



PRIVATE ORCHARDS

The Private Orchards Privacy Guide

A friendly, step-by-step guide to a more private iPhone. Find your level, then do only what you need.

EVERYDAY

PRIVATE

HIGH-RISK

Free guide · For iOS 26 and iOS 27
privateorchards.com

Contents

Overview	2
What's your threat model?	3
1. The Basics	4
2. Apple Account security	5
3. Your recovery plan	6
4. Tracking, ads and location	7
5. Safari	8
6. Apps, permissions and keyboards	9
7. Safety Check	10
8. Find My and tracker alerts	11
9. Password manager	12
10. Email aliases and private email	13
11. Private Relay, DNS or VPN	14
12. Advanced Data Protection	15
13. Siri and Apple Intelligence	16
14. Security keys	17
15. Checking for hidden access	18
16. Lockdown Mode	19
Keep it up	20

Overview

Welcome. This free guide helps you make your iPhone more private, one small step at a time. You don't need to be technical, and you don't need to do everything.

Who it's for

Anyone with an iPhone. It works whether you just want fewer ads following you, or someone may be trying to get into your phone.

What's inside

- **A simple threat model.** Three short descriptions help you pick your level: Everyday, Private or High-risk.
- **Sixteen short guides.** Each one explains why it matters, lists what to do, and links to Apple's own help pages.

How to use it

1. Update your iPhone first: `Settings → General → Software Update`.
2. Read "What's your threat model?" and pick your level.
3. Do the guides for your level, in order. Each guide shows who it's for.
4. Come back every few months and run the short check-up at the end.

Settings paths look like this: `Settings → Privacy & Security → Tracking`. `[your name]` means the banner at the top of Settings. Can't find something? Pull down in Settings and search for it.

If someone close to you might be watching your phone, changing settings can alert them. Read the Safety Check guide first, and think about talking to a domestic-violence advocate before you change anything.

What's your threat model?

A threat model is a quick think about two things: **who might want your data**, and **what you'd lose if they got it**. For most people, that's advertisers and the risk of a lost or stolen phone. For some, it's a person who knows them, or someone with real resources.

Pick the level that sounds most like you. Levels stack: Private includes everything in Everyday, and High-risk includes everything.

EVERYDAY Everyday

Who it's for: most people. You want fewer ads and trackers following you, a stronger Apple Account, and a phone that's safe if it's lost or stolen.

Do guides 1–9. About an hour and a half in total.

PRIVATE Private

Who it's for: you want less of your life online or exposed. That means email aliases, private DNS or a VPN, and Advanced Data Protection for your iCloud data.

Do guides 1–13. About two and a half hours.

HIGH-RISK High-risk

Who it's for: someone close to you, such as a partner, ex or family member, may want access to your phone. Or you face harassment or doxxing, do public or sensitive work, or cross borders where officials may search your phone.

Do all 16 guides, and repeat the check-up often. If you're in danger, get specialist help too: a domestic-violence advocate, or a digital-security helpline for journalists and activists.

Guide	EVERYDAY	PRIVATE	HIGH-RISK
1–9 · The Basics to Password manager	✓	✓	✓
10–13 · Email aliases to Siri and Apple Intelligence		✓	✓
14–16 · Security keys to Lockdown Mode			✓

1. The Basics

For: **EVERYDAY** everyone · about 10 minutes

Why it matters. Your passcode is the lock on everything else. Your Lock Screen shows things to anyone holding your phone. And updates fix security holes that attackers may already be using.

What to do

1. Use a passcode of at least six digits: `Settings → Face ID & Passcode → Change Passcode`. Avoid birthdays and repeats.
2. Set `Settings → Display & Brightness → Auto-Lock` to **1 Minute**.
3. Learn the quick lock. Hold the **side button** and **either volume button** until the power-off screen appears, then tap **Cancel**. Your iPhone now needs your passcode to unlock.
4. Hide message previews: `Settings → Notifications → Show Previews` → **When Unlocked**.
5. In `Settings → Face ID & Passcode → Allow Access When Locked`, turn off what you don't need. Turn off **Control Center**, so a thief can't switch on Airplane Mode.
6. Wired accessories: open `Settings → Privacy & Security → Wired Accessories`. On a USB-C iPhone, choose **Ask for New Accessories**. On a Lightning iPhone, keep **Automatically Allow When Unlocked**.
7. Turn on everything in `Settings → General → Software Update → Automatic Updates`.
8. Turn on **Automatically Install** in `Settings → Privacy & Security → Background Security Improvements`.

Apple help

Set a passcode on iPhone

<https://support.apple.com/guide/iphone/set-a-passcode-iph14a867ae/ios>

Access features from the iPhone Lock Screen

<https://support.apple.com/guide/iphone/access-features-from-the-lock-screen-iphcd5c65ccf/ios>

Allow USB and other accessories to connect

<https://support.apple.com/en-us/111806>

Update iOS on iPhone

<https://support.apple.com/guide/iphone/update-ios-iph3e504502/ios>

Automatically install Background Security Improvements

<https://support.apple.com/guide/iphone/install-background-security-improvements-iph049680987/ios>

2. Apple Account security

For: **EVERYDAY** everyone · about 10 minutes

Why it matters. Your Apple Account holds your photos, messages, backups and Find My. If someone takes it over, they get all of that, and they can lock you out.

What to do

1. Open `Settings → [your name] → Sign-In & Security`. Check that two-factor authentication is on.
2. On the same screen, check the email addresses and phone numbers on your account. To remove one you no longer control, tap it, then tap **Remove from Account**. Then tap **Two-Factor Authentication** and remove any trusted phone number you don't control.
3. Give your Apple Account its own password, used nowhere else. A password manager helps (guide 9).
4. Go back to `Settings → [your name]` and scroll down to your devices. Remove any you don't recognise or no longer own.
5. Turn on Stolen Device Protection: `Settings → Face ID & Passcode → Stolen Device Protection`. Under **Require Security Delay**, choose **Always** for the most protection. It stops a thief who has seen your passcode from changing your password or turning off Find My.
6. Leave **Significant Locations & Routes** turned on. Stolen Device Protection needs it.
7. Review apps that use Sign in with Apple: `Settings → [your name] → Sign in with Apple`. Remove ones you no longer use.

Apple help

Keep your Apple Account secure on iPhone

<https://support.apple.com/guide/iphone/keep-your-apple-account-secure-iph904b71f28/ios>

Two-factor authentication for Apple Account

<https://support.apple.com/en-us/102660>

About Stolen Device Protection for iPhone

<https://support.apple.com/en-us/120340>

Use Sign in with Apple on iPhone

<https://support.apple.com/guide/iphone/sign-in-with-apple-iph238921d37/ios>

3. Your recovery plan

For: **EVERYDAY** everyone · about 10 minutes

Why it matters. Strong security can lock you out too, if you lose your phone or forget a password. A recovery plan makes sure you can always get back in. Do this before guides 12 and 14.

What to do

1. Add a second trusted phone number you control, ideally not on this iPhone: `Settings → [your name] → Sign-In & Security → Two-Factor Authentication → Add a Trusted Phone Number`.
2. Add a recovery contact: `Settings → [your name] → Sign-In & Security → Recovery Contacts → Add Recovery Contact`. Pick someone you trust who has an Apple device. They can give you a code, but they can't see your data.
3. Add a legacy contact: `Settings → [your name] → Sign-In & Security → Legacy Contact`. They can ask for access to your data after your death. Print the access key and keep it with your important papers.
4. Write down your password manager's recovery code or emergency kit, and keep it somewhere safe, offline.
5. **HIGH-RISK** Consider a recovery key: `Settings → [your name] → Sign-In & Security → Recovery Key`. It turns off Apple's usual account recovery. Write it on paper and keep copies in two safe places.

With a recovery key, Apple can't let you back in. If you lose it and your devices, you may lose your account for good. Don't store the key in Notes, Photos or Passwords.

My recovery contact: _____ · My legacy contact: _____

Where my recovery codes are kept: _____

Apple help

Set up a recovery contact for your Apple Account

<https://support.apple.com/en-us/102641>

How to add a Legacy Contact for your Apple Account

<https://support.apple.com/en-us/102631>

Set up a recovery key for your Apple Account

<https://support.apple.com/en-us/109345>

4. Tracking, ads and location

For: **EVERYDAY** everyone · about 10 minutes

Why it matters. Apps and advertisers build a profile from what you do and where you go. Your location history shows where you live, work and sleep. These switches cut most of it, and you won't miss a thing.

What to do

1. Open `Settings → Privacy & Security → Tracking`. Turn off **Allow Apps to Request to Track**.
2. Open `Settings → Privacy & Security → Apple Advertising`. Turn off **Personalized Ads**.
3. Open `Settings → Privacy & Security → Analytics & Improvements`. Turn everything off.
4. Open `Settings → Privacy & Security → Location Services`. For each app, choose **Never**, **Ask Next Time** or **While Using the App**. Turn off **Precise Location** for apps that only need a rough area, like weather.
5. Scroll down to **System Services**. Turn off the items you don't need, but leave **Find My iPhone**, **Emergency Calls & SOS** and **Significant Locations & Routes** on.
6. To delete your location history, tap **Significant Locations & Routes → Clear History**. Keep the setting itself on.
7. When you share a photo, tap **Options** at the top of the share sheet and turn off **Location**.
8. Open the Find My app → **People**. Stop sharing your location with anyone who doesn't need it.

Apple help

Control app tracking permissions on iPhone

<https://support.apple.com/guide/iphone/control-app-tracking-permissions-iph4f4cbd242/ios>

Control how Apple delivers advertising to you

<https://support.apple.com/guide/iphone/control-how-apple-delivers-advertising-to-you-iphf60a6a256/ios>

Control the location information you share

<https://support.apple.com/guide/iphone/control-the-location-information-you-share-iph3dd5f9be/ios>

Clear your location history in Maps

<https://support.apple.com/guide/iphone/clear-location-history-iph32b15b22f/ios>

5. Safari

For: **EVERYDAY** everyone · about 5 minutes

Why it matters. Your browser sees more of your life than any other app. Safari's best protections are built in. A few switches make them stronger and stop websites using your camera or location without asking.

What to do

All of these are in `Settings → Apps → Safari`.

1. Keep **Prevent Cross-Site Tracking** and **Fraudulent Website Warning** on.
2. Open **Hide IP Address**. With iCloud+, choose the option that hides your IP address from both trackers and websites. Otherwise, choose the trackers-only option.
3. Turn on **Require Face ID to Unlock Private Browsing**.
4. Check that **Advanced → Advanced Tracking and Fingerprinting Protection** is set to **All Browsing**. This is the default from iOS 26.
5. Set **Camera**, **Microphone** and **Location** to **Ask**, or **Deny** if you never use them on websites.
6. Under **Extensions**, turn off any you don't use.
7. Optional: choose a private **Search Engine**, such as DuckDuckGo.

Apple help

Customize your Safari settings on iPhone

<https://support.apple.com/guide/iphone/customize-your-safari-settings-iphb3100d149/ios>

Browse the web privately in Safari

<https://support.apple.com/guide/iphone/browse-the-web-privately-iphb01fc3c85/ios>

Get extensions to customize Safari

<https://support.apple.com/guide/iphone/get-extensions-iphab0432bf6/ios>

6. Apps, permissions and keyboards

For: **EVERYDAY** everyone · about 15 minutes

Why it matters. Every app that can see your photos, contacts, camera or microphone could leak them. Most apps ask for more than they need. App Privacy Report shows you what each app actually does.

What to do

1. In `Settings → Privacy & Security`, tap **Photos, Contacts, Camera, Microphone, Bluetooth** and **Local Network** in turn. Turn off any app that doesn't need it. For Photos and Contacts, choose **Limited Access** where you can.
2. Turn on `Settings → Privacy & Security → App Privacy Report`. After a week, look for apps using your location, camera or microphone when you weren't using them.
3. Delete apps you haven't used in months. It's the easiest privacy win there is.
4. Keyboards: open `Settings → General → Keyboard → Keyboards`. Delete keyboards you don't use. For any you keep, turn off **Allow Full Access** unless you really need it.
5. App Store: in `Settings → Apps → App Store`, keep **App Updates** on and turn off **Video Autoplay** and **In-App Ratings & Reviews**. To turn off personalized recommendations, go to `Settings → [your name] → Media & Purchases → View Account`.
6. Health: in the Health app, tap **Sharing** and stop sharing with anyone who doesn't need it. Then tap your picture → **Apps** and **Devices**, and remove what you don't use.
7. To lock a private app, touch and hold its icon, then tap **Require Face ID**.

Apple help

About App Privacy Report

<https://support.apple.com/en-us/102188>

Control access to information in apps

<https://support.apple.com/guide/iphone/control-access-to-information-in-apps-iph251e92810/ios>

Control access to hardware features

<https://support.apple.com/guide/iphone/control-access-to-hardware-features-iph168c4bbd5/ios>

Add or change keyboards on iPhone

<https://support.apple.com/guide/iphone/add-or-change-keyboards-iph73b71eb/ios>

Share your data in Health on iPhone

<https://support.apple.com/guide/iphone/share-your-health-data-iph5ede58c3d/ios>

Lock or hide an app on iPhone

<https://support.apple.com/guide/iphone/lock-or-hide-an-app-iph00f208d05/ios>

7. Safety Check

For: **EVERYDAY** everyone · about 5 minutes

Why it matters. Over time, we share our location, photos and notes with people and forget about it. Safety Check shows everything in one place, so you can stop what you no longer want. In an emergency, it can stop all sharing at once.

What to do

1. Open `Settings → Privacy & Security → Safety Check`.
2. Tap **Manage Sharing & Access**. Review by person and by app.
3. Stop sharing anything you don't recognise or no longer need.
4. **HIGH-RISK** In an emergency, tap **Emergency Reset**. It stops all sharing, resets app permissions and helps you secure your account.
5. **HIGH-RISK** Tap **Quick Exit** at any time to leave instantly. Changes you've made are kept.
6. Safety Check doesn't cover other companies' apps. Check location sharing in apps like Google Maps, Life360 and Snapchat yourself.

People aren't told when you stop sharing, but they may notice. If you're worried about how someone will react, make a plan first, ideally with an advocate.

Apple help

Manage information sharing with Safety Check

<https://support.apple.com/guide/iphone/manage-information-sharing-with-safety-check-iph42f0b2d53/ios>

Reset privacy and security settings in an emergency

<https://support.apple.com/guide/iphone/reset-privacy-security-settings-emergency-iph72e6a13f7/ios>

Apple Personal Safety User Guide

<https://support.apple.com/guide/personal-safety/welcome/web>

8. Find My and tracker alerts

For: **EVERYDAY** everyone · about 5 minutes

Why it matters. Find My helps you find a lost phone, and stops a thief from reusing it. Your iPhone can also warn you if someone hides an AirTag or similar tracker on you or in your car.

What to do

1. Open `Settings → [your name] → Find My → Find My iPhone`. Turn on **Find My iPhone**, **Find My network** and **Send Last Location**.
2. For tracker alerts, keep **Bluetooth**, **Location Services** and **Significant Locations & Routes** on, and Airplane Mode off.
3. Open `Settings → Notifications → Tracking Notifications` and turn on **Allow Notifications**.
4. If you get an alert such as "AirTag Found Moving With You", tap the alert, tap **Continue**, then tap **Play Sound** to find the tracker. Check bags, pockets and your car.
5. To identify a tracker, open Find My → **Items**, scroll to the bottom and tap **Identify Found Item**. For an AirTag, you can also hold the top of your iPhone near its white side. You'll see its serial number and the last four digits of the owner's phone number. Take a screenshot.
6. If you feel unsafe, go somewhere public and contact the police before you disable it. Disabling it means the owner stops getting updates, and they may notice.
7. To disable a tracker, tap **Instructions to Disable** in the alert and follow the steps. Alerts cover AirTags, some AirPods, Find My network accessories, and trackers built to the Apple–Google standard (iOS 17.5 or later).

Apple help

What to do if you get an alert that an AirTag or other tracker is with you

<https://support.apple.com/en-us/119874>

Detect unwanted trackers

<https://support.apple.com/guide/personal-safety/detect-unwanted-trackers-ips139b15fd9/web>

9. Password manager

For: **EVERYDAY** everyone · about 20 minutes

Why it matters. Most hacked accounts start with a reused or leaked password. A password manager makes a unique, strong password for every account and fills it in for you, so you only remember one.

What to do

1. Pick one. Apple's **Passwords** app is built in and free. **Bitwarden** is free, open source and works on any device. **Proton Pass** also creates an email alias for each account.
2. In Passwords, look for warnings about reused or leaked passwords. Fix the important ones first: email, banking and your Apple Account.
3. Switching apps? In the Passwords app, tap ... → **Export Data to Another App** and pick your new app, if it's listed. Passwords and passkeys move across with no file. If it isn't listed, export from `Settings → Apps → Safari → Export`, choose **Passwords**, import the file, then delete it. It isn't encrypted.
4. Turn on AutoFill for your app: `Settings → General → AutoFill & Passwords`. You can fill from up to three password apps. (`Settings → Apps → Default Apps → Passwords & Codes` is another way in.)
5. Turn on two-step login for your password manager. Keep its recovery code on paper.
6. Use passkeys where sites offer them. They're much harder to phish than passwords.

Apple help

Use passwords on iPhone

<https://support.apple.com/guide/iphone/use-passwords-iphd18e98624/ios>

Change weak or compromised passwords

<https://support.apple.com/guide/iphone/change-weak-or-compromised-passwords-iphd5d8daf4f/ios>

Automatically fill in strong passwords

<https://support.apple.com/guide/iphone/automatically-fill-in-strong-passwords-iphf9219d8c9/ios>

Export passwords to another password manager

<https://support.apple.com/guide/iphone/export-passwords-iphf28f2e93e/ios>

10. Email aliases and private email

For: **PRIVATE** Private and up · about 15 minutes

Why it matters. Your email address works like a username for your whole life. Use the same one everywhere, and anyone can link your accounts and match leaks. An alias gives each site its own address. Your real one stays private.

What to do

1. With iCloud+, open `Settings → [your name] → iCloud → Hide My Email`. Tap **Create New Address** for each new sign-up.
2. When an app offers **Sign in with Apple**, choose **Hide My Email**. The app gets a random address that forwards to you.
3. Turn on Mail Privacy Protection: `Settings → Apps → Mail → Privacy Protection` → **Protect Mail Activity**. It stops senders seeing when you open their emails.
4. Prefer another tool? **Proton Pass** and **SimpleLogin** also create aliases.
5. For a new main address, consider **Proton Mail** (end-to-end encrypted between Proton users) or **Fastmail** (private, but not end-to-end encrypted). Move important accounts over slowly.

Apple help

Create and manage Hide My Email addresses

<https://support.apple.com/guide/iphone/create-and-manage-hide-my-email-addresses-iphcb02e76f7/ios>

Use Mail Privacy Protection on iPhone

<https://support.apple.com/guide/iphone/use-mail-privacy-protection-iphf084865c7/ios>

11. Private Relay, DNS or VPN

For: **PRIVATE** Private and up · about 15 minutes

Why it matters. Your internet provider and the Wi-Fi you join can see which sites you visit. Websites see your IP address, which shows roughly where you are. Pick **one** of the three options below. Stacking them often breaks things.

What to do

1. **Easiest: iCloud Private Relay** (iCloud+). Turn it on at `Settings → [your name] → iCloud → Private Relay`. Under **IP Address Location**, choose **Maintain General Location**. It protects Safari and some app traffic, not everything.
2. **Block trackers everywhere: encrypted DNS**. Install a DNS app such as **NextDNS**, or its configuration profile, and turn on a tracker blocklist.
3. **Hide everything: a VPN**. Choose a trusted, audited provider such as **Proton VPN** or **Mullvad**. Turn on its kill switch. On iOS 16.1 and later, some Apple services can still bypass a VPN.
4. Whichever you pick, open `Settings → Wi-Fi`, tap ⓘ beside each network, set **Private Wi-Fi Address** to **Rotating**, and turn on **Limit IP Address Tracking**.
5. Set AirDrop to **Contacts Only**: `Settings → General → AirDrop`.

Apple help

About iCloud Private Relay

<https://support.apple.com/en-us/102602>

Protect web browsing with iCloud Private Relay

<https://support.apple.com/guide/iphone/protect-web-browsing-icloud-private-relay-iph499d287c2/ios>

Use private Wi-Fi addresses on Apple devices

<https://support.apple.com/en-us/102509>

Install or remove configuration profiles

<https://support.apple.com/guide/iphone/install-or-remove-configuration-profiles-iph6c493b19/ios>

Use AirDrop to send items to nearby devices

<https://support.apple.com/guide/iphone/use-airdrop-to-send-items-to-nearby-devices-iphcd8b9f0af/ios>

12. Advanced Data Protection

For: **PRIVATE** Private and up · about 15 minutes

Why it matters. By default, Apple holds the keys to most of your iCloud data, including backups, photos and notes. With Advanced Data Protection, only your devices hold the keys. Apple can't read that data, even after a breach or a legal request.

What to do

1. Finish your recovery plan first (guide 3). Apple can't recover this data for you.
2. Update every Apple device signed in to your account. Older devices may need to be removed.
3. Open `Settings → [your name] → iCloud → Advanced Data Protection` and tap **Turn On Advanced Data Protection**. Follow the steps.
4. iCloud.com access is off by default. Turn on **Access iCloud Data on the Web** only if you need it.

What it doesn't cover

- **Mail, Contacts and Calendars** stay readable by Apple, because those standards don't support end-to-end encryption.
- **iWork collaboration, Shared Albums** in Photos and "**anyone with the link**" sharing are not end-to-end encrypted.
- Advanced Data Protection isn't available to new users in the UK.

Apple help

Use Advanced Data Protection for your iCloud data

<https://support.apple.com/guide/iphone/use-advanced-data-protection-iph584ea27f5/ios>

iCloud data security overview

<https://support.apple.com/en-us/102651>

13. Siri and Apple Intelligence

For: **PRIVATE** Private and up · about 10 minutes

Why it matters. Siri and Apple Intelligence learn from your apps, messages and voice. Most processing happens on your iPhone or on Apple's Private Cloud Compute, but you can still choose how much they keep and what they can see.

What to do

1. Delete your Siri history: `Settings → Siri → Siri & Dictation History → Delete Siri & Dictation History`.
2. Using Siri AI (beta)? Delete old conversations in the Siri app, and choose a short time in `Settings → Siri → Keep Conversations`.
3. Limit what Siri learns from each app: `Settings → Siri → App Access`. Pick an app, then turn off **Learn from this App** for anything private, such as banking or health apps.
4. If you connected ChatGPT, review it or turn off **Use ChatGPT** (`Settings → Siri → ChatGPT`). With Siri AI: `Settings → Siri → Extensions → ChatGPT` → turn off **Use Extension**.
5. See what was sent to Apple's servers: `Settings → Privacy & Security → Apple Intelligence Report`. Choose the last 15 minutes or the last 7 days.
6. Turn off notification summaries for private apps: `Settings → Notifications → Summarize Notifications`.
7. In `Settings → Siri`, under Visual Intelligence, check that **Automatic Visual Look Up** (identifies things in your screenshots) and **Highlight to Search** (Siri AI only, searches the web) are off unless you use them.

Apple help

Apple Intelligence and privacy

<https://support.apple.com/guide/iphone/apple-intelligence-and-privacy-iphe3f499e0e/ios>

Change Siri settings on iPhone

<https://support.apple.com/guide/iphone/change-siri-settings-iphc28624b81abc/ios>

Turn on ChatGPT on iPhone

<https://support.apple.com/guide/iphone/turn-on-chatgpt-iph00fd3c8c2/ios>

Summarize notifications and reduce interruptions

<https://support.apple.com/guide/iphone/summarize-notifications-reduce-interruptions-iph1fbe7d2b9/ios>

14. Security keys

For: **HIGH-RISK** High-risk · about 15 minutes

Why it matters. A text code can be phished or stolen with a SIM swap. A physical security key can't. Once you add keys, signing in to your Apple Account on a new device needs the key, as well as your password.

What to do

1. Buy **two** FIDO-certified keys that work with your iPhone (NFC, USB-C or Lightning). Keep one somewhere safe as a spare.
2. Make sure every device is up to date. You need iOS 16.3 or later.
3. Open `Settings → [your name] → Sign-In & Security → Two-Factor Authentication → Security Keys` and tap **Add Security Keys**.
4. Follow the steps to add both keys. You can add up to six.
5. Review signed-in devices when asked, and sign out of any you don't use.
6. Label the keys, and keep the spare with your recovery papers (guide 3).

If you lose every key and every trusted device, you can be locked out for good. Always keep a spare.

Apple help

About Security Keys for Apple Account

<https://support.apple.com/en-us/102637>

Use security keys to sign in to your Apple Account

<https://support.apple.com/guide/iphone/use-security-keys-iph5acc5b28c/ios>

15. Checking for hidden access

For: **HIGH-RISK** High-risk · about 20 minutes

Why it matters. Someone who once had your passcode or Apple Account password may still have a way in. Usually it's a second Face ID, a signed-in device or a profile. This check finds the common ones. Remember: changes may be noticed.

What to do

- ☐ Signed-in devices: `Settings → [your name]`, then scroll down. Remove what you don't own.
- ☐ Change your Apple Account password and your passcode.
- ☐ Phone numbers and emails on your account (guide 2).
- ☐ Face ID: `Settings → Face ID & Passcode`. If **Alternate Appearance** is set up and it isn't you, tap **Reset Face ID**.
- ☐ Profiles: `Settings → General → VPN & Device Management`. Remove anything you don't recognise, unless it's from your employer.
- ☐ Family Sharing, Screen Time and the Home app: check who's in each.
- ☐ Paired devices: an Apple Watch in the Watch app, and `Settings → Bluetooth`.
- ☐ Apps you don't recognise, including hidden ones in the **Hidden** folder at the bottom of App Library.
- ☐ Location sharing in Find My and in other apps (guide 7).
- ☐ Optional: turn on Contact Key Verification in `Settings → [your name] → Contact Key Verification`.

Apple help

Apple Personal Safety User Guide

<https://support.apple.com/guide/personal-safety/welcome/web>

Install or remove configuration profiles

<https://support.apple.com/guide/iphone/install-or-remove-configuration-profiles-iph6c493b19/ios>

Use Contact Key Verification

<https://support.apple.com/guide/iphone/use-contact-key-verification-iph654dd8c53/ios>

16. Lockdown Mode

For: **HIGH-RISK** High-risk · about 5 minutes

Why it matters. Lockdown Mode is for the rare people who might be targeted by advanced spyware, such as journalists, activists and officials. It shuts off the features attackers use most often. Your iPhone will feel more limited, and that's on purpose.

What to do

1. Install any configuration profiles you need first. You can't add new ones while Lockdown Mode is on.
2. Open `Settings → Privacy & Security → Lockdown Mode`. Tap **Turn On Lockdown Mode**, then **Turn On & Restart**.
3. Expect changes. Most message attachments are blocked, some web features are off, FaceTime calls from people you haven't called in the past 30 days are blocked, and wired accessories won't connect while your iPhone is locked.
4. If a trusted site breaks, open it in Safari, tap the page menu → **Website Settings** and turn off Lockdown Mode for that site only.
5. Turn on Lockdown Mode on all your Apple devices. Full protection needs every device. A paired Apple Watch turns it on too.

Apple help

About Lockdown Mode

<https://support.apple.com/en-us/105120>

Harden your iPhone with Lockdown Mode

<https://support.apple.com/guide/iphone/use-lockdown-mode-iph845f6f40c/ios>

Keep it up

A private iPhone is a habit, not a one-off. Every three months, or after a big iOS update, spend ten minutes on this.

Quarterly check-up

- ☐ Install any updates waiting.
- ☐ Check your signed-in devices and remove old ones.
- ☐ Run Safety Check → **Manage Sharing & Access**.
- ☐ Look at App Privacy Report and remove any app that surprises you.
- ☐ Delete apps you haven't used.
- ☐ Fix new warnings in your password manager.
- ☐ After updates: re-check Tracking, Analytics and Location Services. New switches sometimes appear.
- ☐ Make sure your recovery contacts and codes are still current.

More from Private Orchards

The blog explains the "why" behind each step. It covers things like always-on VPNs, choosing a password manager and keeping your phone number private. Visit privateorchards.com.

Private Orchards is an independent project and is not affiliated with Apple Inc. Apple, iPhone, iCloud, Safari, Siri, AirTag and Face ID are trademarks of Apple Inc. Other product names are trademarks of their owners. Settings names can change between iOS versions. If a step doesn't match your iPhone, search Settings for the feature name. This guide contains no affiliate links.