some people can outweigh the privacy trade-off —especially travelers and remote workers.

7. Advanced Data Protection

Encrypts iCloud data so that not even Apple can access it.



RATING: Must Do
TIME: 2-15 minutes
DIFFICULTY: Medium

How to Access:

- Open your **System Settings**
- Click on your **Apple ID**
- Click **iCloud**
- Enable **Advanced Data Protection**

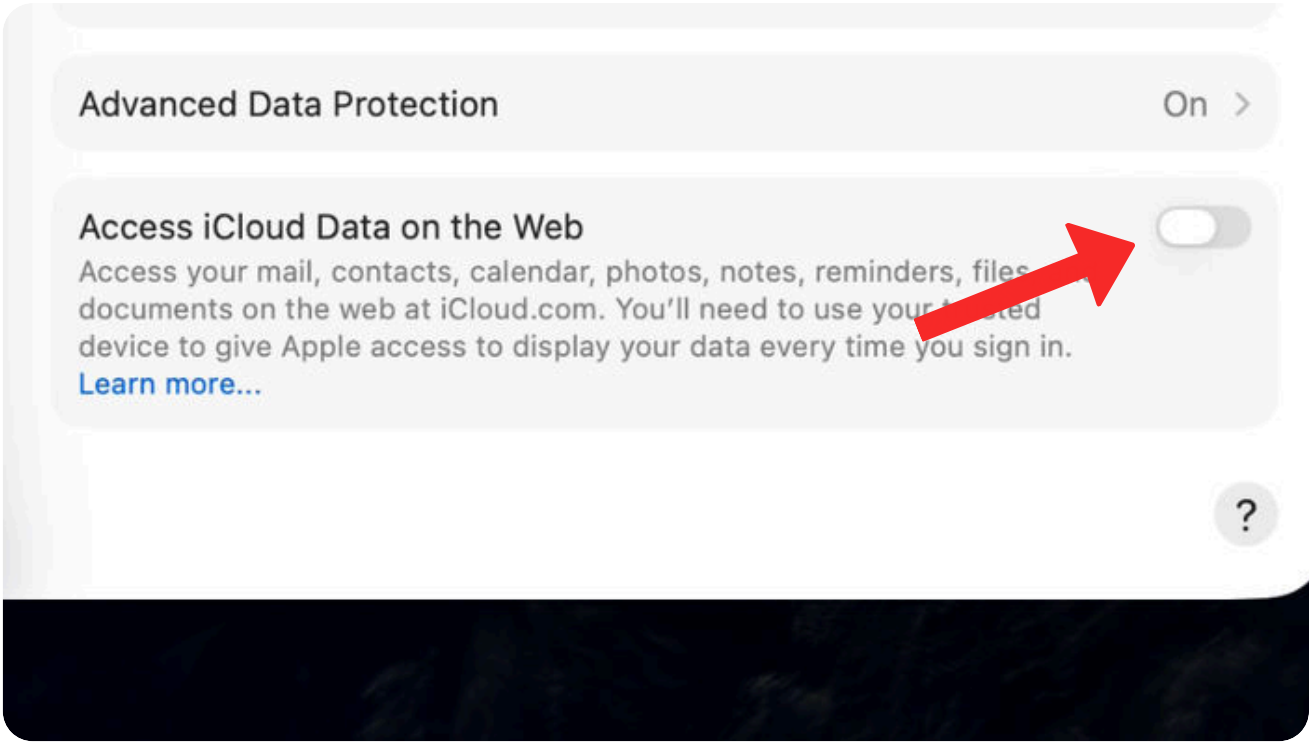
Why is this important?

Advanced Data Protection applies end-to-end encryption to most iCloud data, including photos, notes, backups, and files. This ensures only you—and your trusted recovery methods—can access your data. This setting requires updated devices and proper recovery options, but it represents one of the most meaningful privacy upgrades Apple offers.

Watch our Advanced Data Protection Tutorial on YouTube.

8. iCloud Web Access OFF

Prevent iCloud data from being accessed through a web browser.



RATING: Recommended
TIME: 1 minute
DIFFICULTY: Easy

How to Access:

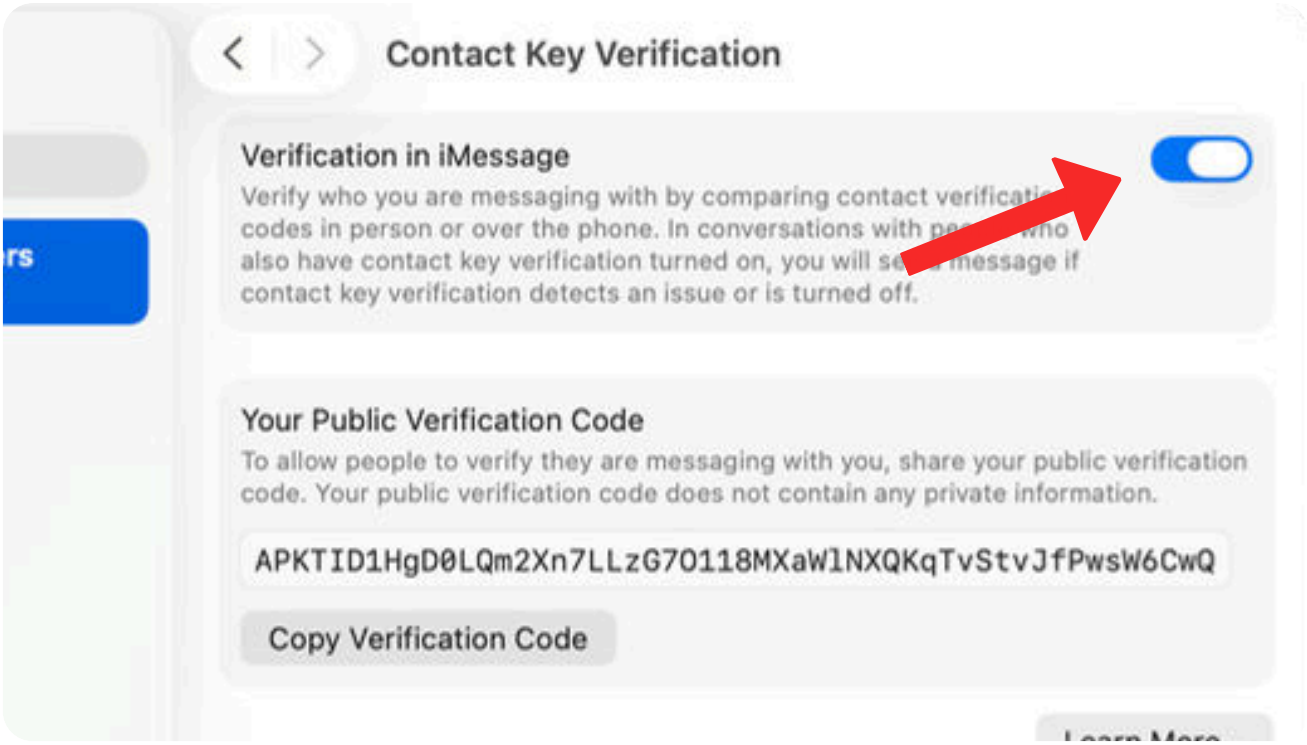
- Open your **System Settings**
- Click on your **Apple ID**
- Click **iCloud**
- Disable **Access iCloud Data on the Web**

Why is this important?

If you never use iCloud.com, leaving web access enabled creates unnecessary exposure. Disabling it reduces the attack surface for phishing and account compromise. This change has little downside for most users and immediately tightens account security.

9. Contact Key Verification

Confirm the identity of iMessage contacts to prevent impersonation.



RATING: Very Useful
TIME: 1-10 minutes
DIFFICULTY: Difficult

How to Access:

- Open your **System Settings**
- Click on your **Apple ID**
- Click **Contact Key Verification**
- Turn on **Verification in iMessage**

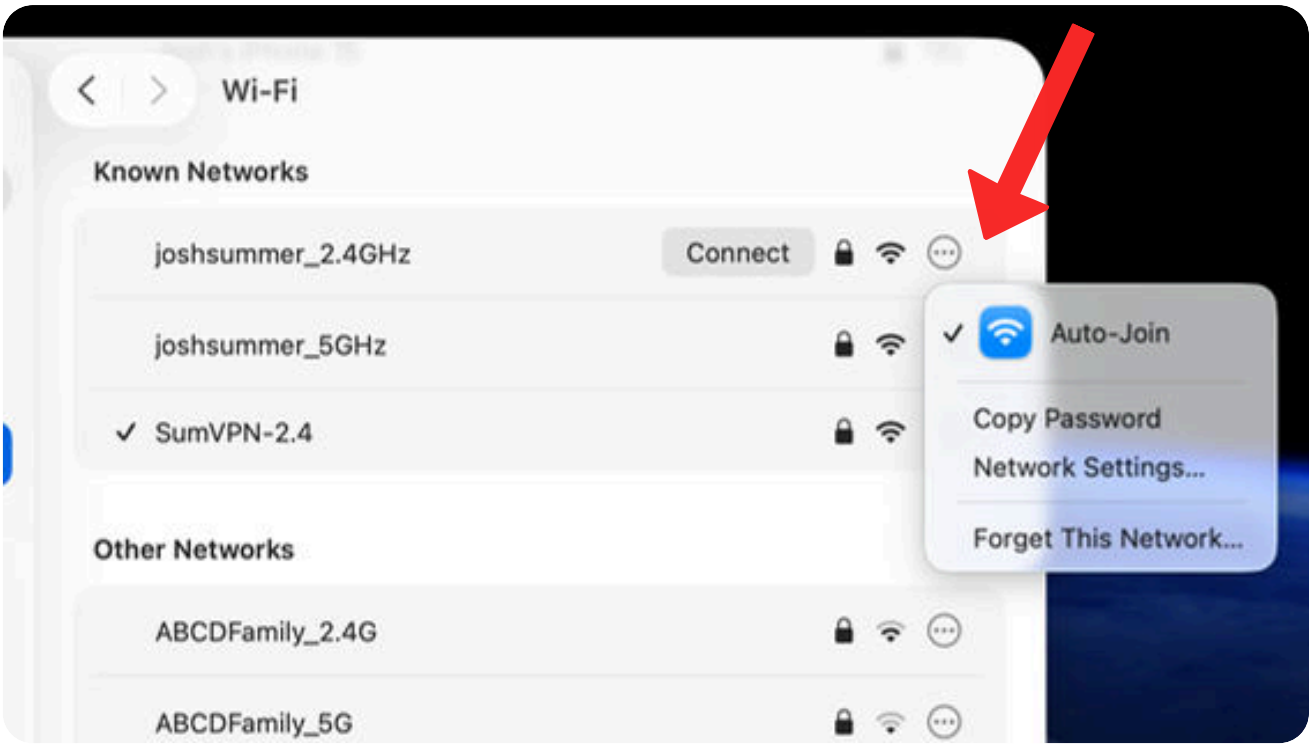
Why is this important?

Contact Key Verification ensures that the person you're messaging is truly who they claim to be. It protects against SIM-swap attacks and advanced interception attempts. Once enabled, verified contacts display a confirmation checkmark. The setup is the only real inconvenience, and the security benefit is substantial.

Watch our full [Contact Key Explanation on YouTube.]

10. AutoJoin Wifi Settings

Prevent your Mac from connecting to malicious look-alike networks.



RATING: Recommended
TIME: 5 minutes
DIFFICULTY: Medium

How to Access:

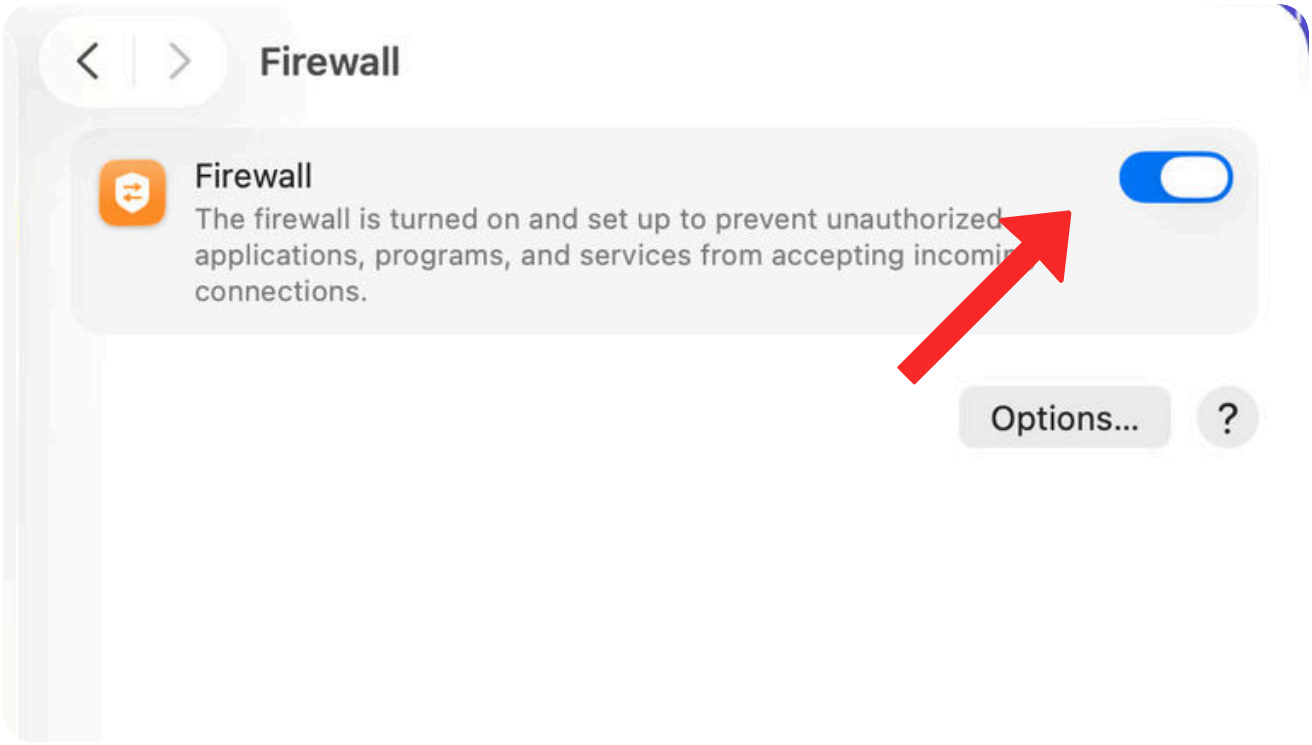
- Open your **System Settings**
- Click on **WiFi**
- Adjust the **Auto-Join** settings

Why is this important?

Attackers often name rogue networks after popular locations like cafés or hotels. Disabling auto-join prevents your Mac from connecting without your knowledge. Known networks such as your home or work can still be set to auto-join for convenience, but unknown or public networks should always require manual approval.

11. Turn on Firewall

Block unwanted inbound network connections.



RATING: Recommended
TIME: 1 minute
DIFFICULTY: Easy

How to Access:

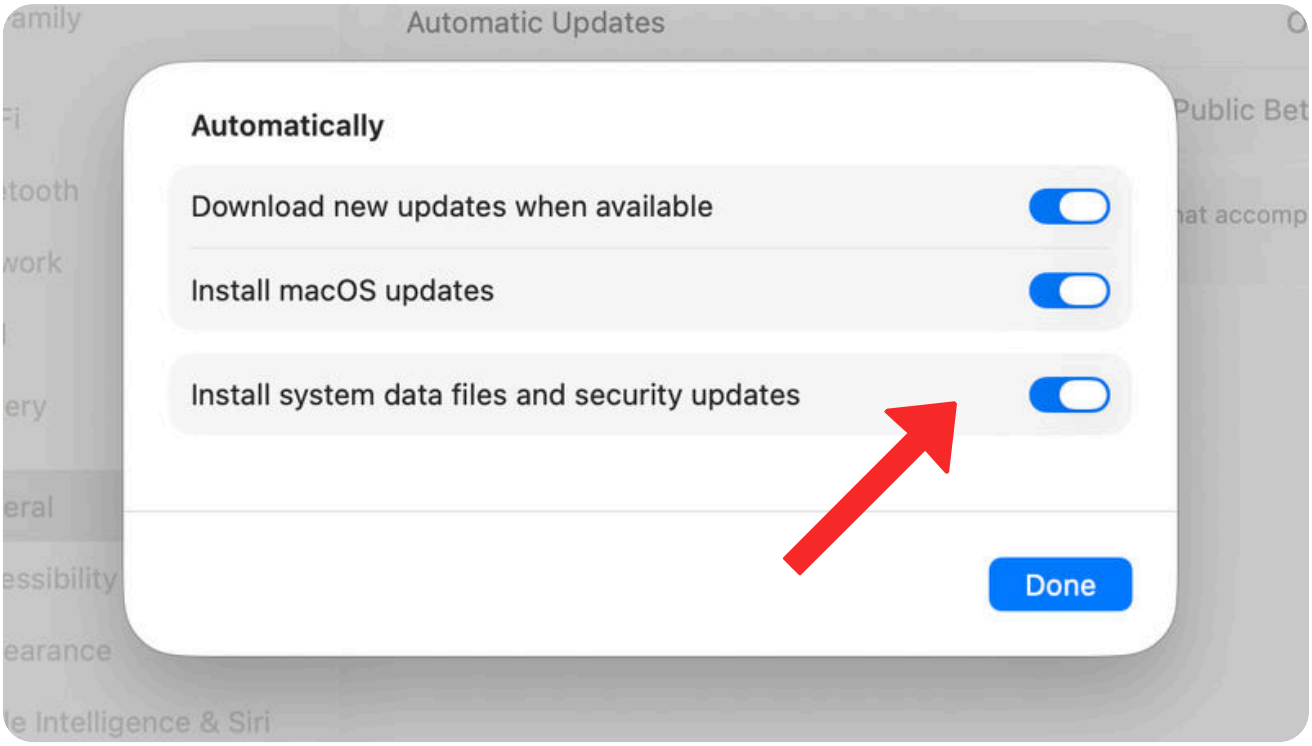
- Open your **System Settings**
- Click on **Network**
- Click on **Firewall**
- Turn on Firewall and adjust **Options** as desired.

Why is this important?

The firewall acts as a gatekeeper, preventing unauthorized devices or services from initiating connections to your Mac. This protects against network-based attacks and misbehaving applications. Advanced options like stealth mode further reduce your device's visibility on shared networks.

12. Security Updates

Install critical security patches without user intervention.



RATING: Must Do
TIME: 1 minute
DIFFICULTY: Easy

How to Access:

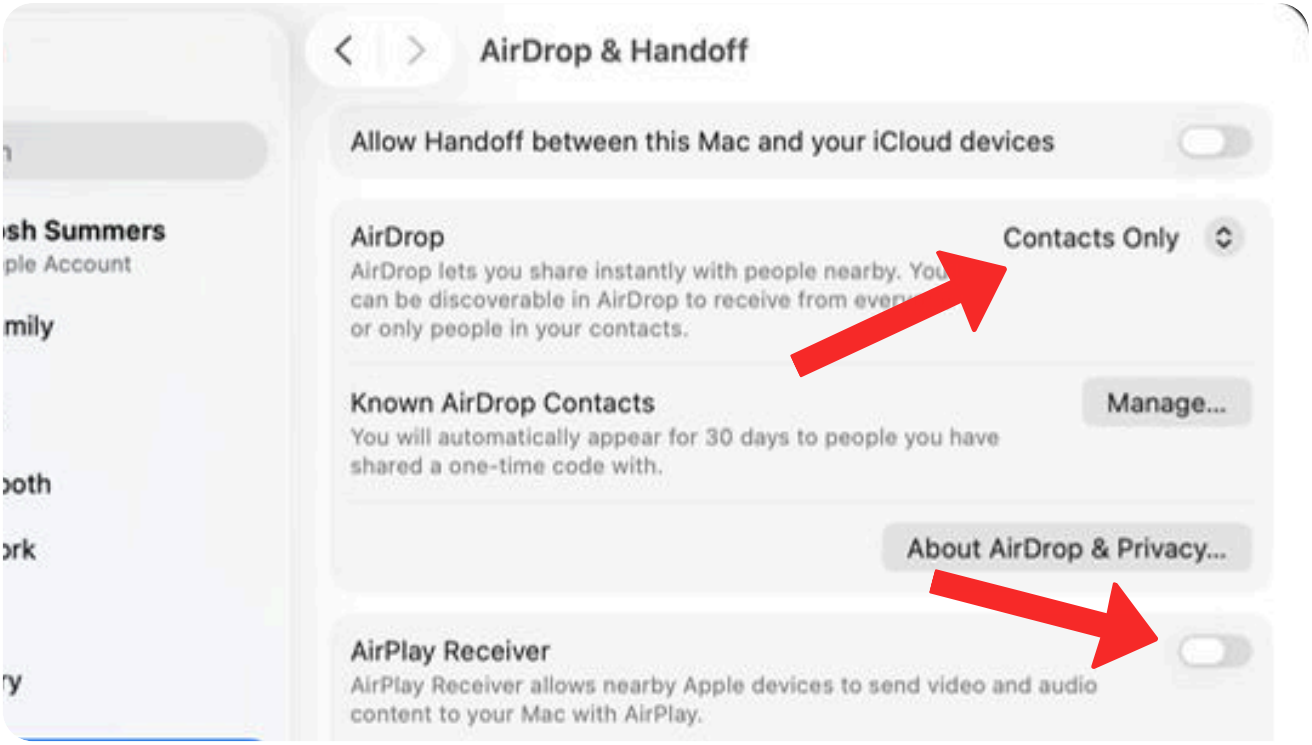
- Open your **System Settings**
- Click on **General**
- Click on **Software Update**
- Click the info icon next to **Automatic Udpates**
- Turn all settings on

Why is this important?

Security vulnerabilities are discovered constantly. Automatic updates ensure your Mac receives fixes quickly, even if you forget to check manually. At minimum, system data files and security updates should always be enabled, and it's up to you whether you want to Install macOS updates automatically when they become available.

13. Adjust Airdrop / Handoff

Limit unwanted file transfers and device interactions.



RATING: Recommended

TIME: 1 minute

DIFFICULTY: Easy

How to Access:

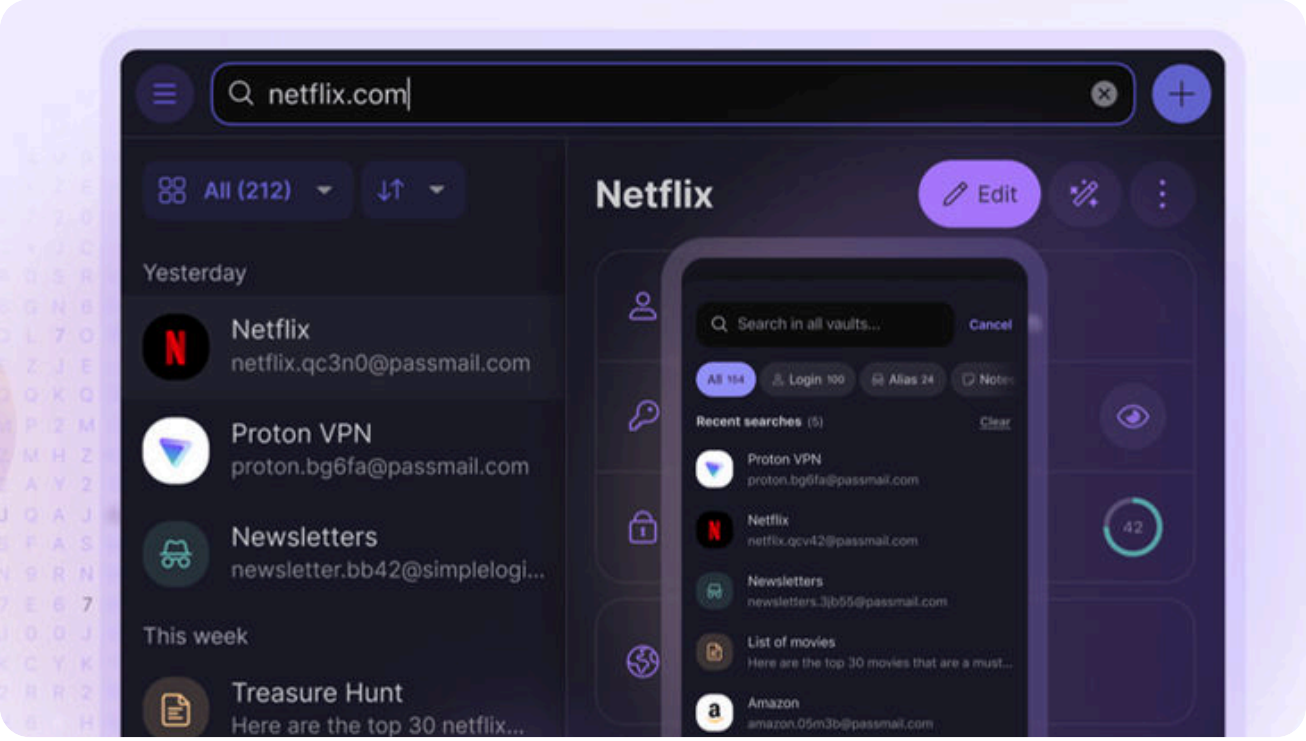
- Open your **System Settings**
- Click on **General**
- Click on **Airdrop & Handoff**
- Set Airdrop to **Contacts Only**
- Turn off **Airplay Receiver**

Why is this important?

AirDrop set to “Everyone” can expose you to spam or inappropriate content. Restricting it to Contacts Only minimizes risk without eliminating convenience. Handoff and AirPlay Receiver should be disabled if you don’t actively use them.

14. Download Proton Pass

Securely & conveniently store passwords outside of Apple's ecosystem.



RATING: Recommended
TIME: 10 minutes
DIFFICULTY: Medium

How to Access:

- Open your browser
- Visit Proton.me/pass
- Create a free account
- Download the Proton Pass app

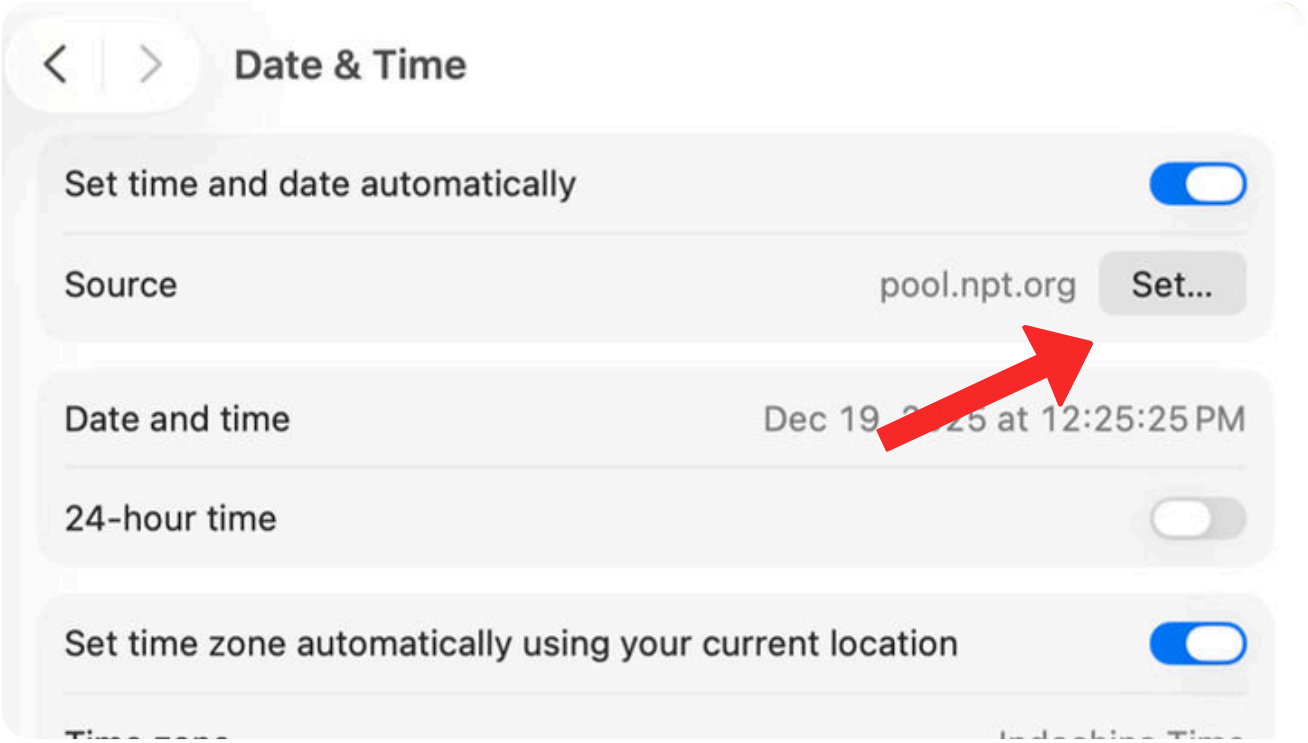
Why is this important?

Using a dedicated password manager reduces reliance on a single ecosystem and improves visibility into account security. Proton Pass offers encryption, open-source auditing, and optional features like aliases and built-in 2FA. Use the app for free or get extra features with a premium account.

Try Proton Pass

15. Change Date/Time Server

Reduce reliance on Apple-controlled infrastructure.



RATING: a Good idea
TIME: 1 minute
DIFFICULTY: Easy

How to Access:

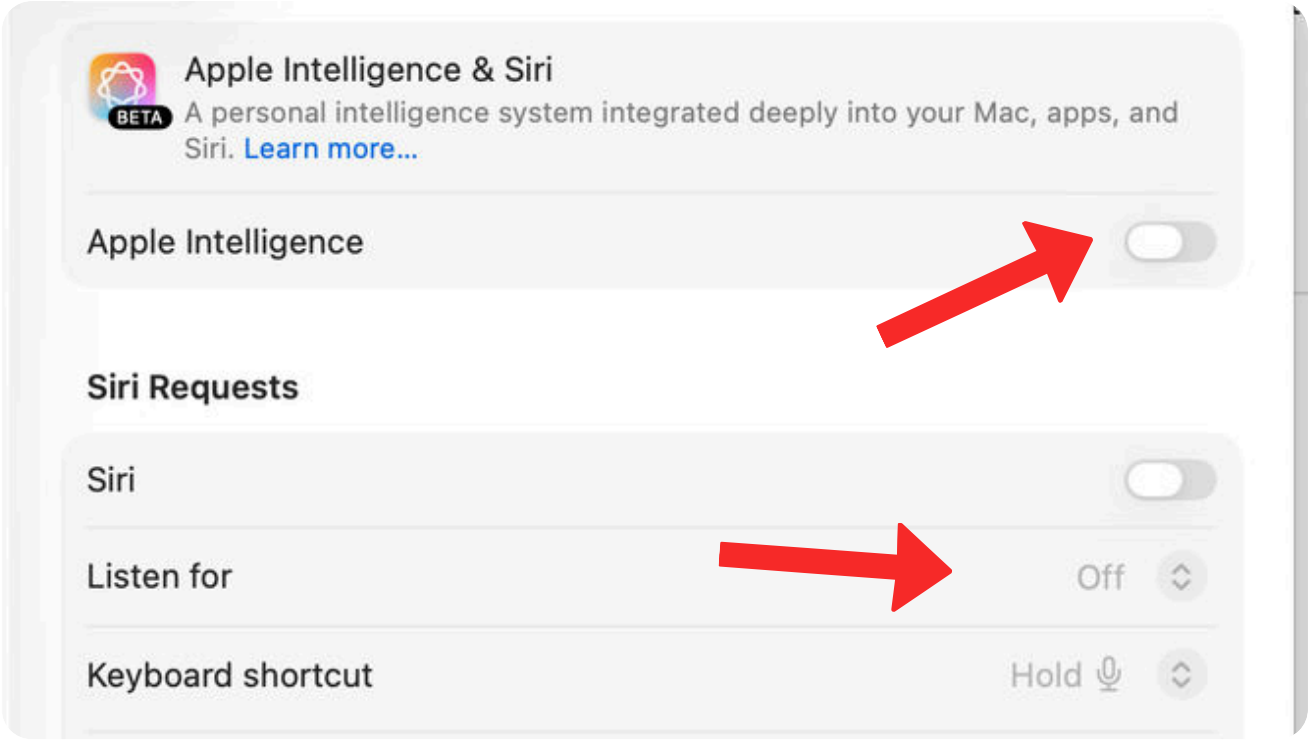
- Open your **System Settings**
- Click on **General**
- Click on **Date & Time**
- Under Source click **Set**
- Change to pool.npt.org

Why is this important?

Switching to a public NTP server slightly improves privacy by reducing communication with Apple servers. While the benefit is modest, it's easy to implement and doesn't have any impact on the daily usage of your MacBook. This is a classic "set it and forget it" improvement.

16. Apple Intelligence / Siri

Prevent unnecessary data collection and microphone activation.



RATING: a Good idea
TIME: 1 minute
DIFFICULTY: Easy

How to Access:

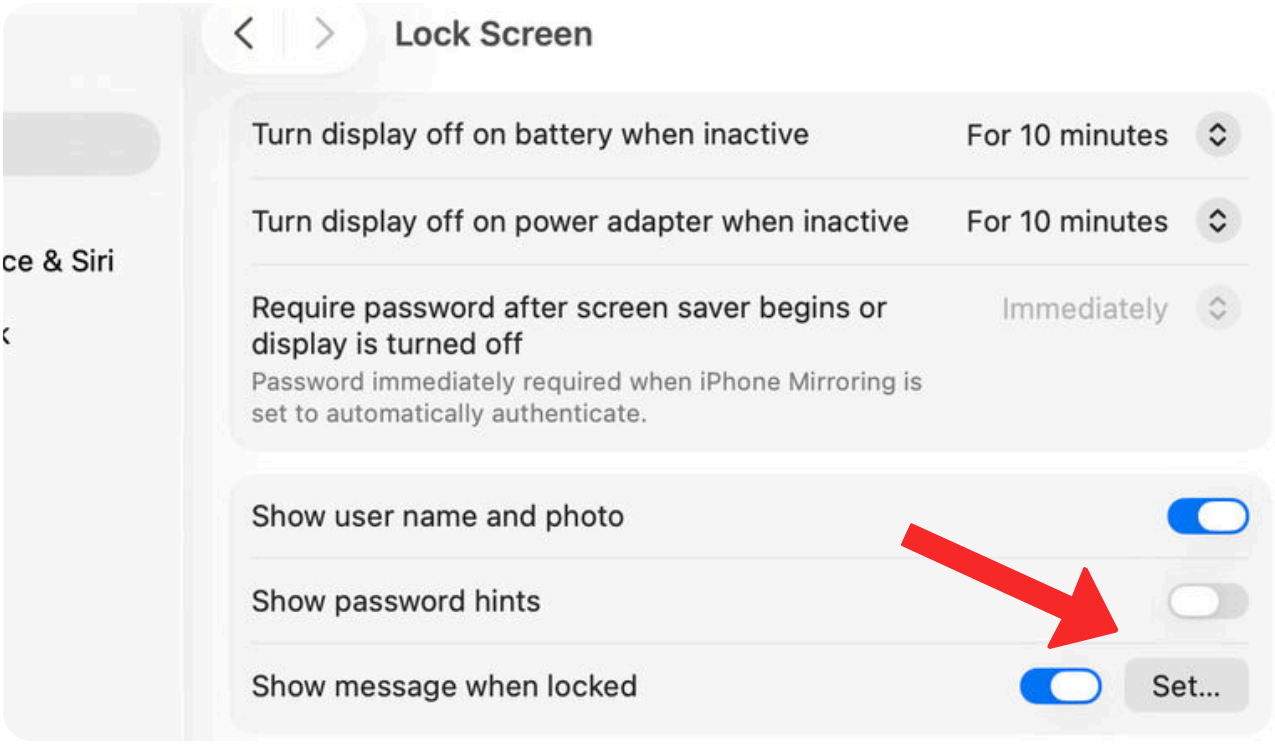
- Open your **System Settings**
- Click on **Apple Intelligence & Siri**
- Turn off **Apple Intelligence**
- Under **Listen for** choose “Off”

Why is this important?

If you do not actively use Siri or Apple Intelligence, disabling them reduces background data processing and microphone activity. At the very least, for Siri users, switching to a keyboard shortcut instead of the “Listen for” feature keeps your MacBook from being in “always listening” mode for the wake words.

17. Lock Screen Message

Provide contact details in case you lose or misplace your MacBook.



RATING: a Good idea
TIME: 1 minute
DIFFICULTY: Easy

How to Access:

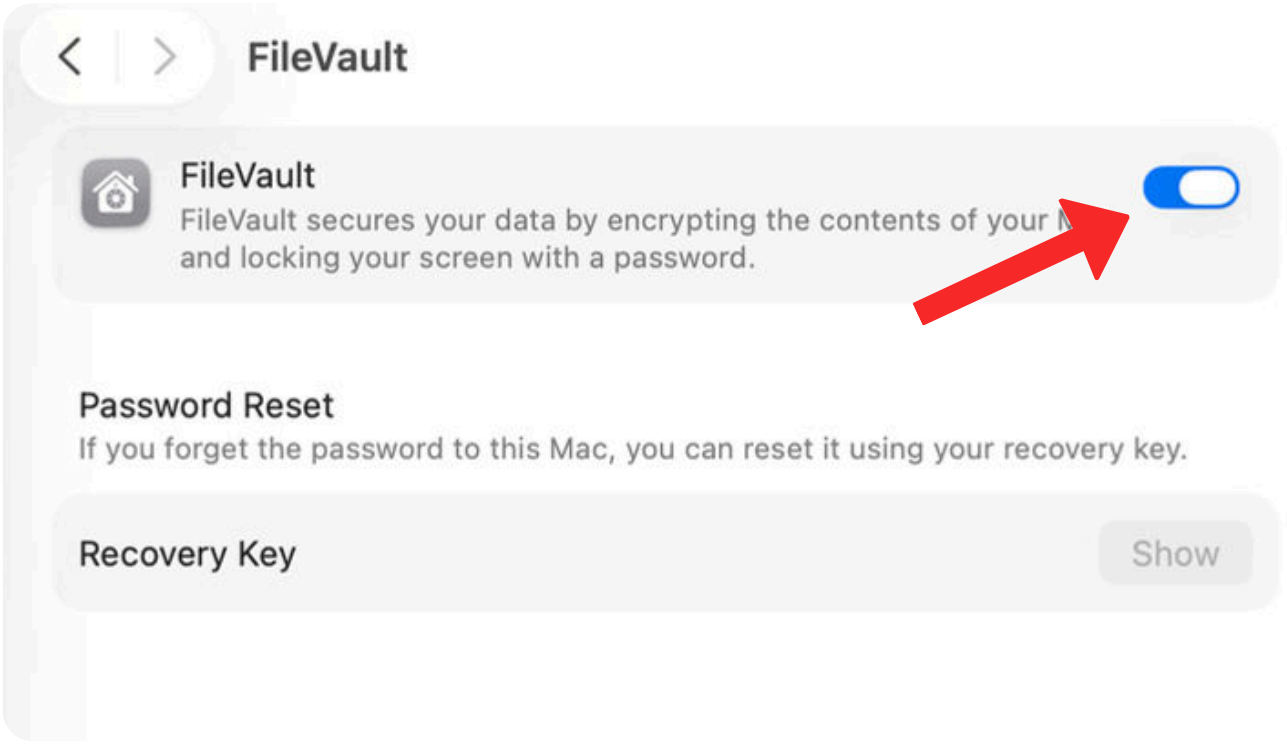
- Open your **System Settings**
- Click on **Lock Screen**
- Turn off **Apple Intelligence**
- Under **Show message when locked** click “Set”

Why is this important?

In the unlikely event that you lose or misplace your MacBook and a good samaritan finds it, how are they going to return it to you? Showing a message on the lock screen with some contact details such as a phone number or email address is a quick and easy solution. The message should read something like: “If found, please contact [phone/email]”

18. Filevault Encryption

Encrypt your entire hard drive.



RATING: Must Do
TIME: 1+ hours
DIFFICULTY: Medium

How to Access:

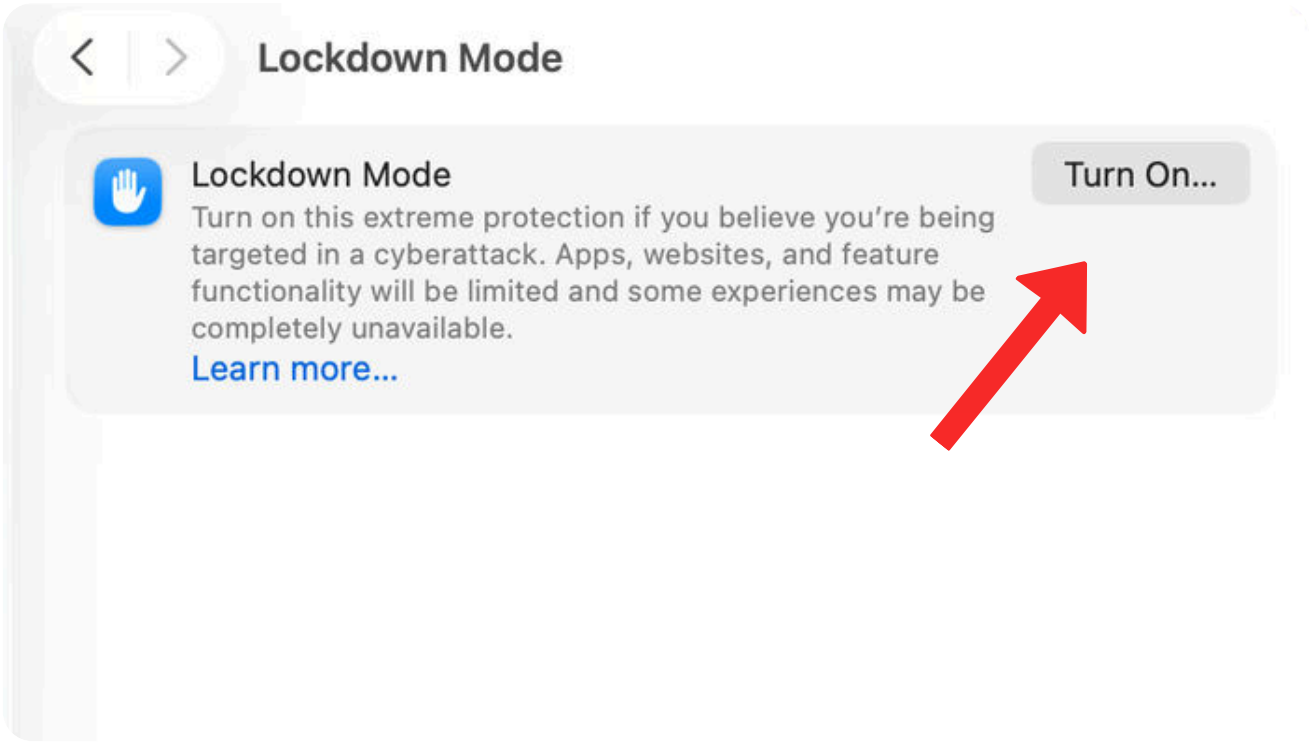
- Open your **System Settings**
- Click on **Privacy & Security**
- Click on **Filevault**
- Turn the toggle on

Why is this important?

FileVault ensures that even if someone removes your Mac's internal drive, your data remains unreadable. This is critical protection against physical theft. Everyone should enable FileVault, which is basically adding encryption to your hard drive. The only real cost is initial encryption time, which could be an hour for a new computer or multiple hours for an older computer.

19. Lockdown Mode

Add extreme protection against advanced targeted attacks.



RATING: Optional

TIME: 15 min

DIFFICULTY: Medium

How to Access:

- Open your **System Settings**
- Click on **Privacy & Security**
- Click on **Lockdown Mode**
- Turn the toggle on

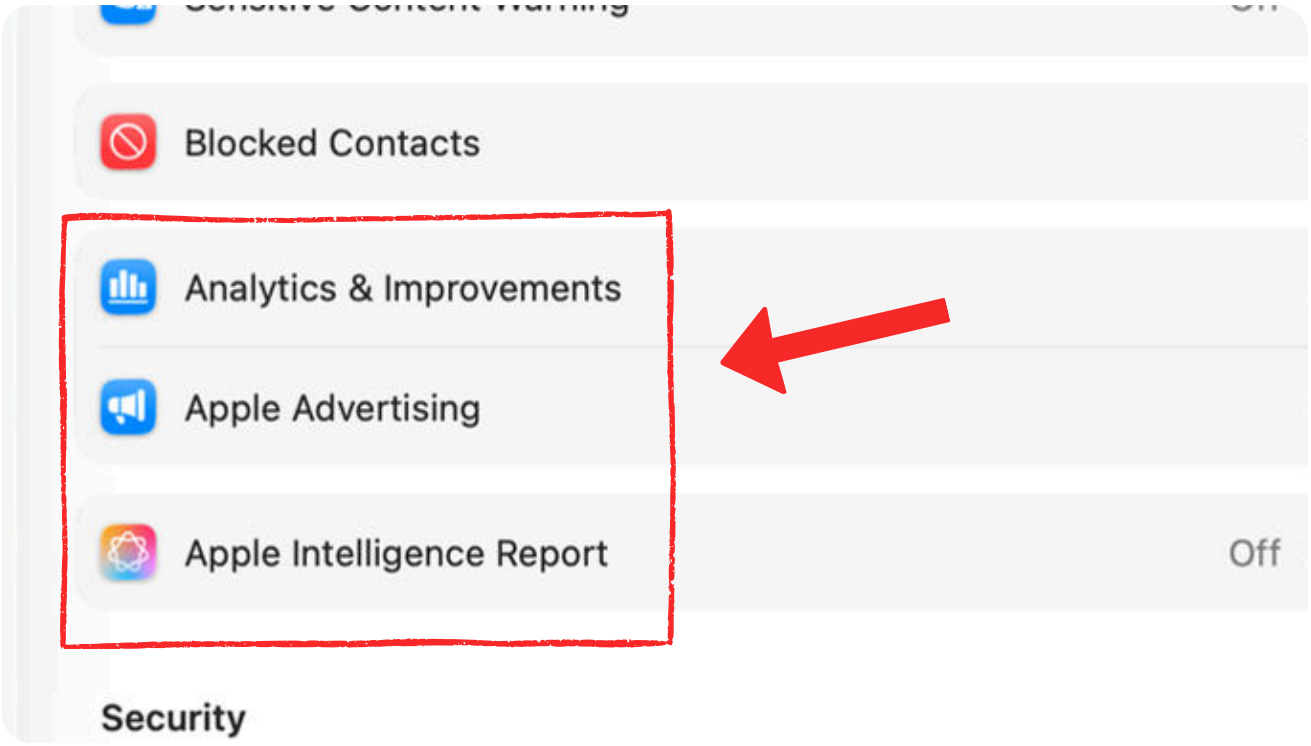
Why is this important?

Lockdown Mode restricts certain features to reduce exposure to sophisticated exploits. While designed for high-risk individuals, many users experience minimal disruption. If security is a priority, it's worth testing. If it introduces too much friction or inconvenience, you can easily reverse the decision and turn it off.

Watch our full Lockdown Mode Tutorial on YouTube.

20. Privacy Tweaks

Reduce unnecessary data sharing with Apple.



RATING: Optional
TIME: 1 minute
DIFFICULTY: Easy

How to Access:

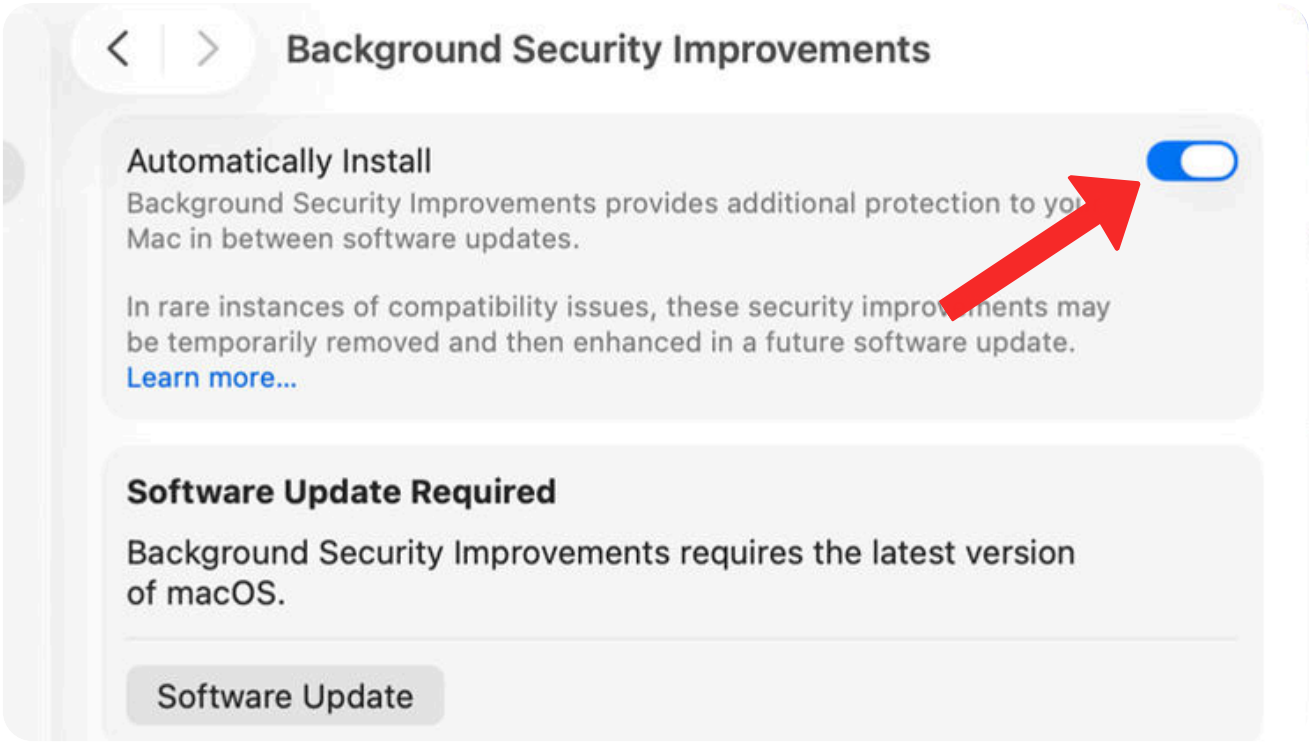
- Open your **System Settings**
- Click on **Privacy & Security**
- Turn off all settings in **Analytics & Improvements**, **Apple Advertising** and **Apple Intelligence Report**

Why is this important?

Turning off analytics and advertising personalization limits passive data collection. Adjusting app permissions ensures apps only access what they genuinely need. It's not much, but these small changes can add up to meaningful privacy and overall personal security improvements.

21. Background Security

Install silent security fixes in the background.



RATING: Must do
TIME: 1 minute
DIFFICULTY: Easy

How to Access:

- Open your **System Settings**
- Click on **Privacy & Security**
- Click on **Background Security Improvements**
- Turn the toggle on for **Automatically Install**

Why is this important?

This setting allows Apple to deploy critical fixes without waiting for major updates. While oddly separated from standard updates, it plays a crucial role in rapid response security. It should always remain enabled.