



Keep your Apple devices secure

A practical, senior-friendly review for your iPhone, Mac, and Apple Watch.

How to use this checklist

Check each box after you confirm the setting or action. You do not need to change every setting—focus on anything you do not recognize or have never reviewed.

01 Apple Account

- ☐ Two-factor authentication is turned on.
- ☐ Your trusted phone numbers and email addresses are current.
- ☐ You recognize every device listed as signed in to your Apple Account.
- ☐ Your Apple Account password is unique and not reused anywhere else.
- ☐ You know how you would recover your account if you lost your iPhone and Mac.
- ☐ Recovery Contacts or a Recovery Key are set up if appropriate for you.

02 iCloud

- ☐ You have reviewed what information is being synced to iCloud.
- ☐ You understand what Advanced Data Protection for iCloud does and whether you want to use it.
- ☐ You have considered how you would recover your account if you enabled stronger iCloud protection.

03 Passwords & Passkeys

- ☐ You have reviewed Apple Passwords for weak or reused passwords.
- ☐ You have checked for passwords that Apple identifies as compromised.
- ☐ You use passkeys when they are available and appropriate.
- ☐ Your primary email account has a strong, unique password and two-factor authentication.
- ☐ Important accounts such as banking, cloud storage, and your password manager have their own strong authentication.

Mac, iPhone & Apple Watch

Review the settings that protect the devices you use every day.

04 Passcodes & Biometrics

- ☐ Your iPhone uses a strong passcode that is not easy to guess.
- ☐ Your Mac uses a strong login password.
- ☐ Face ID is enabled for sensitive actions on your iPhone.
- ☐ Your Apple Watch has a passcode.
- ☐ You understand that Apple may occasionally require the underlying passcode or password instead of Face ID or Touch ID.

05 Mac Security

- ☐ macOS is set to install security updates automatically.
- ☐ FileVault is enabled.
- ☐ You have reviewed System Settings > Privacy & Security.
- ☐ You know which apps have Full Disk Access.
- ☐ You know which apps have Accessibility access.
- ☐ You have reviewed Screen Recording and Input Monitoring permissions.
- ☐ You have reviewed camera and microphone permissions.
- ☐ You have removed applications you no longer use, especially old or unsupported software.

06 iPhone Security

- ☐ iOS is up to date and automatic updates are enabled.
- ☐ You have reviewed Settings > Privacy & Security.
- ☐ You have reviewed which apps can use your location.
- ☐ You have reviewed Bluetooth, Local Network, Photos, Contacts, microphone, and camera permissions.
- ☐ You have reviewed Safety Check if you share information or location with other people.
- ☐ You understand that Lockdown Mode is intended for people facing unusually sophisticated security threats; it is not necessary for most people.

Find My, Watch & Home Wi-Fi

Protect the devices and connections around you.

07 Find My & Stolen Device Protection

- ☐ Find My is enabled on your iPhone.
- ☐ Find My is enabled on your Mac.
- ☐ Stolen Device Protection is enabled on your iPhone.
- ☐ You know how to use Find My if an Apple device is lost or stolen.

08 Apple Watch

- ☐ watchOS is up to date.
- ☐ A passcode is enabled.
- ☐ Wrist Detection is enabled.
- ☐ You understand that your Apple Watch security is closely tied to the security of its paired iPhone.

09 Home Wi-Fi

- ☐ Your Wi-Fi uses WPA2 or WPA3 security.
- ☐ Your Wi-Fi password is strong and unique.
- ☐ Your router's administrator password is not the manufacturer's default.
- ☐ Your router firmware is kept up to date.
- ☐ You recognize the devices connected to your home network.
- ☐ Guest or IoT devices are separated from your main network when practical.

Physical Security, Backups & Final Checks

Finish with the safeguards that matter if a device is lost, stolen, or damaged.

10 Physical Security

- ☐ Your devices lock automatically after a reasonable period of inactivity.
- ☐ You have reviewed what notifications can appear while the iPhone is locked.
- ☐ You avoid leaving an iPhone or Mac unattended while it is unlocked.
- ☐ Automatic login is disabled on your Mac.

11 Backups & Recovery

- ☐ Time Machine is backing up your Mac.
- ☐ You have a backup that is not continuously connected to your Mac, when practical.
- ☐ You know where your most important files are backed up.
- ☐ You have tested that important files can actually be restored.
- ☐ You know how you would recover your Apple Account if you lost your iPhone and Mac at the same time.

12 Account & Session Review

- ☐ You have reviewed signed-in devices and active sessions on your important accounts.
- ☐ Recovery email addresses and phone numbers are current.
- ☐ Two-factor authentication is enabled where available.
- ☐ You have removed third-party apps and services you no longer use.
- ☐ You have reviewed connected apps and account permissions.

The Stolen iPhone Test

Imagine someone takes your iPhone while it is unlocked. What could they access, change, or use to reset? Pay particular attention to email, Apple Account settings, saved passwords, financial apps, and messages.

The Stolen Mac Test

Imagine someone steals your Mac. Could they get to your files or accounts? FileVault, a strong login password, automatic locking, and current backups are key protections.