



# **Personal Safety User Guide for Apple devices**



**Strategies and solutions**

# Contents

<b>Overviews</b>	<b>3</b>
Overview	3
What's new in personal safety	5
<b>Strategies and solutions</b>	<b>6</b>
Get safe guide	6
Stay safe guide	13
Safety Check	16
Checklists for devices with iOS 15 or earlier	33
<b>Limit account or device access</b>	<b>39</b>
Apple Account access	39
Device access	47
Passwords, passkeys, passcodes	63
<b>Manage location information</b>	<b>71</b>
Use Check In for Messages	71
Detecting unwanted trackers	75
Find My and location sharing	81
Manage Location Services settings	86
Manage automatic ETA sharing in Maps	88
Manage location metadata in Photos	90
<b>Manage content</b>	<b>93</b>
General	93
Specific apps and features	114
<b>Additional information</b>	<b>158</b>
Safety considerations	158
Other support resources	159
<b>Copyright</b>	<b>160</b>

# Overviews

## Personal safety overview



If you want to review, limit, stop, or prevent others from accessing your Apple devices, account, or personal information, this guide can help.



*Note:* This resource applies primarily to Apple devices with the latest operating systems (iOS 18, iPadOS 18, and macOS 15) but also applies to Apple Watch and HomePod.

### Not sure what you need?


- The [Get safe guide](#) can help with immediate solutions.
- The [Stay safe guide](#) can help with planning ahead.

## Looking for a specific solution?

- Review and manage what you're sharing (and with whom) using Safety Check or Checklists (see below).
- Access all of the content in this guide using the search field or table of contents (top left of every guide page), or use our topic-based indexes for more guidance.

## Safety Check

Safety Check offers an easy way to quickly review and manage the information you're sharing with apps and individuals—all on your iPhone with iOS 16 or later. To find your iOS version, go to Settings > General > About. To update, see "[Update your Apple software](#)" later in this guide.

To access Safety Check, use your iPhone to go to Settings  > Privacy & Security > Safety Check.

To learn more about Safety Check (requirements, directions, FAQs), see [Safety Check](#) later in this guide.

## Checklists

While many find Safety Check easier to use, Apple also offers checklists later in this guide to help you manually review and manage what you're sharing:

- [Checklist 1: Limit device and account access](#)
- [Checklist 2: Manage location information](#)
- [Checklist 3: Manage content](#)

## Offline help

If you want to reference this information later offline, you can:

- Download the full guide as a PDF using the *Download this guide* link (bottom left of all guide pages).
- Print individual pages using ⌘-P or Control-click > Print Page. To keep links clickable in your downloaded copy, choose Save as PDF in the lower-left PDF menu in your printer window.

## Other concerns

- [Apple Support](https://support.apple.com/) (https://support.apple.com/): Access solutions for all of your Apple products and services—including user guides, forgotten password help, and more.
- [Other support resources](#) (later in this guide)—If you feel your safety is at risk, these additional resources might be helpful.

This guide is updated regularly to provide you with the information you need to feel safe and secure while using Apple products. See [What's new](#) later in this guide.

# What's new in personal safety

## Apple ID name change

Apple ID is now called Apple Account. This is a global update across all Apple services.

## Personal Safety User Guide updates

Apple has made extensive changes to this guide, including:

### New content

- [Manage iPhone Mirroring](#) helps users see which Mac computers are set up for iPhone mirroring, revoke access, and adjust settings.
- [Lock or hide apps](#) offers peace of mind for users that don't want other people to get into certain apps.
- [Manage Screen Sharing and Screen Control](#) helps users understand what someone can do when viewing or controlling their screen.

### Improvements

- [Safety Check](#) includes a new bullet about iPhone Mirroring.
- [Checklist 1: Limit device and account access](#) includes new steps about iPhone Mirroring and changing your passcode and password.

# Strategies and solutions

## Get safe guide


If you or someone you know is concerned they might be experiencing technology-related stalking or harassment on an Apple related product, or wants to sever digital ties with someone, the strategies below can help. To connect with an advocacy organization providing support related to harassment, domestic violence, stalking, or other concerns, see the [Here to Help webpage](https://learn.appleservices.apple/here-to-help) (<https://learn.appleservices.apple/here-to-help>).

If you're looking for proactive ways to guard against future technology-related issues, see the [Stay safe guide](#) later in this guide.

## Strategies for getting safe

Use the steps below to help manage what you're sharing and secure your devices and accounts.

### Step 1. Safety first

 **IMPORTANT:** Before making changes or deleting information, [consider potential impacts to your safety](#).

You can download or print a copy of this Get safe guide for future reference by Control-clicking and selecting either Save Page As or Print Page.

### Step 2. Update your Apple software

To help secure your device, make sure all of your Apple devices have the latest operating system installed with the latest security and privacy updates. To learn how, see [Update your Apple software](#).

*Note:* Device updates may take time and device power to complete. If you're in an urgent situation or emergency, you may want to continue on to the next step.

### Step 3. Use guided solutions

Most tech-related personal safety issues relate to sharing and access. For guided help with these, use either:

- *Safety Check*: The fastest, easiest way to view and manage sharing directly on your iPhone. To learn how, see [Safety Check](#) later in this guide.

To access, use your iPhone with iOS 16 or later: Go to Settings > Privacy & Security > Safety Check. (You may need to scroll down.)

- *Checklists*: For iOS 15 or earlier, or for other Apple devices, see the following later in this guide:

- [Limit access](#)
- [Stop sharing](#)
- [Manage location](#)

### Step 4. Go further

Some things can't be reviewed or changed using the guided solutions. Review these important [additional steps](#).

This guide contains dozens of personal safety articles pertaining to devices, features, and settings. If you'd prefer help with a specific feature or issue, use:

- The search field (top left)
- This guide's table of contents (top left)
- Help for specific situations (below)

## Urgent measures

⚠ **IMPORTANT:** Before making changes or deleting information, [consider potential impacts to your safety](#) and privacy.

### Quick help

- Quickly stop all sharing using [Emergency Reset \(option one\)](#)
- [Make an emergency call or text on iPhone or Apple Watch](#)
- [Block calls and messages](#)
- [Reject unknown sign-in attempts](#)
- [Receive warnings about sensitive images and videos](#)
- [Securely control your Home accessories](#)
- [Manage Touch ID fingerprints](#)

### Gather evidence

- [Record suspicious activity](#)
- [Obtain evidence related to another Apple Account](#)

### Restore a device to factory settings

If you want to erase all information and settings—including any apps that were installed without your knowledge—and reset your privacy settings so you aren't sharing location with any people or apps, see [Restore device to factory settings](#).

### Lockdown Mode

If you believe you may have been targeted by a highly sophisticated cyberattack, such as by a private company developing state-sponsored mercenary spyware, see [Harden your devices with Lockdown Mode](#).



## Help for specific situations

It's recommended that you start with steps 1–4 above, but you can also use the sections below to quickly find articles that may be helpful to your situation.

### Someone always knows where I am

This may relate to someone sharing your Apple Account, a Family Sharing group, or location or content sharing (such as shared calendars or photos posted on social media or shared calendars).

Start with steps 1–4 above. If you're using checklists in Step 3, start with [Limit access](#) and [Manage location](#).

### I can't get into my Apple Account

To regain access to your Apple Account, consider the following Apple Support articles:

- [If you think your Apple Account has been compromised](#)
- [If your Apple Account is locked, not active, or disabled](#)
- [If you forgot your Apple Account password](#)
- [How to use account recovery when you can't reset your Apple Account password](#)

After your access is regained, consider the following:

- [Change your Apple Account — Apple Support article](#)
- [Secure your device, app, and website passwords](#)
- [Help prevent account and device lockouts](#)
- [Proactive ways to guard against future issues: Stay safe guide](#)

## **Someone locked me out of my device, or I can't unlock my device**

To regain access, see the Apple Support article [If you forgot your iPhone passcode, use your Mac or Windows device to reset it](#).

After your access is regained, consider these resources to help protect your device in the future:

- [Checklist 1: Limit device and account access](#)
- [Set a unique device passcode or password](#)
- Use [Touch ID](#) to secure your devices or delete unknown fingerprints
- [Secure your devices with Face ID](#) (iPhone or iPad)
- Consider adding an [account recovery contact](#)
- Consider taking precautionary measures using the [Stay safe guide](#).

## **I want to escape or am considering leaving a relationship that doesn't feel safe**

To connect with a victim advocacy organization that provides support related to harassment, domestic violence, stalking, or other concerns, see the [Here to Help webpage](https://learn.appleservices.apple/here-to-help) (<https://learn.appleservices.apple/here-to-help>).

1. Use guided solutions (above) to review your access and sharing preferences—and make changes if it's safe for you to do so.
2. Review these [urgent measures](#) to learn more about blocking, evidence collection, and more.
3. Review these [additional safety steps](#) that include unwanted tracking alerts, non-apple accounts, cellular plans, and more.

## **I need to protect something else**

## Access to your devices

Review Checklist 1: [Limit device and account access](#).

Also consider:

- [Set a unique passcode or password](#)
- [Help prevent being locked out](#)
- [Use Lockdown Mode](#)

To view more articles about protecting your devices and accounts, see the Table of Contents (upper left corner) under "Limit account or device access—articles."

## Your location

Review Checklist 2: [Manage location information](#).

Also consider:

- [Keep your browsing history private](#)

## Your content

Review Checklist 3: [Manage content](#).

Also consider:

- [Safely manage how you forward content—mail, text messages, and calls](#)
- [Sensitive image and video warnings](#)
- [Manage Photos sharing settings](#)
- [Manage location metadata in Photos](#)

## Your apps and browser

- [Passwords security](#)
- [Shared password and passkeys](#)
- [App privacy features](#)
- [Review and delete apps](#)
- [Third-party app settings](#)
- [Safari browsing history privacy](#)
- Messages
  - [Safety settings](#)
  - [Block calls and messages from certain people](#)
  - [Use Check In](#)
- Photos
  - [Manage Photos sharing settings](#)
  - [Manage location metadata](#)

## Your family and home

- [Family Sharing](#)
- [Home accessories](#)

## Which devices do you have?

### iPhone, iPad, and Mac

Nearly all Personal Safety User Guide content applies to iPhone, iPad and Mac.

- To review, limit, or stop others from accessing your devices, account, or personal information, see [Strategies for getting safe](#) earlier in this guide.
- If you're planning ahead to prevent others from getting access, see the [Stay safe guide](#).
- For additional ways to engage with the wide array of content in this user guide, see the [overview](#).

For other topics relating to these devices, see the [iPhone User Guide](#), [iPad User Guide](#), or [Mac User Guide](#).

### Apple Watch

For personal safety information relevant to Apple Watch, see:

- [Manage Activity sharing on Apple Watch](#)
- [Use Find My to manage location sharing](#)
- [Make an emergency text](#)
- [Secure NameDrop \(proactive\)](#)
- [Use Check In for Messages \(proactive\)](#)

For other topics, see the [Apple Watch User Guide](#).

### Home accessories

For personal safety information specific to Home, see [Securely control your Home accessories](#).

For other topics, see the [Home User Guide](#).

### AirTag

For personal safety information specific to AirTag, see [Detecting unwanted trackers](#).

For other topics, search [Apple Support](#) for "AirTag."

# Stay safe guide

This page is for anyone seeking to proactively protect against potential technology-enabled abuse, stalking, or harassment. If you're currently experiencing a related issue, see the [Get safe guide](#) earlier in this document. For other types of help with an Apple product or service, see [Other support resources](#) later in this document.

## Strategies for staying safe

Apple has many features to help support your personal safety and privacy. Here are some ways to leverage them:

### Level 1: Minimum protection

As a first line of defense, everyone should take these steps to protect their devices and Apple Account.

- Update the Apple software on all of your Apple devices to ensure you have the latest security and privacy updates. See [Update your Apple software](#). To learn how, see [Update your Apple software](#).
- Protect access to your devices:
  - [Set a unique passcode or password](#).
  - [Secure your iPhone or iPad with Face ID](#).
  - [Manage Touch ID fingerprints](#).
  - [Manage shared password and passkeys](#).

Secure your Apple Account:

- [Keep your Apple Account secure](#).
- [Use two-factor authentication](#).
- [Set up an account recovery contact](#).

## Level 2: Better protection

In addition to level 1, consider your apps, protecting related passwords, and the managing data you share with them.

- [Strengthen your device, app, and website passwords.](#)
- Review specific sharing settings:
  - Use Safety Check's [Manage Sharing & Access \(option two\)](#) option on iPhone with iOS 16 or later.
  - [Checklist 3: Manage content](#) (On other devices or iOS 15 or earlier).
  - [Secure AirDrop.](#)
  - [Secure NameDrop.](#)
  - [Manage shared Tab Groups in Safari.](#)
  - [Manage Shared with You settings.](#)
- Manage app privacy:
  - [App privacy features.](#)
  - [Review and delete apps.](#)
  - [Third-party app settings.](#)
  - [Safari and Maps: Keep your browsing history private.](#)

## Level 3: Best protection

In addition to levels 1 and 2, learn about Apple's personal safety tools and make safety a habit for best protection.

- Be prepared
  - [Enable tracking notifications.](#)
  - [Avoid fraudulent requests to share info.](#)
  - [Reject unknown sign-in attempts.](#)
  - [Learn how to block certain people.](#)
  - [Messages, AirDrop, FaceTime: Set up sensitive content warnings.](#)
  - [Consider using Check In for Messages to automatically let a friend know when you've arrived home.](#)
  - [Know how to make an emergency call or text](#) (iPhone or Apple Watch; country or region dependent).
- Make safety a habit
  - Take [additional steps](#) to protect your non-Apple Accounts, third-party apps, passwords and social media, as well as Home, Apple Wallet, and Family Sharing.
  - Use [Safety Check](#) on iPhone with iOS 16 or later at a regular cadence to manage what you're sharing.

Extras below


- [Manage Touch ID fingerprints.](#)
- [Harden your devices with Lockdown Mode.](#)
- [Manage safety settings in Messages.](#)
- [Obtain evidence related to another Apple Account.](#)


# Safety Check

## Safety Check for an iPhone with iOS 16 or later



Safety Check—a feature available through the Settings app on an iPhone with iOS 16 or later—allows you to quickly review, update and stop sharing your information with individual people and apps. Safety Check has two options:

- Manage sharing and access options to review and make individual changes.
- Use Emergency Reset to immediately stop sharing all information.

To access Safety Check, use your iPhone to go to Settings  > Privacy & Security > Safety Check.

 **IMPORTANT:** Before making changes or deleting information, [consider potential impacts to your safety](#) and privacy.

### Requirements

- Have an iPhone with iOS 16 or later.
  - To find your iOS version, go to Settings  > General > About.
  - To update from iOS 15.8.3 or earlier: Settings  > General > Software Update. See [Update your Apple software](#) for additional options.
- Have an Apple Account that uses two-factor authentication.
- Be signed in to Settings > [Your Name] on your iPhone.

*Note:* You may notice differences in Safety Check if your iPhone has Stolen Device Protection turned on. For more information, see the Apple Support article [About Stolen Device Protection for iPhone](#).

### Alternative: Checklists

If you're using a different device (iPad, Mac) or having trouble using Safety Check, you can adjust sharing and access manually using the following checklists:

- [Checklist 1: Limit device and account access](#)
- [Checklist 2: Manage location information](#)
- [Checklist 3: Manage content](#)



## Overview

Safety Check on iPhone allows you to quickly stop sharing your information, or to review and update sharing with individual people and apps. You can:

- Check whom you're sharing information with
- Review and change devices connected to your Apple Account
- Reset system privacy permissions for apps
- Change your iPhone passcode
- Change your Apple Account password
- Make additional changes



To view a video on how to use Safety Check on your iPhone, see "[Use Safety Check on your iPhone](https://www.youtube.com/watch?v=y9QX-0IVQL4)" (<https://www.youtube.com/watch?v=y9QX-0IVQL4>).

## Safety considerations before you begin

🚩 **IMPORTANT:** Plan for your safety.

- Before making changes or deleting information, [consider potential impacts to your safety](#) and privacy.
- Quick Exit helps you quickly protect your privacy. Tap Quick Exit to immediately close the Settings app and return to the Home Screen (top-right corner on all screens in Safety Check). Any changes you made before using Quick Exit are saved.
- To restart sharing with someone after using Safety Check, open the app or service you'd like to share information from and share that content again. Some apps or services notify you that you've resumed sharing information.


You can use Safety Check to check whom you're sharing information with, restrict Messages and FaceTime to your iPhone, reset system privacy permissions for apps, change your passcode, change your Apple Account password, and more.

If you want to restart sharing with someone after using Safety Check, open the app or service you'd like to share information from and share that content again.

If you have Stolen Device Protection turned on, Safety Check may work a little differently. To learn more about Stolen Device Protection, see the Apple Support article [About Stolen Device Protection for iPhone](https://support.apple.com/120340) (<https://support.apple.com/120340>).

**Note:** If your iPhone has Screen Time restrictions turned on or has a mobile device management (MDM) profile installed, you can still use Safety Check but some options may not be available.


## What do I need to use Safety Check?

Safety Check is available only on an iPhone with iOS 16 or later. To use Safety Check, you must have an Apple Account that uses two-factor authentication. You must also be signed in to Settings > [your name] on your iPhone. (To find the software version installed on your device, go to Settings  > General, then tap About.)

To access Safety Check, go to Settings  > Privacy & Security > Safety Check. (You may need to scroll down.)

**Note:** If you don't have access to Safety Check or you're having trouble using the feature, you can manually adjust your sharing settings and access to your device and accounts. See [Checklist 3: Manage content](#) later in this guide.

## Step 1: Open Safety Check

On your iPhone, go to Settings  > Privacy & Security > Safety Check. (You may need to scroll down.)

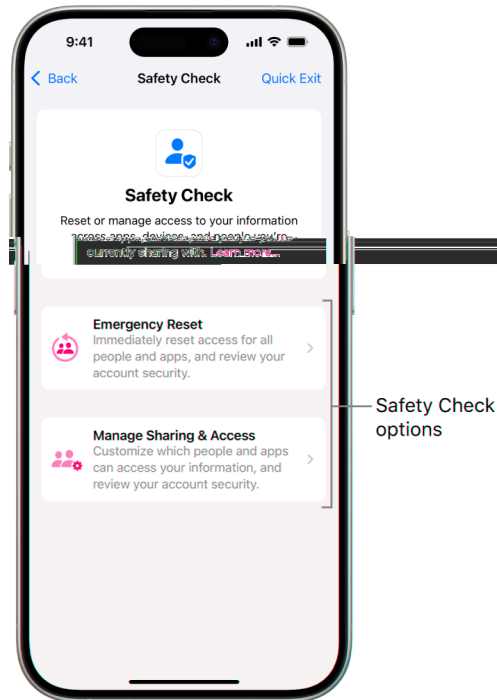


## Step 2: Choose an option

Safety Check offers two ways to manage sharing, access, and account security:

- *Emergency Reset*: Immediate and universal reset of sharing for all people and apps.
- *Manage Sharing & Access*: Review and customize sharing and access for individual people and apps.

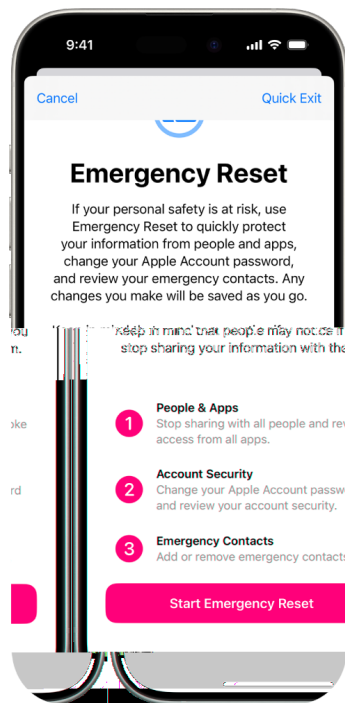
For specific details about what can be changed in Safety Check, see the [Safety Check FAQ](#) later in this guide.



## Emergency Reset (option one)

Use Emergency Reset to:

- Quickly stop sharing with all people and apps (see the [Safety Check FAQ](#) for specifics).
- Review your emergency contacts.
- Review devices connected to your Apple Account.
- Review phone numbers used to verify your identity.
- Change your Apple Account password and review device and account security.



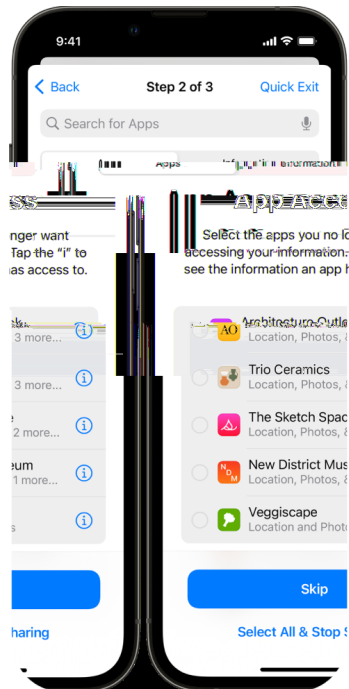
- Tap Emergency Reset, then follow the onscreen instructions. Progress is saved as you go.

*Note:* If you have Stolen Device Protection turned on, Safety Check may work a little differently. To learn more about Stolen Device Protection, see the Apple Support article [About Stolen Device Protection for iPhone](https://support.apple.com/HT212510) (<https://support.apple.com/HT212510>).

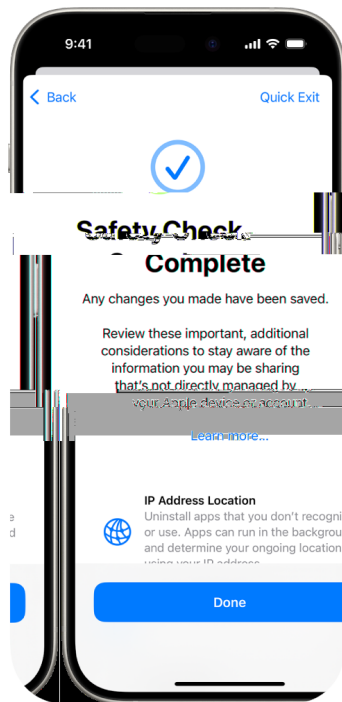
## Manage Sharing & Access (option two)

The Manage Sharing & Access option helps you review and manage information you're sharing with people, the information that apps have access to, and update your device and Apple Account security. Follow these five steps:

1. Tap Manage Sharing & Access. (Your changes are saved as you go.)
2. To review and stop sharing information with other people, either:
  - *Tap People:* Select people in the list, review the information shared with people, then decide which information you want to stop sharing with selected people.
  - *Tap Information:* Select apps in the list, review the information shared with people, then decide which information you want to stop sharing with selected people.
3. To review and stop sharing information with other apps, either:
  - *Tap Apps:* Select apps in the list, review the information shared with them, then decide which information you want to stop sharing with the selected apps.
  - *Tap Information:* Select the information being shared in the list, review the information shared with apps, then decide which information you want to stop sharing with the selected apps.



4. Tap Continue, then do any of the following:
  - Review and remove devices connected to your Apple Account.
  - Review and update phone numbers used to verify your identity.
  - Update your Apple Account password.
  - Add or update your emergency contacts.
  - Update your device passcode, or your Face ID or Touch ID information.
  - If you have synced computers, you can review and remove them (iOS 17 or later only).
  - If you have computers with iPhone Mirroring set up, you can review and remove them (iOS 18 or later only).
  - If you have iCloud+ and haven't yet turned on Private Relay, you can do so now (iOS 17 or later only).
5. Tap Done.

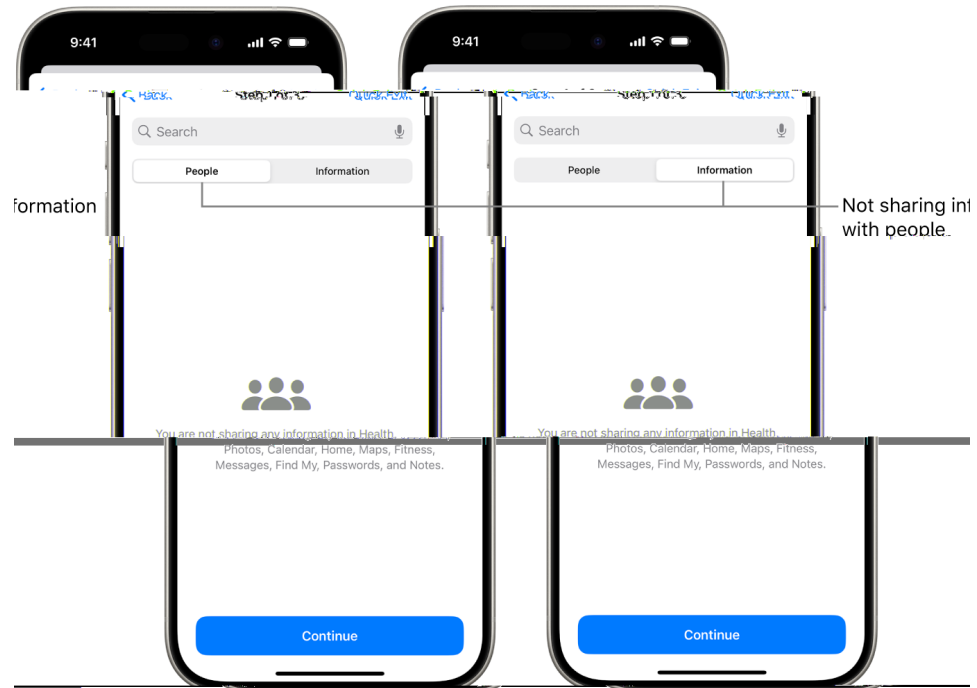


6. When you've finished, go to the next task to verify that you've stopped sharing.  
⚠ **IMPORTANT:** Review [additional steps](#) later in this guide to learn about tips for protecting your private information beyond Safety Check.

### Step 3: Verify your changes

After using Safety Check, you can confirm any changes you made to your sharing options using these 4 steps.

1. Tap the Back button (or you can quit and reopen Safety Check).
2. Verify that your intended changes have been made relating to the information you're sharing with people.

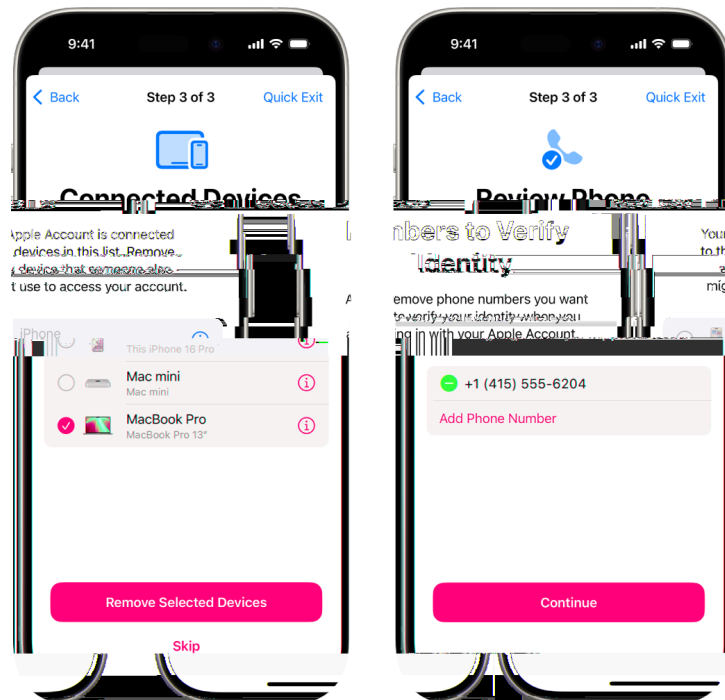




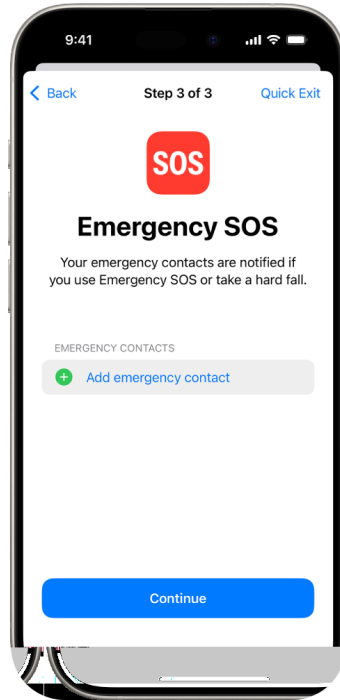
3. Verify that your intended changes have been made relating to the information you're sharing with apps.



4. Verify any account changes you made to:
  - Devices connected to your Apple Account.
  - Phone numbers used to verify your identity.



- Emergency contacts you added or changed.



- Synced computers you removed.



## Beyond Safety Check












Safety Check can't review or change some types of shared information, including:

- Non-Apple accounts and passwords.
- Social media sharing.
- Devices where you're signed in to a different Apple Account.
- An iPad or Mac with information sharing settings turned on for other apps.

## Safety Check FAQ
















### Which Apple apps and features can I review and manage in Safety Check?

You can use Safety Check to review or stop sharing information with other people from the following Apple apps:

App	Information you want to manage
	Activity
	Check In
	Health
	Home
	Shared Calendars
	Shared items in Find My
	Shared location using Find My
	Shared Maps ETA
	Shared Notes
	Shared Passwords
	Shared Photos (Including Shared Library and Shared Albums)

## What third-party app access can I review and manage in Safety Check?

You can use Safety Check to turn off third-party app access to the types of information listed below.

	Bluetooth®
	Calendars
	Camera
	Contacts
	Files and Folders
	Health
	Local Network
	Location Services
	Media and Apple Music
	Microphone
	Motion & Fitness
	Photos
	Reminders
	Research
	Speech Recognition

## What changes can I make to my Apple Account using Safety Check?

Safety Check can be used to modify information associated with your Apple Account. For example:

- Review and remove devices signed into your account.
- Review and update trusted phone numbers.
- Change your Apple Account password.
- Update your emergency contacts.
- Update your device passcode and your Face ID or Touch ID information.


If you have Stolen Device Protection turned on, Safety Check may work a little differently. To learn more about Stolen Device Protection, see the Apple Support article [About Stolen Device Protection for iPhone](https://support.apple.com/HT212510) (<https://support.apple.com/HT212510>).

## Why is there a Quick Exit button?


Individuals in abusive situations may need to rapidly hide their use of Safety Check. The Quick Exit button offers a way to do that.

## Additional safety steps

Most personal safety issues relate to sharing and access. For guided help managing these, use either:

- *Safety Check*: On your iPhone with iOS 16 or later, go to Settings  > Privacy & Security > Safety Check, or see [Safety Check](#).
- *Checklists*: For an earlier iOS or other devices, see the following checklists: [Limit Access](#), [Stop sharing](#), or [Manage location](#).

Some things can't be reviewed or changed using Safety Check or checklists. To further limit sharing, consider taking the additional steps below.

 **IMPORTANT:** Before making changes or deleting information, [consider potential impacts to your safety](#) and privacy.

## Non-Apple steps

### Non-Apple apps

Apps installed on your device may gather information about your general location. Taking into account any [potential impacts to your safety and privacy](#), you may want to review installed apps and delete the ones you don't use or recognize. See [Review and delete apps](#) and [Third-party app settings](#).

### Non-Apple accounts and passwords

Protect sensitive personal information in accounts like banking, shopping, email, social media, education:

- Change account passwords.
- Review security and privacy settings.
- Review communications accounts (email, phone, messaging) to make sure nothing is being forwarded without your permission.

### Social media, shopping, and other accounts

Posting photos and other personal information on social media, shopping, or other websites can reveal details about your location and personal life. Be sure you:

- Check the privacy and security settings in your social media, shopping, and other web based accounts
- Review your lists of connections and followers
- Think carefully about what you post to attain the level of privacy you need
- Manage location metadata in Photos

See "[Manage location metadata in Photos](#)" later in this guide.

### **Other devices you own or use**

Check sharing and access settings for any other devices you use to help secure your information. To learn how, see the [Limit device and account access](#) checklist. If anyone else is with you, like a child or friend, be aware that their devices may also be sharing information.

### **Cellular plan**

If you're part of a shared cellular plan, other members of the plan may have access to your location, call and messaging activity, or billing details. Contact your carrier to learn more about your plan and to see what additional safety measures can be placed on your account, such as an access PIN or security code, before changes can be made.

If you don't have a shared plan but someone else has online access to your cellular plan account, they may also have access to your location, call and messaging activity, or billing details. Taking into account any [potential impacts to your safety and privacy](#), you may want to consider updating your the passwords, pins, and any other security features associated with your cellular plan.

## Apple-related steps

### Unwanted tracking

Consider enabling notifications to detect unwanted trackers (like AirTag or other Find My network accessories). To receive alerts if one of these is moving with you, turn on:

- Bluetooth
- Location Services
- Tracking Notifications (open the Find My app, tap Me, scroll to Customize Tracking Notifications, then turn on Allow Notifications)

See "[Detecting unwanted trackers](#)" later in this guide.

### Home and HomeKit

If you're a member of an Apple home and decide to remove yourself, consider that the person who manages the home can still use HomeKit accessories, like cameras, that could impact your personal safety.

See "[Securely control your Home accessories](#)" later in this guide.

### Apple Wallet

If you share financial cards or access keys with someone in Apple Wallet, the person you're sharing with may be able to view your purchase history or when you unlocked your door.


Details of financial transactions may also be viewed through shared bank accounts and shared credit cards, or if someone else has online access to your financial accounts.

To review your recent transactions and logs, open Apple Wallet. Taking into account any [potential impacts to your safety and privacy](#), you may want to consider updating the passwords associated with your bank and credit cards.

### Family Sharing

If you're a member of an Apple Family Sharing group, the Family Sharing organizer may be able to see the purchases you've made and make changes to a child's device settings. To leave a family group, go to Settings, tap your name, and open Family Sharing settings. Although you can't remove a child account from a Family Sharing group, you can move the child account to another Family Sharing group or simply delete its Apple Account.

See "[Manage Family Sharing settings](#)" later in this guide.

**Note:** To see if you're part of a Family Sharing group, go to Settings  > [your name] > Family Sharing tab. If you see family members names, you're in a Family Sharing group.



# Checklists for devices with iOS 15 or earlier

## Checklist 1: Limit device and account access


Securing access to your devices and Apple Account is critical to tech-related personal safety. This checklist offers related pathways you can review and update to help you limit your device sharing to only those you want to grant access to.

▼ **IMPORTANT:** If you have an iPhone with iOS 16 or later, you can use the [Safety Check](#) feature.

▼ **IMPORTANT:** If you have an iPhone with iOS 16 or later, you can use the [Safety Check](#) feature, shown earlier in this guide.



## Limit access to your devices


1. Change the passcode on your iPhone and iPad, and change the login password on your Mac. To learn how, see [Set a unique device passcode or password](#) later in this guide.
2. Review devices signed in to your Apple Account by going to Settings  > [your name] > Devices. To remove a device you don't recognize, tap the device name and select "Remove from Account." For more information, see [Keep your Apple Account secure](#) later in this guide.
3. Check your devices for an unexpected [Face ID](#) appearance or [Touch ID fingerprint](#). See Face ID and Touch ID information later in this guide.
4. Review your Apple Account's personal and security information by signing in to the [Apple Account website](#). For more information, see [Keep your Apple Account secure](#) later in this guide.
5. If you're using [two-factor authentication](#), check the trusted devices for any you don't recognize. See two-factor authentication later in this guide.
6. Review apps installed on your device for any you don't recognize or remember installing. To learn how, see [Review and delete apps](#) later in this guide.
7. Determine whether iPhone Mirroring is set up, and revoke access if necessary. To learn how, see [Manage iPhone Mirroring on your iPhone or Mac](#) later in this guide.
8. Look for a potential unknown mobile device management (MDM) configuration profile. MDM profiles are typically installed by employers, schools, or other official organizations. To learn how, see [Review and delete configuration profiles](#) later in this guide.
9. Review and manage what you're sharing using the checklist [Checklist 3: Manage content](#) later in this guide.

## Checklist 2: Manage location information



If you're using an iPhone with iOS 15 or earlier, use this checklist to limit who can see your location or to stop sharing your location entirely. If you're using an iPhone with iOS 16 or later, see [Safety Check](#).



1. If you don't have the latest version of iOS, iPadOS, or macOS and are concerned someone may have had physical access to your device, you can restore the device to factory settings. A factory restore erases all the information and settings on your device. This includes removing any apps that were installed without your knowledge and resetting your privacy settings so you aren't sharing location with any people or apps. The factory restore also installs the latest version of the operating system. To restore it to factory settings, see [Restore device to factory settings](#).

2. To stop sharing your location with all apps and services for even a short period of time, go to Settings  > Privacy > Location Services and turn off location sharing. This stops all apps on your device, even Maps, from using your location. No one is notified if you turn off Location Services, but some features may not work as expected without access to your location.

*Note:* You can also temporarily turn off Find My iPhone in the same tab if you're concerned someone may have access to your iCloud account. In the list of apps using Location Services, tap Find My, then select Never.

3. To stop sharing your location with certain apps and services, go to Settings  > Privacy > Location Services, then choose the apps and services you want to stop sharing with. Tap the app name, then under Allow Location Access, select Never.
4. To stop sharing your location with a particular person, open the Find My app , tap People, select a person, then tap Stop Sharing My Location at the bottom of the screen.

If you started—and later stopped—sharing your location in Find My, the person isn't notified and can't see you in their list of friends. If you reenable sharing, they get a notification that you've started sharing your location with them.

5. To stop sharing your estimated time of arrival (ETA) in Maps, open Maps, select Favorites to open a window containing all of the locations you've designated as a Favorite. Tap ⓘ next to each location you want to review automatic ETA sharing settings, then scroll down to the Share ETA section and remove the person you want to stop sharing with.
6. To check which devices and accessories are currently available through Find My to anyone who has access to your Apple Account, go to Find My, tap Devices and review the list. If there's a device you don't recognize and want to remove it, tap the device, then tap Remove This Device.

*Note:* If you're part of a Family Sharing Group, members of your sharing group that have allowed you to see the location of their devices will be listed, separated by owner name.


7. When photos and videos that include location metadata are shared, the people you share them with may be able to access the location metadata and learn where it was taken. If you're concerned about someone having access to the location metadata associated with your photos or videos, you [can remove the current metadata](#) and stop it from being collected in the future.

## Checklist 3: Manage content

If you're using an iPhone with iOS 15 or earlier, use this checklist to learn how to stop sharing with someone you previously shared with. If you're using an iPhone with iOS 16 or later, see "[Safety Check for an iPhone with iOS 16 or later](#)" earlier in this guide.



1.

6. If you have an Apple Watch and shared your Activity rings with someone, you can choose to stop sharing. On iPhone, go to the Activity app , then tap Sharing. Tap a person you share with, tap their name, then tap either Remove Friend or Hide my Activity.
7. You can also choose to share information with others using third-party apps. Conduct a review of apps you've installed on your device to see if any of them are sharing information. See [Manage Photos sharing settings](#).

# Limit account or device access

## Apple Account access

### Keep your Apple Account secure

Your Apple Account is the personal account you use to sign in to your devices and access Apple services, like the App Store, iCloud, Messages, FaceTime, and Find My. It also includes personal information that you store with Apple and share across devices, like contacts, payment info, photos, device backups, and much more. If someone else has access to your Apple Account, they can view information that is synced across devices, which may include such things as Messages and location. Learn here how to secure your Apple Account on iPad, iPhone, and Mac.



Below are a few important things you can do to secure your Apple Account and protect your privacy.



## Secure your Apple Account

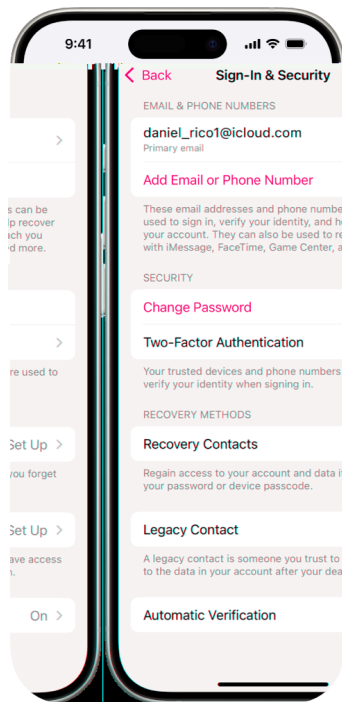
1. Don't share your Apple Account with anyone, even family members, partners, and close friends. If you share an Apple Account, you're giving someone else access to all your personal data and your content. If someone else set up your Apple Account and password for you or has had access to your password, you should change your password.
2. Use two-factor authentication for your Apple Account. Two-factor authentication is designed to ensure that you're the only person who can access your account, even if someone else knows your password. With two-factor authentication, you'll need to provide both your password and a six-digit verification code that automatically appears on your trusted devices when you want to sign in to a new device for the first time.  
  
To enroll in two-factor authentication, you must verify at least one trusted phone number—a number where you can receive verification codes by text message or automated phone call.
3. Pay attention to notifications about your Apple Account. Apple notifies you by email, text, or push notification when changes are made to your account, such as when there's a sign-in for the first time on a new device or when your password is changed. For this reason, be sure you keep your contact information up to date.  
  
See "[Reject unknown sign-in attempts](#)" earlier in this guide.
4. If you receive a notification that there was a sign-in attempt or that changes were made to your account that you didn't authorize, this could mean someone has accessed or is trying to access your account.



## Check and update your Apple Account security information

To help ensure that the personal information connected to your Apple Account is yours:

1. Do one of the following:
  - *On your iPhone or iPad:* Go to Settings  > [your name].
  - *On your Mac:* Choose Apple menu  > System Settings, then click your name at the top of the sidebar.
  - *In a web browser on your Mac or Windows device:* Go to the [Apple Account website](https://account.apple.com) (https://account.apple.com).
2. In the Sign-In & Security section, update any information that isn't correct or that you don't recognize, including your name, and the phone numbers and email addresses where you're reachable.







3. Do one of the following:
  - If you have two-factor authentication turned on, review your trusted devices. If you see devices that you want to remove from your account, follow the directions in the next section.
  - If you haven't yet set up two-factor authentication, see "[Use two-factor authentication](#)" later in this guide.

## Secure your account and remove unknown devices

If there are devices connected to your Apple Account that you don't recognize or haven't authorized to use your account, you can secure your account and remove them using the steps below. Removing an unknown device helps ensure that it can no longer display verification codes and that access to iCloud (and other Apple services on the device) is blocked until you sign in again with two-factor authentication.

You may also want to take a screenshot of the devices for documentation before securing your account.

Follow the steps below to review your account information and protect your account.


1. If you want to change your password:
  - *On your iPhone or iPad:* Go to Settings  > [your name] > Sign-in & Security > Change Password. Choose a strong password (eight or more characters, including upper and lowercase letters, and at least one number).
  - *On your Mac:* Choose Apple menu  > System Settings, then click your name at the top of the sidebar. Click Sign-In & Security, then click Change Password.
2. If you want to change the email address associated with your Apple Account for added safety, open Safari  and sign in to the [Apple Account website](https://account.apple.com) (https://account.apple.com). Select Account, and under your current Apple Account, select Change Apple Account, then enter the new email address you want to use.
3. If you want to remove the devices you don't want connected to your account:
  - *On your iPhone or iPad:* Go to Settings > [your name], scroll down to the list of devices, tap the device you want to remove, then tap Remove from Account.
  - *On your Mac:* Choose Apple menu  > System Settings, then click your name at the top of the sidebar. Scroll down to the list of devices, click the device you want to remove, then click Remove from Account.

## Use two-factor authentication

Two-factor authentication is an extra layer of security for your Apple Account designed to ensure that you're the only person who can access your account, even if someone knows your password. You can set up two-factor authentication on your iPhone, iPad, and Mac.



### Set up two-factor authentication on your iPhone or iPad

1. Go to Settings  > [your name] > Sign-in & Security.
2. Tap "Turn on two-factor authentication," then tap Continue.
3. Enter a trusted phone number, a phone number where you want to receive verification codes for two-factor authentication (it can be the number for your iPhone).

You can choose to receive the codes by text message or automated phone call.

4. Tap Next.
5. Enter the verification code sent to your trusted phone number.


To send or resend a verification code, tap "Didn't get a verification code?"

You won't be asked for a verification code again on your iPhone unless you do one of the following:

- Sign out completely
- Erase your iPhone
- Sign in to your Apple Account from the Apple Account webpage
- Need to change your Apple Account password for security reasons

After you turn on two-factor authentication, you have a two-week period during which you can turn it off. After that, you can't turn off two-factor authentication. To turn it off, open your confirmation email and click the link to return to your previous security settings. Keep in mind that turning off two-factor authentication makes your account less secure and means you can't use features that require a higher level of security.

## Set up two-factor authentication on your Mac

1. Choose Apple menu  > System Settings, click your name at the top of the sidebar, then click Sign-in & Security.
2. Click Set Up Two-Factor Authentication, then click Continue.
3. Answer the verification questions, then click Verify.
4. Enter your phone number for verification, select a verification method, then click Continue.
5. When asked, verify your identity with the six-digit verification code sent to your trusted phone. You won't be asked for a verification code again on your Mac unless you sign out of your Apple Account completely, erase your Mac, or need to change your password for security reasons.

## Security keys for Apple Account

A security key is a small external device that looks like a thumb drive or tag, and that can be used for verification when [signing in to your Apple Account](#) using two-factor authentication. Security Keys for Apple Account is an optional advanced security feature designed for people who want extra protection from targeted attacks, such as phishing or social engineering scams. Because you use a physical key instead of the six-digit code, security keys strengthen the two-factor authentication process and help prevent your second authentication factor from being intercepted or requested by an attacker.

To learn more about security keys, see the Apple Support article "[About Security Keys for Apple Account](https://support.apple.com/102637)" (<https://support.apple.com/102637>).

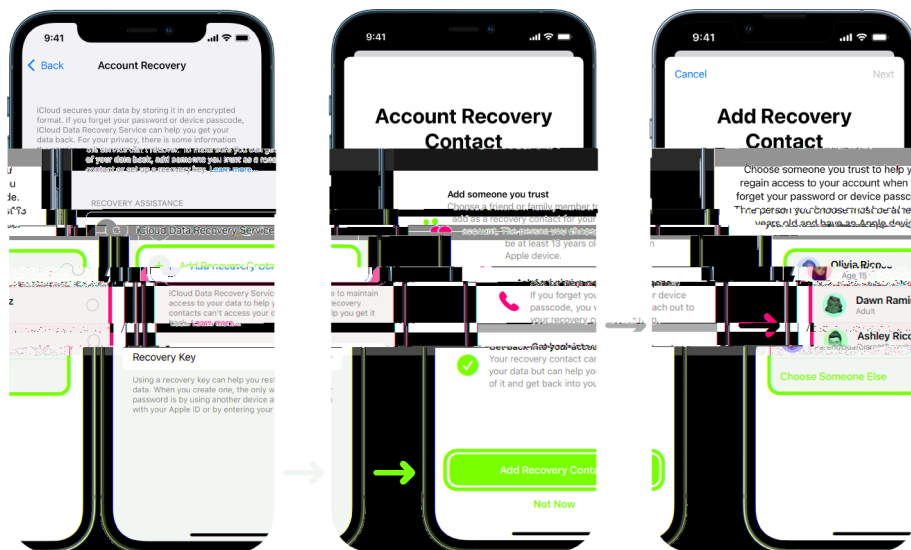
## Help prevent Apple Account and device lockouts

Account recovery contacts are trusted people who can help you regain access to your account if you forget your password or device passcode, or if your password or passcode was changed without your permission. Account recovery contacts don't have access to your account; they only have the ability to send you an account recovery code if you need one. Set up an account recovery contact on your iPhone, iPad, or Mac so that you can regain access to your data if you ever get locked out.





*Note:* In addition to a recovery contact, a *Legacy Contact* is the easiest, most secure way to give someone you trust access to the data stored in your Apple Account after your death. See the Apple Support article "[How to add a Legacy Contact for your Apple Account](https://support.apple.com/102631)" (<https://support.apple.com/102631>).

To be an account recovery contact, the person must be over the age of 13, have a device with iOS 15, iPadOS 15, macOS 12, or later, have two-factor authentication turned on for their Apple Account, and have a passcode set up on their device.





## Set up an account recovery contact

If you're concerned that someone may access your account to change your password and lock you out of your account, you can set a trusted account recovery contact to help you regain access.

1. Do one of the following:
  - *On your iPhone or iPad:* Go to Settings  > [your name], then tap Sign-in & Security.
  - *On your Mac:* Choose Apple menu  > System Settings, click your name at the top of the sidebar, then click Sign-in & Security.
2. Select Account Recovery, add a recovery contact, then authenticate with Face ID, Touch ID, a passcode or password.
3. If you're in a Family Sharing group, the members of the group are recommended. Or you can choose one of your contacts.
4. If you select a family member, they're added automatically. If you select a contact, they must accept the request.
5. After they accept your request, you see a message that they've been added as your account recovery contact.

## View and remove a recovery contact

If you want to view or remove your recovery contact.

1. Do one of the following:
  - *On your iPhone or iPad:* Go to Settings  > [your name], then tap Sign-in & Security.
  - *On your Mac:* Choose Apple menu  > System Settings, click your name at the top of the sidebar, then click Sign-in & Security.
2. Under Recovery Assistance, you see a list of your recovery contacts.
3. Choose the Recovery Contact you want to remove, then remove the contact.

# Device access

## Manage Touch ID fingerprints

Use Touch ID to securely and conveniently unlock iPhone, iPad, or Mac, authorize purchases and payments, and sign in to many third-party apps by pressing the Home button with your finger or thumb.

To use Touch ID, you must first set up a passcode on your iPhone, iPad, or Mac.


▼ **IMPORTANT:** Before making changes or deleting information, [consider potential impacts to your safety](#) and privacy.



## Secure your devices with Touch ID

To use Touch ID, you must first set up a passcode on your iPhone or iPad.



### Set up Touch ID on your iPhone or iPad

1. If you didn't turn on fingerprint recognition when you first set up your iPhone or iPad, go to Settings  > Touch ID & Passcode.
2. Turn on any of the options, then follow the onscreen instructions.

*Note:* If you can't add a fingerprint or unlock your iPhone or iPad using Touch ID, see the Apple Support article "[If Touch ID isn't working on your iPhone or iPad](#)" (<https://support.apple.com/101612>).


## Set up Touch ID on your Mac or Magic Keyboard

To use Touch ID, you must first set up a password on your Mac.

1. Choose Apple menu  > System Settings, then click Touch ID & Password  in the sidebar.
2. Click Add Fingerprint, enter your password, then follow the onscreen instructions.  
If your Mac or Magic Keyboard has Touch ID, the sensor is located at the top right of your keyboard. You can add up to three fingerprints to your user account (and you can save up to five fingerprints total on your Mac).
3. Click the checkboxes to select how you want to use Touch ID:
  - *Unlocking your Mac:* Use Touch ID to unlock this Mac when you wake it from sleep.
  - *Apple Pay:* Use Touch ID to complete purchases you make on this Mac using Apple Pay.
  - *iTunes Store, App Store & Apple Books:* Use Touch ID to complete purchases you make on this Mac from the Apple online stores.
  - *Password AutoFill:* Use Touch ID to automatically fill in user names and passwords and to automatically fill in credit card information when requested while using Safari and other apps.
  - Use Touch ID sensor for fast user switching: Use Touch ID to switch Mac user accounts.

## Delete unknown Touch ID fingerprints from an iPhone or iPad



If there are multiple Touch ID fingerprints on your iPhone or iPad, you can delete them to help safeguard access to your device.

1. Go to Settings  > Touch ID & Passcode.
2. If more than one fingerprint is available and they are unnamed, you can place a finger on the Home button to identify your finger's print. Consider naming your fingerprint to help you identify it later.
3. If necessary, tap the fingerprint, then tap Delete Fingerprint.

*Note:* If you can't add a fingerprint or unlock your iPhone or iPad using Touch ID, see the Apple Support article [If Touch ID isn't working on your iPhone or iPad](#).

## Delete unknown Touch ID fingerprints from a Mac or Magic Keyboard

If there are multiple Touch ID fingerprints on your Mac or Magic Keyboard, you can delete them to help safeguard access to your device.

1. Choose Apple menu  > System Settings, then click Touch ID & Password  in the sidebar.
2. Do any of the following:
  - *Delete a fingerprint:* Click a fingerprint, enter your password, click OK, then click Delete.
  - *Add a fingerprint:* Click Add Fingerprint to add new fingerprint, then choose which options you want to use with Touch ID.




## Secure your iPhone or iPad with Face ID

Face ID is for anyone to use who wants to add an extra layer of security to their iPhone or iPad. It helps ensure that no one else can access the information stored on your device. To use Face ID, you must first set up a passcode on your iPhone or iPad.

To see a list of supported devices, see the Apple Support article "[iPhone and iPad models that support Face ID](https://support.apple.com/102854)" (<https://support.apple.com/102854>).



## Secure your iPhone or iPad with Face ID

- If you didn't set up Face ID when you first set up your iPhone or iPad, go to Settings  > Face ID & Passcode > Set up Face ID, then follow the onscreen instructions.

If you have physical limitations, you can tap Accessibility Options when you're setting up Face ID. When you do this, setting up facial recognition doesn't require the full range of head motion. Using Face ID is still secure, but it requires more consistency in how you look at iPhone or iPad.


Face ID also has an accessibility feature you can use if you're blind or have low vision. If you don't want Face ID to require that you look at your iPhone or iPad with your eyes open, go to Settings > Accessibility, then turn off Require Attention for Face ID. This feature is automatically turned off if you turn on VoiceOver when you first set up your iPhone or iPad.



See "[Change Face ID and attention settings on iPhone](https://support.apple.com/guide/iphone/iph646624222)" (<https://support.apple.com/guide/iphone/iph646624222>) in the iPhone User Guide or "[Change Face ID and attention settings on iPad](https://support.apple.com/guide/ipad/ipad058b4a31)" in the iPad User Guide (<https://support.apple.com/guide/ipad/ipad058b4a31>).

## Reset Face ID to delete alternate appearances

If there's an alternate Face ID appearance that you don't want to keep or if you think someone may have added an alternate appearance on your device without your permission, you can reset Face ID and then set it up again.

1. Go to Settings  > Face ID & Passcode, then tap Reset Face ID.
2. See the above task to set up Face ID again.

## Reject unknown sign-in attempts

When two-factor authentication is turned on and a sign-in attempt occurs on a new device, you get a notification on your other trusted devices. The notification includes a map that shows the new device's location. This notification can appear on any trusted iPhone, iPad, or Mac.

The location of the sign-in attempt is approximate, based on the IP address or network that the device is currently using, rather than on the exact location of the device.



If you see a notification that your Apple Account is being used to sign in on a new device you don't recognize, select **Don't Allow** to block the sign-in attempt.

**⚠️ IMPORTANT:** You may want to capture a screenshot of the notification before dismissing it. See [“Record suspicious activity”](#) later in this guide.

If you think your Apple Account might be compromised, see [“Keep your Apple Account secure”](#) (later in this guide) and remove unknown devices.

## Update your Apple software

To secure your device and manage access to your personal information, always make sure you have the latest operating system installed with the latest security and privacy updates. After your devices are up to date, you can learn how to manage your Apple Account. All Apple devices benefit from software updates.




Updating your operating system software is one of the most important things you can do to protect your device and your information. Apple makes it easy to download and install these updates.

To see a list of security updates for Apple devices, see the Apple Support article “[Apple security updates](https://support.apple.com/100100)” (<https://support.apple.com/100100>).

### Update iPhone and iPad automatically

If you didn’t turn on automatic updates when you first set up your device, you can do so now.

1. Go to Settings  > General > Software Update > Automatic Updates.
2. Turn on all three options: Automatically Install [iOS or iPadOS] Updates, Security Responses & System Files, and Automatically Download [iOS or iPadOS] Updates.

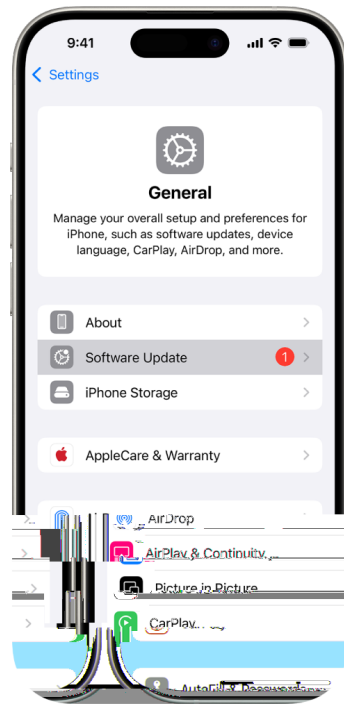
When an update is available, the device downloads and installs the update overnight while it’s charging and connected to Wi-Fi. You’re notified before an update is installed.

To turn off automatic updates, go to Settings > General > Software Update > Automatic Updates, then turn off Automatically Install [iOS or iPadOS] Updates and Security Responses & System Files.

## Update iPhone or iPad manually

At any time, you can check for and install software updates manually.

- Go to Settings  > General > Software Update.





The screen shows the currently installed version of iOS and alerts you if an update is available.

## Update iPhone or iPad using your computer

1. Make sure you have one of the following:
  - A Mac with a USB port and OS X 10.9 or later
  - A Windows device with a USB port and Windows 7 or later
2. Do one of the following:
  - Connect your device to your computer using the included Lightning to USB Cable. If your computer has a USB-C port, use a USB-C to USB Adapter or a USB-C to Lightning Cable (each sold separately).
  - If your device came with a USB-C to Lightning Cable and your computer has a USB port, use a Lightning to USB Cable (sold separately).
  - If your iPad came with a USB-C Charge Cable and your computer has a USB port, use a USB-C to USB Adapter and a USB-A cable (each sold separately).
  - If your iPad came with a Thunderbolt 4/USB-4 charging cable and your computer has a USB port, use a USB-C to USB Adapter and a USB-A cable (each sold separately). You can use Thunderbolt or USB cables with Thunderbolt devices like iPad Pro 12.9-inch (5th generation) and iPad Pro 11-inch (3rd generation).
3. After you've successfully connected your device to your computer, do one of the following:
  - *In the Finder sidebar on your Mac:* Select your device, then click General at the top of the window.

To use the Finder to update your device to iOS 15 or iPadOS 15, you must have macOS 10.15 or later. With earlier versions of macOS, [use iTunes](#) to update your device. See "Update software on iOS devices in iTunes" (at <https://support.apple.com/guide/itunes/itns3235/12.9/mac/10.14>).
  - *In the iTunes app on your Windows device:* Click the iPhone button near the top left of the iTunes window, then click Summary.
4. Click Check for Update.
5. To install an available update, click Update.

## Update your Mac automatically




1. Choose Apple menu  > System Settings, click General  in the sidebar, then click Software Update.
2. To automatically install macOS updates, select "Automatically keep my Mac up to date."
3. To set advanced update options, click Advanced, then do any of the following:
  - *To have your Mac check for updates automatically:* Select "Check for updates."
  - *To have your Mac download updates without asking:* Select "Download new updates when available."
  - *To have your Mac install macOS updates automatically:* Select "Install macOS updates."
  - *To have your Mac install app updates from the App Store automatically:* Select "Install app updates from the App Store."
  - *To have your Mac install system files and security updates automatically:* Select "Install Security Responses and system files."
4. Click OK.

To receive the latest updates automatically, it's recommended that you select "Check for updates," "Download new updates when available," and "Install system data files and security updates."

*Note:* MacBook, MacBook Pro, and MacBook Air must have the power adapter plugged in to automatically download updates.

## Update your Mac manually

You can manually update your Mac's operating system and any software you've gotten from the App Store.

- Choose Apple menu  > System Settings, click General , then click Software Update.
- To update software downloaded from the App Store, click the Apple menu. The number of available updates, if any, is shown next to App Store. Choose App Store to continue in the App Store app .

## Review and delete configuration profiles

Device configuration profiles, mobile device management (MDM) tools, and custom apps may be used by organizations (like schools and businesses) to manage or supervise devices, and these tools may allow access to data or location information on the device.

A configuration profile can manage a variety of settings for user accounts, along with other device functionality. Configuration profiles can work on iPhone, iPad, Mac, Apple TV, and Apple Watch.

If you see a configuration profile installed on your device that isn't supposed to be there, you may be able to delete it, depending on who installed it. Doing so deletes all of the settings, apps, and data associated with the configuration profile.

▼ **IMPORTANT:** Before making changes or deleting information, [consider potential impacts to your safety](#) and privacy.



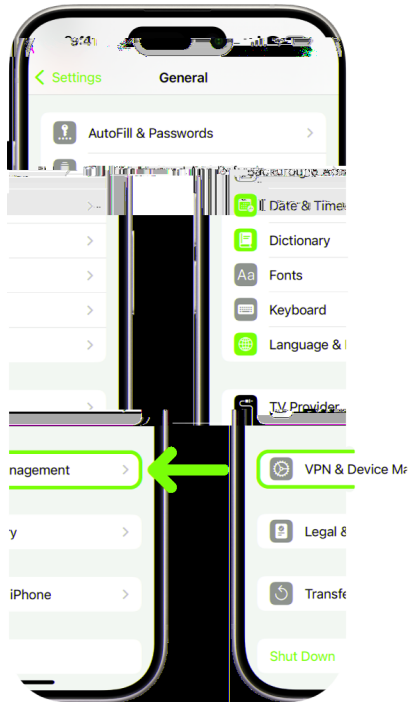
### Review configuration profiles


**Important:** If your device belongs to a school or business, check with your system administrator before deleting any apps or profiles.



## Delete unknown configuration profiles from your iPhone or iPad

When you remove a profile, all of its settings and information are deleted. For example, if the profile provided permissions for a virtual private network (VPN) to give access to a school network, the VPN can no longer connect to that network.







1. Go to Settings  > General > VPN & Device Management.

If you don't see any profiles, then no device management profiles are installed on your device.

2. Select the profile, tap Delete Profile, and follow the onscreen instructions.
3. Restart your device.

## Delete unknown configuration profiles from your Mac

When you remove a profile, all of its settings and information are deleted. For example, if the profile sets up your email account, removing the profile deletes the email account information from your Mac.

1. Do one of the following:
  - On your Mac with macOS 13 or later: Choose Apple menu  > System Settings, click General  in the sidebar, then click Device Management.
  - On your Mac with macOS 12 or earlier: Choose Apple menu  > System Preferences, then click Profiles .

If you don't see the Profiles preference pane, then no device management profiles are installed on your device.


2. Select a profile in the Profiles list, then click —.
3. Restart your Mac.

## Manage iPhone Mirroring on your iPhone or Mac

iPhone Mirroring allows access to and control of iPhone directly from Mac, and also sends iPhone notifications directly to the Mac.

iPhone Mirroring only works when your iPhone is nearby and locked. Once you begin to use your iPhone directly, iPhone Mirroring automatically stops.

You can revoke access to iPhone Mirroring from either device, including when you get a notification that iPhone Mirroring is live. Revoking access resets iPhone Mirroring, so you need to go through the setup process again if you want to use it.

 **IMPORTANT:** Before making changes or deleting information, [consider potential impacts to your safety](#).

### View and revoke access to iPhone Mirroring when you get a notification


If iPhone Mirroring is live, or was recently live, you receive a notification on your iPhone. You can tap the notification to review the session history and revoke access to a specific Mac.


1. On your iPhone, tap the notification.

A list of Mac computers that are set up for iPhone Mirroring appears. Information about recent sessions, including when the session started and how long it lasted, is also visible.

2. Tap Edit in the top right, then select the Mac you want to remove.

### View and revoke access to iPhone Mirroring on iPhone

 **Tip:** You can also use Safety Check to view information and remove Mac computers. See [Safety Check for an iPhone with iOS 16 or later](#).

1. On your iPhone, go to Settings  > General.
2. Tap AirPlay & Continuity, then tap iPhone Mirroring.

A list of Mac computers that are set up for iPhone Mirroring appears. Information about recent sessions, including when the session started and how long it lasted, is also visible.

3. Tap Edit in the top right, then select a Mac to remove.

### **Revoke access to iPhone Mirroring on your Mac**

1. On your Mac, go to the iPhone Mirroring app.
2. Choose iPhone Mirroring > Settings from the menu bar at the top of your screen.
3. Choose Revoke Access to [*name of your iPhone*].


### **Require Touch ID or a passcode for iPhone Mirroring**

Certain settings for iPhone Mirroring allow your devices to connect automatically. You can choose to require authentication instead, such as Touch ID or your device passcode.

1. On your Mac, go to the iPhone Mirroring app.
2. Choose iPhone Mirroring > Settings from the menu bar at the top of your screen.
3. Choose Ask Every Time.

### **Stop an app from sending notifications**

When iPhone Mirroring is live, iPhone notifications are sent directly to the Mac. You can turn this option off for specific apps.

1. On your iPhone, go to Settings  > Notifications.
2. Choose any app, then turn off Show on Mac.

## Harden your devices with Lockdown Mode

Lockdown Mode is an extreme, optional protection for iPhone, iPad, and Mac with iOS 16, iPadOS 16.1, macOS 13, or later that should be used only if you believe you may be targeted by a highly sophisticated cyberattack, such as by a private company developing state-sponsored mercenary spyware.

*Note:* Most people are never targeted by this type of attack.






When a device is in Lockdown Mode, it doesn't function as it typically does. Apps, websites, and features are strictly limited for security, and some experiences aren't available. Lockdown Mode includes the following protections:

- *Messages:* Most message attachment types other than images are blocked. Some features, like link previews, are disabled.
- *Web browsing:* Certain complex web technologies, like just-in-time (JIT) JavaScript compilation, are disabled unless the user excludes a trusted site from Lockdown Mode.
- *Apple services:* Incoming invitations and service requests, including FaceTime calls, are blocked if the user has not previously sent the initiator a call or request.
- *Tethered connections:* Connections with a computer or accessory are blocked when the device is locked.
- *Configuration profiles:* Configuration profiles can't be installed, and the device is unable to enroll into mobile device management (MDM) while Lockdown Mode is turned on. However, any MDM profiles that were enabled prior to Lockdown Mode remain on the device.

## Turn Lockdown Mode on or off

Lockdown Mode must be turned on separately for iPhone, iPad, and Mac. When you turn on Lockdown Mode on iPhone, it automatically turns on Lockdown Mode for any paired Apple Watch with watchOS 10 or later. You can't turn Lockdown Mode on or off directly on an Apple Watch.


- Do one of the following:
  - *On your iPhone or iPad:* Go to Settings  > Privacy & Security > Lockdown Mode, tap Turn On Lockdown Mode, tap Turn On & Restart, then enter your device passcode.
  - *On your Mac:* Choose Apple menu  > System Settings, click Privacy & Security  in the sidebar, then click Lockdown Mode. Click Turn On, then enter your password if prompted and click Turn On & Restart.

## Securely control your Home accessories

If you're currently a member of a Home, you can easily and securely view and control your Home accessories by using the Home app on your iPhone, iPad, or Mac, or by using HomePod.


*Note:* Home accessories may be Apple products or third-party products. To view a list of available Home accessories compatible with the Home app and your Apple devices, see "[Home accessories](https://www.apple.com/home-app/accessories/)" (<https://www.apple.com/home-app/accessories/>).

### Stop sharing your home with someone

1. Select the Home app , then select Home Settings. If you see multiple homes, choose the home you want to leave, then select Home Settings.
2. Under People, select the user you want to remove from your home, then select Remove Person.

### Leave a home you were invited to share


If you leave a home, you can no longer view the accessories in that home.

1. In the Home app , select the Home icon, then select Home Settings. If you see multiple homes, choose the one you want to leave, then select Home Settings.
2. Scroll down, and select Leave Home. Select Leave.

### Reset a home

In iOS 16, iPadOS 16.1, and macOS 13, or later, when you remove a home from the Home app, all HomeKit devices must be added back to a new home. Before you remove a home, make sure you've updated the software on all home accessories to their latest versions.

If you haven't upgraded your operating systems, make sure you complete step 4 below.

1. In the Home app , select the Home icon, then select Home Settings.
2. At the bottom of the dialog, select Remove Home, then select Remove.
3. Close the Home app.
4. Find all home accessories, then reset each one to its factory settings.
5. Open the Home app again and create a new home.
6. Add each accessory to the new home.

# Passwords, passkeys, passcodes


## Secure your device, app, and website passwords

On your iPhone or iPad with iOS 17, iPadOS 17, or earlier, you can manage your passwords in Settings, in Spotlight Search, or using Siri. You can also use the Password Security Recommendations feature to identify any weak or vulnerable passwords. Saved passwords appear in alphabetical order organized by the website or platform they're saved on.

On your iPhone or iPad with iOS 18, iPadOS 18, or later, you can manage your passwords in the Passwords app, where you can find all your passwords, passkeys, and verification codes in one place. You can use them on all your devices when you sign in to iCloud with the same Apple Account and turn on Passwords & Keychain in iCloud settings. And if you use AutoFill to sign in to apps and websites, your passwords automatically appear in Passwords.




### Manage passwords with iOS 18, iPadOS 18, or later

1. Go to the Passwords app  on your iPhone.
2. Tap All, then tap the account for the password you want to manage.
3. Tap Edit.
4. Change or delete the password, then tap to confirm.

### Manage passwords with iOS 17, iPadOS 17, or earlier

You can manage your passwords in Settings, in Spotlight Search, or using Siri.


1. Go to Settings  > Passwords, then do any of the following:
  - To add a new password manually, tap Add in the top-right corner.
  - To edit or delete a password, tap Edit in the top-right corner, tap "Select saved passwords," then tap Edit or Delete.

**Important:** After you've deleted a password, you can no longer recover it.

2. If you added a new password, test it to make sure you entered it correctly.

### Use Password Security Recommendations with iOS 17, iPadOS 17, or earlier







If you create and store your own passwords for websites and apps, you can use the Password Security Recommendations feature to identify any weak or vulnerable passwords (for example, if they're easily guessed or used multiple times). You can also use the feature to securely monitor your passwords and to alert you if any have been compromised through a known data leak.

1. Go to Settings  > Passwords > Security Recommendations.
2. Turn on the Detect Compromised Passwords to let iPhone securely monitor your passwords and to alert you if any passwords have appeared in known data leaks.
3. Review these recommendations for the passwords you've created:
  - Passwords marked as *reused* have been used across different domains. Using the same password for more than one service may leave the account vulnerable to an attacker who has discovered your credentials.
  - Passwords marked as *weak* may be easily guessed by an attacker.
  - Passwords are marked as *leaked* if the Password Monitoring feature has identified them in a known data leak.
4. To make an update to a reused, weak, or leaked password, tap the item and follow the onscreen instructions.



## Automatically delete one-time verification codes

In iOS 17, iPadOS 17, macOS 14, or later, one-time verification codes are filled in automatically, so you don't need to leave the app or website you're signing in to. You can choose to automatically delete the verification codes after entering them with Autofill, or keep them.

- Do one of the following:
  - On your iPhone or iPad with iOS 18 or iPadOS 18, or later: Go to Settings  > General > Autofill & Passwords. Under Verification Codes, tap Delete After Use, then turn it on.
  - On your iPhone or iPad with iOS 17 or iPadOS 17, or earlier: Go to Settings  > Password, tap Password Options, then turn on Clean Up Automatically.
  - On your Mac with macOS 15: Choose Apple menu  > System Settings, click General  in the sidebar, then click Autofill & Passwords. Under Verification Codes, turn on Delete After Use.
  - On your Mac with macOS 14 or macOS 13: Choose Apple menu  > System Settings, click Passwords  in the sidebar, click Password Options, then turn on Clean Up Automatically.

## Set a unique device passcode or password


To prevent anyone except you from using your devices and accessing your information, set a unique passcode or password that only you know. If you share a device, or if others know your passcode or password, they'll be able to view and make changes to the information on your device and associated Apple Account. If you believe someone else knows your device passcode or password and you want to set one that only you know, you can reset them in Settings or System Preferences, depending on the device (see instructions below).



## Set a passcode on your iPhone or iPad

For better security, set a passcode that needs to be entered to unlock iPhone or iPad when you turn it on or wake it. Setting a passcode also turns on data protection, which encrypts your iPhone or iPad data so that only someone who knows the passcode can access it.


*Note:* Your device *passcode* isn't your Apple Account *password*, which provides access to the iTunes Store, App Store, Apple Books, iCloud, and other Apple services.

- Go to Settings , then do one of the following:
  - On your iPhone or iPad with Face ID: Tap Face ID & Passcode, then tap Turn Passcode On or Change Passcode.
  - *On your iPhone or iPad with a Home button:* Tap Touch ID & Passcode, then tap Turn Passcode On or Change Passcode.

To view options for creating a password, tap Passcode Options. Passcodes default to six digits, but options range from the least secure, four-digit, to most secure (alphanumeric).


## Change the passcode and expire the previous passcode on iPhone or iPad

If you're concerned someone has access to your passcode and you want to secure your iPhone, you can change the passcode to protect your privacy and expire the previous passcode. To change your passcode, follow the steps below.

1. Go to Settings , then do one of the following:
  - On your iPhone or iPad with Face ID: Tap Face ID & Passcode, then enter your passcode.
  - *On your iPhone or iPad with a Home button:* Tap Touch ID & Passcode, then enter your passcode.
2. Tap Change Passcode, enter your current passcode.
3. If you want extra security, tap Passcode Options to select the format for your future passcode.

Available formats include a four-digit numeric code, six-digit numeric code, custom alphanumeric code, or custom numeric code.






4. Enter your new passcode twice.

 **IMPORTANT:** After changing your passcode in iOS 17 or iPadOS 17, you can use your old passcode to reset your passcode for 72 hours. This is to protect against accidentally forgetting the new passcode. If you want to completely deactivate your old passcode after changing it, tap Expire Previous Passcode Now on the Face ID & Passcode (or Touch ID & Passcode) page in Settings.

## Change the login password on your Mac

If you're concerned someone has access to your password and you want to secure your Mac, you can change the user password to protect your privacy.


*Note:* Your login password is the password you enter to unlock your Mac when you turn it on or wake it from sleep. Because you created it, it may be the same as your Apple Account password, which provides access to the iTunes Store, App Store, Apple Books, iCloud, and other Apple services.

1. Do one of the following:
  - On your Mac with macOS 13 or later: Choose Apple menu  > System Settings, click Users & Groups  in the sidebar, then click .
  - On your Mac with macOS 12 or earlier: Choose Apple menu  > System Preferences, then click Users & Groups  in the sidebar.

2. Click Change Password.

3. Enter your current password in the Old Password field.

4. Enter your new password in the New Password field, then enter it again in the Verify field.

For help choosing a secure password, click  next to the New Password field.



5. Enter a hint to help you remember the password.

The hint appears if you enter the wrong password three consecutive times or if you click the question mark in the password field in the login window.

6. Click Change Password.

## Automatically lock your devices

To further increase personal privacy, you can set your device up to automatically lock under certain conditions.

- *iPhone, iPad:* Go to Setting > Display & Brightness > Auto-Lock, then set a length of time.
- *Mac:* Choose Apple menu  > System Settings, click Lock Screen  in the sidebar, then set a length of time.

For more information, see "[Change Lock Screen settings on Mac](https://support.apple.com/guide/mac-help/mh11784)" in the Mac User Guide. (<https://support.apple.com/guide/mac-help/mh11784>)

- *Apple Watch:* Open the Settings app, tap Passcode, then turn Wrist Detection on or off.

For more information, see "[Lock automatically](https://support.apple.com/guide/watch/apd0e1e73b6f#apd6771615db)" in the Apple Watch User Guide. <https://support.apple.com/guide/watch/apd0e1e73b6f#apd6771615db>)

## Manage shared password and passkeys






In iOS 17, iPadOS 17, macOS 14, or later, you can create or join a group of trusted contacts to share passwords and passkeys across devices. There are two distinct user roles in Shared Password groups: Group Owner and Group Member. Each user role determines the kind of tasks you can perform.

- *Group Owner:* The Group Owner is the group member who created the group. The owner is the only person who can add or remove other members.
- *Group Member:* Each person who has received and accepted an invitation from the owner is a group member. All group members can add, view, edit, or delete passwords at any time. Group members can leave a group at anytime they choose.








*Note:* If you delete a password or passkey that you shared with a group, you have 30 days to recover it. If you delete a password or passkey that someone else shared with the group, they receive a notification to recover it within 30 days. See "[Recover a recently deleted password or passkey on Mac](https://support.apple.com/guide/passwords/mchlee73013a/mac)" (<https://support.apple.com/guide/passwords/mchlee73013a/mac>) in the Passwords User Guide for Mac.

### Determine your role in a shared password group

- Do one of the following:
  - *On your iPhone or iPad with iOS 18, iPadOS 18, or later:* Open the Passwords app, tap the name of the group, then see if you're the group owner or member
  - *On your iPhone or iPad with iOS 17, iPadOS 17, or earlier:* Go to Settings  > Password, look for a shared password group , select the group, then see if you're the group owner or a member.
  - *On your Mac with macOS 15 or later:* Go the Passwords app, click the shared group in the sidebar, click Manage, then see if you're the group *owner* or a *member*.
  - *On your Mac with macOS 14 or earlier:* Choose Apple menu  > System Settings, then click Passwords  in the sidebar. Look for a shared password group , select the group, click Manage, then see if you're the group *owner* or a *member*.






## Remove someone from a shared password group that you own

If you remove someone else from a shared password group, that person may still have access to the accounts and passwords you shared while they were in the group. After removing someone, you should also change passwords for the accounts you own that you no longer want them to have access to.

- Do one of the following:
  - *On your iPhone or iPad with iOS 18, iPadOS 18, or later:* Open the Passwords app, tap the name of the group, then remove a member
  - *On your iPhone or iPad with iOS 17, iPadOS 17, or earlier:* Go to Settings  > Password, look for a shared password group , select the group, then remove a member.
  - *On your Mac with macOS 15 or later:* Go the Passwords app, click the shared group in the sidebar, click Manage, then remove a member.
  - *On your Mac with macOS 14 or earlier:* Choose Apple menu  > System Settings, then click Passwords  in the sidebar. Look for a shared password group , select the group, click Manage, then remove a member.

## Leave a shared password group you're a member of






If you remove yourself from a shared password group, previous group members may still have access to the accounts and passwords or passkeys you shared while you were in the group. After leaving the group, you should also change passwords or passkeys for the accounts you own that you no longer want group members to have access to.

- Do one of the following:
  - *On your iPhone or iPad with iOS 18, iPadOS 18, or later:* Open the Passwords app, tap the name of the group, then remove yourself.
  - *On your iPhone or iPad with iOS 17, iPadOS 17, or earlier:* Go to Settings  > Password, look for a shared password group , select the group, then remove yourself from it.
  - *On your Mac with macOS 15 or later:* Go the Passwords app, click the shared group in the sidebar, click Manage, then remove yourself from it.
  - *On your Mac with macOS 14 or earlier:* Choose Apple menu  > System Settings, then click Passwords  in the sidebar. Look for a shared password group , select the group, click Manage, then remove yourself from it.

## Delete a password or passkey from a shared password group

If you decide to delete passwords or passkeys from a shared password group, group members may still have access to the accounts and passwords or passkeys you shared with the group. After deleting them, you should also change passwords or passkeys for the accounts you own that you no longer want group members to have access to.

*Note:* If you delete a password or passkey that you shared with a group, you have 30 days to recover it. If you delete a password or passkey that someone else shared with the group, they receive a notification to recover it within 30 days. See "[Recover a recently deleted password or passkey on Mac](https://support.apple.com/guide/passwords/mchlee73013a/mac)" in the Passwords User Guide for Mac (<https://support.apple.com/guide/passwords/mchlee73013a/mac>).

- Do one of the following:
  - *On your iPhone or iPad with iOS 18, iPadOS 18, or later:* Open the Passwords app, tap the name of the group, then tap the account with the password or passkey you want to delete. Tap Edit, tap Delete, then tap Delete Password or Delete Passkey again to confirm.
  - *On your iPhone or iPad with iOS 17, iPadOS 17, or earlier:* Go to Settings  > Password, look for a shared password group , select the group, then tap Delete Password or Delete Passkey.
  - *On your Mac with macOS 15 or later:* Go the Passwords app, click the shared group in the sidebar, then click the account with the password or passkey you want to delete. Click Edit, click Delete Password or Delete Passkey, then click Delete Password or Delete Passkey (again).
  - *On your Mac with macOS 14 or earlier:* Choose Apple menu  > System Settings, click Passwords  in the sidebar, then click  next to the account with the password or passkey you want to delete. Click Delete Password or Delete Passkey, then click Delete Password or Delete Passkey (again).

# Manage location information

## Use Check In for Messages

You can use Check In on iPhone to automatically notify a friend that your iPhone has arrived, and choose what details they can see if you don't successfully complete your Check In.

Similarly, if a friend sends you a Check In but their iPhone hasn't arrived as expected, you can view their location, battery percentage, cellular signal, and more.

*Note:* Check In requires iOS 17 or later for both the sender and the recipient. Location sharing isn't supported in South Korea and might be unavailable in other regions due to local laws.

When you start a *travel-based* Check In, your contact is informed about:

- Your destination and approximate arrival time
- What they can expect if you don't respond to prompts, if you place an Emergency SOS call during Check In, or if your phone doesn't arrive at the destination as expected

When you start a *timer-based* Check In, your contact is informed about:

- What time you started the timer
- What time the timer ends
- What they can expect if you don't respond to prompts about the timer or if you place an Emergency SOS call during Check In

## What information is shared, and when?

While setting up Check In, you can choose the amount of information you want to share with your contact when the Check In doesn't end as expected. After setting up Check In, you can change the type of data you're sending in Settings > Messages > Check In > Data.

Your information level choices are:

- *Limited data*: Includes your current location and details about your battery and network signal for iPhone and Apple Watch.
- *Full data*: Includes all data from Limited plus your route traveled and the location of your last iPhone unlock and Apple Watch removal.

Your contact is automatically sent a link to view the information you chose to share with them in the following circumstances:

- Your phone doesn't arrive at your destination.
- You're significantly delayed during travel and don't respond to the prompt to add time.
- You place an Emergency SOS call and don't respond to the follow up Check In prompt.
- You don't respond to the prompt at the end of your timer-based Check In.

**Important:** If your phone is lost while Check In is running, your contact receives notifications as if you weren't responding.



## While Check In is running

When a travel-based Check In is running, the following message appears on your Lock Screen: "Check In Unlock to view details." If you tap this message and unlock the device, you see the destination you set, your current ETA which is updated automatically based on traffic and driving conditions, and the type of data shared with your contact if the Check In is not successfully completed (Limited or Full). You also have the ability to cancel the Check In.



### Start timer-based Check In

If you aren't feeling safe in your current location and want a trusted contact to support you using Check In, you can start a timer-based Check In. The timer-based Check In notifies your trusted contact if you don't respond to the prompt at the end of the timer.

When the timer-based Check In is running, the following message appears on your Lock Screen: "Check In: Unlock to view details." If you tap this message and unlock the device, you can see the following:

- The time remaining on your Check In
- The contact you've chosen to receive your Check-In
- The type of data shared with your contact:
  - Limited or Full

To start a timer-based Check In:



1. Open Messages , then select the person who you want notify.
2. Tap New Message at the top of the screen and add a recipient, or select an existing conversation.
3. Tap , tap Check In, then tap Edit.  
You may need to tap More to find Check In.
4. Select "After a timer."
5. Select the amount of time you want to put on the timer.

When the timer-based Check In ends, you receive a prompt to tap End the Check In or Add More Time. When ending the Check In, your contact is notified it has successfully ended. You can also choose to Add Time, which allows you to add 15, 30, or 60 more minutes to your Check In. Your contact receives the updated end time.

## Start travel-based Check In

If you're traveling by car, transit, or walking, you can start a Check In to automatically notify a friend after you've arrived at your intended destination.

When a travel-based Check In is running, the following message appears on your Lock Screen: "Check In Unlock to view details." If you tap this message and unlock the device, you see the destination you set, your current ETA (which is updated automatically based on traffic and driving conditions), and the type of data shared with your contact if the Check In isn't successfully completed. You also have the ability to cancel the Check In.

1. Open Messages , then select the person who you want notify.
2. Tap New Message at the top of the screen and add a recipient, or select an existing conversation.
3. Tap , tap Check In, then tap Edit.  
You may need to tap More to find Check In.
4. Select "When I arrive."
5. Tap Change and then enter your intended location in the search field.
6. To set your location arrival radius, tap Small, Medium, or Large at the bottom of the screen. Your friend receives an Arrival notification once you've entered that radius.
7. Tap Done.
8. Tap Driving, Transit, or Walking, then tap Add Time if needed.

If your device isn't progressing toward your intended destination, you'll receive a prompt and have 15 minutes to respond. If there's no response, your loved one is automatically notified.

When your iPhone arrives at the destination set for a travel-based Check In, Check In ends and your contact receives an alert indicating that you arrived.

## Detecting unwanted trackers

Apple designed AirTags and the Find My network to help users keep track of belongings and—at the same time—discourage unwanted tracking. To further help safeguard that no device is unknowingly tracking users, Apple and Google created an industry standard. With it, users (iPhone, iPad, and Android) can be notified if they are being tracked.



If you feel your safety is at risk, contact your local law enforcement. If the item is an Apple product, law enforcement [can work with Apple to request information related to the item](https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf) (<https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>). You may need to provide the AirTag, AirPods, or Find My network accessory, and the device's serial number.

### Unwanted tracking notifications

Unwanted tracking notification software availability:

- Unwanted tracking notifications for AirTags and other Find My accessories are available on iPhone or iPad with iOS 14.5, iPadOS 14.5, or later.
- Unwanted tracking notifications for unknown Bluetooth tracking devices that are compatible with the [Detecting Unwanted Location Trackers](#) industry specification are available on an iPhone with iOS 17.5 or later.
- Google provides [unwanted tracking detection](#) on devices with Android 6.0 or later. Those with earlier operating systems can update or use the [Tracker Detect app](#).

## Turn on unwanted tracking notifications

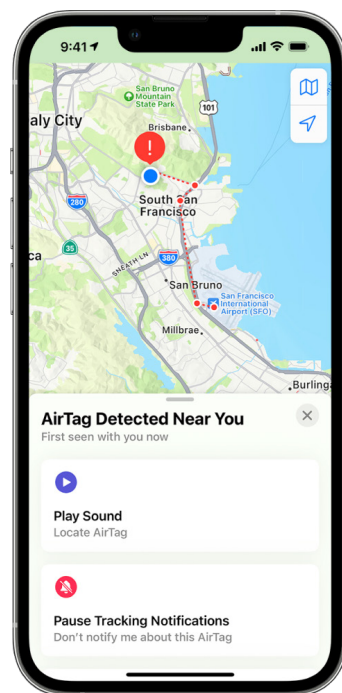
To receive unwanted tracking notifications on an iPhone or iPad with iOS 14.5, iPadOS 14.5, or later, make sure that you:

- Go to Settings > Privacy & Security > Location Services, and turn Location Services on.
- Go to Settings > Privacy & Security > Location Services > System Services, and turn Find My iPhone on.
- Go to Settings > Bluetooth, and turn on Bluetooth.
- Go to Settings > Notifications > scroll down to Tracking Notifications, then turn on Allow Notifications.
- Turn off airplane mode. If your device is in airplane mode, you don't receive tracking notifications.

## If you get an unwanted tracking notification



Follow these steps to find the item:

1. Tap the notification.
2. Tap continue and then tap Play Sound, or, if available, tap Find Nearby to use Precision Finding to help you locate the unknown item.



If the option to play a sound isn't available or if you're unable to locate the item with Precision Finding, the item may not be near you anymore. If you believe the item is still with you, look through your belongings to try to locate it. Check on your person, or in anything in your possession that could contain the device. It could be in an item that you don't check often, like a jacket pocket, the outer compartment of a bag, or your vehicle. If you can't find the device and if you feel your safety is at risk, go to a safe public location and contact law enforcement.

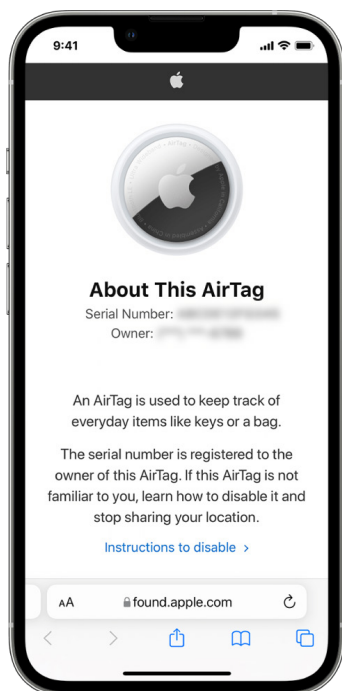
**If you previously received an unwanted tracking notification and want to review the information again, do one of the following:**

- *On your iPhone or iPad:* Open the Find My app , then tap Items, then tap Items Detected With You.
- *On your Mac:* Open the Find My app , click Items, then click Items Detected With You.

**If you find an AirTag, Find My accessory, or compatible Bluetooth tracking device**

Follow these steps to get information about it:

1. Hold the top of your iPhone or near the item until a notification appears.
2. Tap the notification. This opens a website that provides information about the item, including:
  - Serial number or device ID
  - Last four digits of the phone number or an obfuscated email address of the person who registered it. This can help you identify the owner, if you know them.
3. If the owner marked the item as lost, you might see a message with information about how to contact the owner.



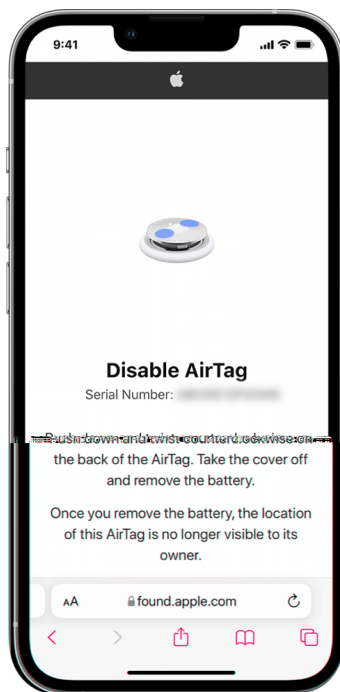
## If you're concerned the item might be being used to track you

⚠️ **IMPORTANT:** Before making changes, [consider potential impacts to your safety](#) and privacy. If you feel your safety is at risk, contact your local law enforcement. If the item is an Apple product, law enforcement [can work with Apple to request information related to the item](#) (<https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>). You may need to provide the AirTag, AirPods, or Find My network accessory, and the device's serial number.

1. [Take a screenshot](#) of the item and owner information for your records.
2. Disable the device and stop it from sharing its location by tapping Instructions to Disable and following the on screen steps.
3. If you feel your safety is at risk, contact your local law enforcement. If the item is an Apple product, law enforcement can [work with Apple to request information related to the item](#). You may need to provide the AirTag, AirPods, or Find My network accessory, and the device's serial number.

See <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>.

After the item is disabled, the owner can no longer get updates on its current location. You will also no longer receive any unwanted tracking notifications for this item.



## Check for AirTags or Find My accessories using an Android device

See the ["Find Unknown Trackers support page"](https://support.google.com/android/answer/13658562?visit_id=638525910154486952-839086324&) for more information on how to check for unwanted tracking on Android devices. ([https://support.google.com/android/answer/13658562?visit\\_id=638525910154486952-839086324&](https://support.google.com/android/answer/13658562?visit_id=638525910154486952-839086324&))

## If you hear an AirTag make a sound

When moved, any AirTag separated for a period of time from its owner makes a sound to notify those nearby. If you find an AirTag after hearing it make a sound, you can use any device that has Near Field Communication (NFC) technology, such as an iPhone or Android phone, to see if its owner marked it as lost and help return it.

**⚠️IMPORTANT:** If you feel your safety is at risk, you can contact your local law enforcement, [who can work with Apple](https://www.apple.com/legal/transparency/government-information.html) (<https://www.apple.com/legal/transparency/government-information.html>). You may need to provide the AirTag or its serial number.

## Devices connected to another Apple Account

If you try to set up AirPods, an AirTag, or another Find My network accessory and see a message that it's paired to another Apple Account, the device or item needs to be removed from that Apple Account first. To learn more about removing or unpairing your item or device, or to set it up with a different Apple Account, see the Apple Support article ["If an item or device is connected to another Apple Account"](https://support.apple.com/102620) (<https://support.apple.com/102620>).

## AirTag sharing

Item Sharing allows AirTag owners to share the item with up to five people at a time. Borrowers can:

- See the location of the AirTag in Find My
- Use Precision Finding to locate the AirTag
- Play a sound if the AirTag is lost
- Be notified when someone new has joined the sharing group
- See each member of the sharing group's Apple Account or Contact Information if the other member is saved to their Contacts

*Note:* Borrowers can't see which borrower has the AirTag.


Because everyone in the sharing group can see the location of the AirTag, unwanted tracking notifications for that AirTag are suppressed for all sharing group members. When someone leaves the sharing group or when the item owner removes them from the group, they're unable to view the location of the AirTag, and unwanted tracking notifications resume.

To learn more, see [Share an AirTag or other item in Find My on iPhone](https://support.apple.com/guide/iphone/iph419cc5f28) in the iPhone User Guide. (<https://support.apple.com/guide/iphone/iph419cc5f28>)

## Remove yourself from a Sharing Group


If you want to remove yourself from a sharing group, you can use Find My or Safety Check.

**⚠ Caution:** After you remove yourself, you can't see the location of the AirTag, and unwanted tracking notifications resume. You may want to see if the AirTag is near you before removing yourself from the share.

1. Go to Settings  > Privacy & Security > Safety Check.
2. Tap Manage Sharing & Access.
3. Tap Items > Stop Sharing.


## Using Find My

To remove yourself using Find My:

1. Open the Find My app .
2. Tap Items, then tap the item you'd like to remove yourself from.
3. Tap Remove.


## Using Safety Check

To remove yourself using Safety Check:

1. Go to Settings  > Privacy & Security > Safety Check.
2. Tap Manage Sharing & Access.
3. Tap Items > Stop Sharing.


## Remove others from a sharing group using Find My

As an owner, you can remove other people from a sharing group using Find My.

1. Open the Find My app .
2. Tap Items, then tap the item name.
3. Tap the name of the person you want to stop sharing with.
4. Tap Remove > Stop Sharing.

## Remove others from a sharing group using Safety Check

As an owner, you can remove other people from a sharing group using Safety Check.

1. Go to Settings  > Privacy & Security > Safety Check.
2. Tap Manage Sharing & Access > Continue.
3. Tap the name of the person you want to stop sharing with, then tap Review Sharing.
4. Tap Items, then tap Stop Sharing.



## Find My and location sharing

The Find My app for iPhone, iPad, Mac, and Apple Watch helps you keep track of your devices and lets you and other people share your locations with each other.






If you set up Family Sharing and use Location Sharing, your family members automatically appear in the People tab, although they still have to share their location with you. See [“Manage Family Sharing settings”](#) later in this guide.




## Location sharing details and where they are viewable

When you share your location with other people through Find My, they can view it in the apps listed in the table below.

If you and the person you share your location with both have an iPhone with iOS 15 or later, you also share your Live Location in all the apps listed below. If you're on the move, they can get a sense of the direction you're traveling in and your speed.






App	Description
 <p>The Find My app</p>	<p>In the Find My app, others can go to the People tab and tap your name to see your location.</p>
 <p>The Find My app</p>	<p>If you and another person both share your location with each other, both have an iPhone 15, and are near each other, you can use Precision Finding to find each other's exact location. When you're located near this person, Precision Finding helps them find you until they're within a few feet of your location. If someone's trying to find you with Precision Finding, you receive a notification that they're trying to locate you.</p> <p>To learn more, see <a href="#">Use Precision Finding on iPhone 15 to meet up with a friend</a> in the iPhone User Guide. (<a href="https://support.apple.com/guide/iphone/iph3effd0ed6">https://support.apple.com/guide/iphone/iph3effd0ed6</a>)</p>
 <p>The Find My app</p>	<p>If you set up Family Sharing and use Location Sharing, your family members automatically appear in the People tab but location sharing doesn't start until you share your location with each other. See <a href="#">Manage Family Sharing settings</a> later in this guide.</p>

App	Description
 The Messages app	In Messages, when others you've shared your location with tap on your contact icon, they are taken to a Details view that shows your current location shared through Find My.
 The Messages app	In Messages in iOS 17 and iPadOS 17 or later, others you've shared your location with can also see your approximate location at the top of the Messages thread.
 The Maps app	In Maps, when others you've shared your location with search for your name, they see your current location being shared through Find My on their map.

### Location change notifications

You can use the Find My app to [notify a friend when your location changes](https://support.apple.com/guide/iphone/iph9bfec93b1) (<https://support.apple.com/guide/iphone/iph9bfec93b1>). People you share location with can also set up notifications to see when your location changes.


You can turn off any location change notification about you. This includes notifications you set and notifications your friends create.


1. To see all notifications about you, do one of the following:
  - *On your iPhone or iPad:* Open the Find My app , then tap Me.
  - *On your Mac:* Open the Find My app , click Me, then click .
2. Look for a Notifications About You section.
  - If you *do* see the Notifications About You section, select a name to see more details.
  - If you *don't* see the Notifications About You section, your friends aren't notified when your location changes.
3. If you see a notification you want to delete, select a name, then select a notification.
4. Delete the notification, then confirm that you want to delete it.

## Stop sharing your location in Find My on iPhone or iPad

When you stop sharing through any of the methods listed below, your location will disappear from the other person's Find My, Maps, Contacts, and Messages apps.



**⚠️IMPORTANT:** When you stop sharing your location, the people you previously shared with may notice that you've stopped. On earlier operating systems, they may receive a notification in Messages that you stopped sharing.

1. Open the Find My app .
2. Do one of the following:
  - *To stop sharing with a one person:* Select the People tab, find the person you want to stop sharing with and tap their name, then scroll down and tap Stop Sharing My Location.
  - *To stop sharing with everyone:* Select the Me tab, then turn off Share My Location.

*Note:* If the Find My app has been deleted from your device, you can turn off Location Services (go to Settings  > Privacy & Security > Location Services) to help ensure that your location isn't being shared. Then download the Find My app from the App Store again.


## Stop sharing your location in Messages on iPhone or iPad

When you stop sharing through any of the methods listed below, your location disappears from the other person's Messages app on their devices.

1. Open the Messages app .
2. Do one of the following:
  - *To stop sharing messages in a conversation:* Choose the conversation with the person you want to stop sharing with, tap on the person's name at the top of the conversation, then tap Stop Sharing.
  - *To stop sharing by deleting the conversation:* In the Messages conversation list, swipe left on the conversation, tap , then tap Yes to confirm you want to stop sharing your location with the participants in this conversation.

## Stop sharing your location in Contacts on iPhone or iPad

When you stop sharing through either of the methods listed below, your location disappears from the other person's Contacts apps on their devices.

1. Open the Contacts app .
2. Tap the person's name.
3. Tap Stop Sharing My Location.


## When to disable Find My iPhone for a lost or stolen device

Find My iPhone (in Settings  > Find My) helps you find your phone if it is lost or stolen.

When Find My iPhone is turned on, your device may be found through the Find My network for up to 24 hours after it has been powered off or disconnected from the internet.


The location of your device is visible through Find My in the Devices tab on your other devices, and to anyone in Family Sharing you share your location with.

If you need to get to a safe location and you want to turn off your device, but you're concerned that someone else may use this feature to find your location, you can temporarily turn off the Find My Network when you power off the device by tapping iPhone Findable After Power Off (under Slide to Power Off) and following the onscreen instructions. Use the task below if you want to disable this feature.

 **Caution:** When you turn off Find My [device] and Find My network, you aren't able to locate, lock, or erase your device if it's lost or stolen.

- *On your iPhone or iPad:* Go to Settings  > [your name] > Find My > Find My iPhone > Find My network.


Disabling this feature means you can't use it if your device is lost or stolen and powered down.

- *On your Mac:* Choose Apple menu  > System Settings, click your name at the top of the sidebar, then click iCloud. Click Show More Apps then click Find My Mac.

# Manage Location Services settings

Location Services lets you choose the apps (like Maps, Camera, Weather, and others) and websites you want to share your location with. When turned on, Location Services uses information from various kinds of networks to determine your approximate or precise location. You can find Location Services on iPhone, iPad, Mac, and Apple Watch.










When an app is using Location Services, the Location Services icon  appears on iPhone and iPad (in the status bar at the top of the screen) and on Mac (in the menu bar).

Even if you disable Location Services, third-party apps and websites may still use other ways to determine your location. For safety, your device's location information may be used for emergency calls to aid response efforts regardless of whether you turn on Location Services.

## Turn Location Services on or off

When you set up a device, you're asked if you want to turn on Location Services. After you've completed setup, you can turn Location Services on or off at any time.


- *On your iPhone or iPad:* Go to Settings  > Privacy & Security > Location Services turn location sharing on or off.
- *On your Mac with macOS 13 or later:* Choose Apple menu  > System Settings, click Privacy & Security  in the sidebar, then click Location Services. Turn Location Services on or off, enter your password if asked, then click Unlock.
- *On your Mac with macOS 12 or earlier:* Choose Apple menu  > System Preferences, click Security & Privacy  in the sidebar, click Privacy, then click Location Services. If the lock at the bottom left is locked , click it to unlock the preference pane. Turn Location Services on or off.
- *On your Apple Watch:* Go to Settings  > Privacy & Security > Location Services.

## Specify which apps can use Location Services on iPhone or iPad

Some apps might not work unless you turn on Location Services. The first time an app needs to access your Location Services information, you receive a notification asking for permission. Choose one of these options:

- Allow Once
- Allow While Using App
- Don't Allow

You can also review or change an individual app's access to your location and indicate how often it may use your location. Instructions follow for iPhone or iPad.






1. Go to Settings  > Privacy & Security > Location Services, then review or change access settings for an app.

To see its explanation for requesting Location Services, tap the app.

2. Determine how closely you want apps to know your location.
  - To allow an app to use your specific location, leave Precise Location turned on.
  - To share only your approximate location—which may be sufficient for an app that doesn't need your exact location—you can turn Precise Location off.

*Note:* If you set the access for an app to Ask Next Time, you're asked to turn on Location Services again the next time an app tries to use it.

## Specify which apps can use Location Services on Mac



1. Do one of the following:
  - On your Mac with macOS 13 or later: Choose Apple menu  > System Settings, click Privacy & Security  in the sidebar, then click Location Services. Turn off Location Services, enter your password, then click Unlock.
  - On your Mac with macOS 12 or earlier: Choose Apple menu  > System Preferences, click Security & Privacy  in the sidebar, click Location Services, then deselect Enable Location Services. You may need to first unlock System Preferences to make changes. To do this, click  in the bottom-left corner, then enter your password.

2. Select the checkbox next to an app to allow it to use Location Services. Deselect the checkbox to turn off Location Services for that app.

If you turn Location Services off for an app, you're asked to turn it on again the next time that app tries to use your location data.

3. Scroll to the bottom of the list of apps to reveal System Services, then click the Details button to see specific system services that use your location.

To allow the location of your Mac to be used by Siri Suggestions and Safari Suggestions, select Location-Based Suggestions.



To allow your Mac to identify places significant to you and provide useful related information in Maps, Calendar, Reminders, and more, select Significant Locations. Significant locations are encrypted and can't be read by Apple. Click Details to view a list of locations that have been identified. To remove a location from the list, select it and click . To remove all the locations, click , then click Clear History.

## Manage automatic ETA sharing in Maps

In Maps on iPhone and iPad (Wi-Fi + Cellular models), you're able to automatically share your estimated time of arrival (ETA) to a Favorite location with anyone in your Contacts. After you set this up, each time you navigate to the Favorite location, your ETA is shared with the contacts. After you're on your route, the bottom of the screen indicates you're sharing ETA with other people.




### Manage ETA sharing on your iPhone or iPad


1. In the Maps app  on your iPhone or iPad (Wi-Fi + Cellular models), tap your profile icon to the right of the search field.
2. Select Favorites to open a window containing all of the locations you've designated as a Favorite.
3. Tap  next to the Favorite point of interest.
4. Scroll down to the Share ETA section to review the names of people you're automatically sharing your ETA with.
5. To remove someone, tap Stop Sharing ETA beside the name of the person you want to remove.
6. To add someone, tap Add Person, then in the Contacts app, select the person you want to automatically share your ETA with for this point of interest.
7. Repeat steps 3–6 for all additional points of interest in your Favorites.



### Stop automatic ETA sharing after navigating has started

You can stop automatic ETA sharing even after you begin navigating to a Favorite location. If you stop sharing your ETA using this method, the person has already received a notification on their device informing them that you're navigating to the Favorite location you selected; however, they're no longer able to access your ETA or route information.

 **IMPORTANT:** This method doesn't permanently remove automatic sharing with that person. The next time you navigate to this same Favorite location, automatic ETA sharing begins again. To prevent this, you must remove the contact from Share ETA in the Favorite location.

1. In the Maps app  on your iPhone or iPad (Wi-Fi + Cellular), tap "Sharing with [*Name of Contact*]" at the bottom of the screen.
2. Identify the person on the list you no longer want to share your ETA with.
3. Select "Tap to stop," located under that person's name.

## Manage location metadata in Photos

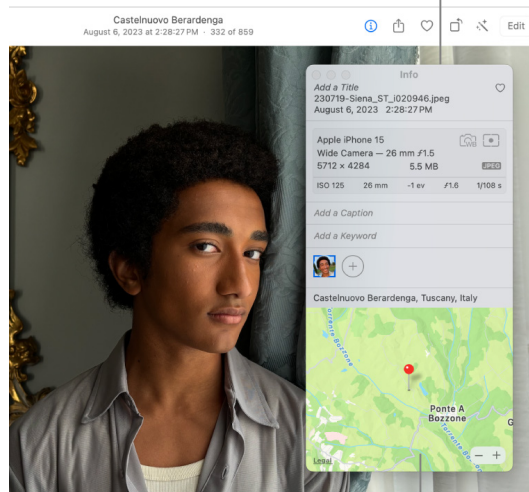
When Location Services is turned on for the Camera app, it uses information known as metadata gathered from cellular, Wi-Fi, GPS networks, and Bluetooth to determine the location coordinates where the photo or video is taken. These coordinates are embedded into each photo and video so that you can later search for them in the Photos app based on the location they were taken, or view location based collections in the Places album.

When photos and videos that include location metadata are shared, the people you share them with may be able to access the location metadata and learn where it was taken. If you're concerned about someone having access to the location metadata associated with your photos or videos, you can remove the current metadata and stop it from being collected in the future.




## Review photos that contain location metadata on iPhone or iPad

Use the Info window to view and edit a photo's information.





If a photo has GPS information, the photo's location appears in the Info window.

You can use the Places album in Photos to easily review the photos in your library that have location metadata embedded.

1. Open the Photos app , then tap Albums.
2. Tap the Places album, then do any of the following:
  - If you want to review the photos from a specific time period, tap Grid to view in chronological order.
  - If you want to review by location taken, tap Map to view by location.



## Review photos that contain location metadata on Mac

You can use the Places album in Photos to easily review the photos in your library that have location metadata embedded.

1. In the Photos app  on your Mac, select the photos you want to review.
2. Click , then review the location information.


## Remove location metadata in Photos on iPhone or iPad

To remove location metadata associated with a certain photo:

1. Open the Photos app , then tap Albums.
2. Tap the Places album, then do one of the following:
  - If you want to review the photos from a specific time period, tap Grid to view in chronological order.
  - If you want to review by location taken, tap Map to view by location.
3. Open the photo you want to remove location metadata from, then tap  or swipe up. You see an image in the Maps app showing where the photo was taken.
4. To remove the location metadata, tap Adjust, then tap Remove Location.


### **Remove location metadata in Photos on Mac**

To remove location metadata associated with photos:

1. In the Photos app  on your Mac, select the photos you want to change.
2. Choose Image > Location, then choose Hide Location or Revert to Original Location.




### **Stop location metadata collection in Camera on iPhone or iPad**

Location metadata in photos and videos can be collected only if your Camera app has access to Location Services.

- Go to Settings , tap Privacy & Security > Location Services > Camera, then tap Never.  
If you don't want to completely stop collecting location metadata, you can turn off Precise Location instead of selecting Never. This allows the Camera app to collect data on your approximate location instead of on your specific location.

### **Don't share location metadata when you share photos in Photos on iPhone or iPad**

You can share photos with others without sharing the location where the photos were taken.

1. Do any of the following:
  - Open the Camera app , select the camera roll, then select one or more photos you want to share.
  - Open the Photos app , then select one or more photos you want to share.
2. Tap , then tap Options.
3. Turn off Location, then tap Done.
4. Share the photos using one of the methods shown in the Share Sheet.

# Manage content

## General

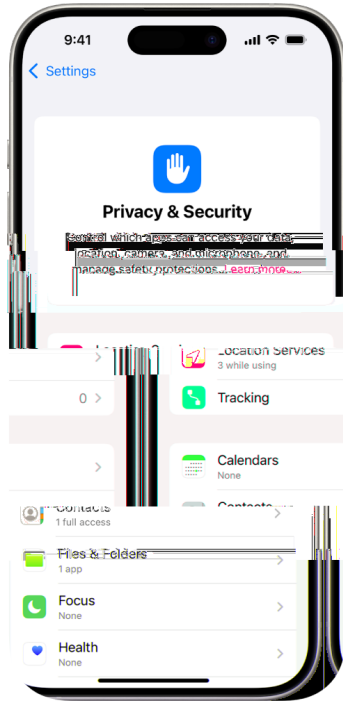
### App privacy features in Apple products





Apple provides settings, features, and controls to help you review and manage the data you share with apps.



## Review and update app privacy settings on Apple devices

Privacy settings on your device have been carefully designed to put you in control of your data. For example, you can allow a social networking app to use your camera so you can take and upload pictures to that app. One reason to review these settings is if someone else set up your device or had access to it and knows your passcode. You want to make sure they haven't changed your settings.




1. Do one of the following:
  - *On your iPhone or iPad:* Go to Settings  > Privacy & Security .
  - *On your Mac:* Choose Apple menu  > System Settings, then click Privacy & Security  in the sidebar.
2. Review the list of data types (for example, Calendars, Contacts, Photos, Reminders, and so on).
3. Select a data type from the list to see which apps on your device have access to it.

An app doesn't appear on the list until it asks for permission, and you can grant or remove permission from any app that has asked for access. For photos you can also change access given to apps. An app can use the data type in the setting only if you have given the app permission.

*Note:* Changing the privacy settings on your Apple device changes only how those apps can access your data. If you want to change the Privacy & Security settings for a third-party app (apps created by companies other than Apple), you must sign in to the third-party account (through its app or through a browser) and update the settings from there.

## Use App Tracking Transparency


App Tracking Transparency allows you to decide whether an app can track your activity across other companies' apps and websites. You can withdraw permissions to track your activity anytime. If you turn off "Allow Apps to Request to Track," you don't get prompts from apps that want to track your activity. Each app that asks for permission to track while this setting is turned off is treated as if you selected Ask App Not to Track.

- Do one of the following:
  - *On your iPhone or iPad:* Go to Settings  > Privacy & Security > Tracking, then turn off Allow Apps to Request to Track.
  - *On your Apple TV:* Go to Settings > General > Privacy & Security > Tracking, then turn off Allow Apps to Request to Track.

## See how apps are accessing your data with App Privacy Report

If you're concerned that someone close to you installed apps on your iPhone or iPad without your permission—or that they changed the settings of apps you installed—you can turn on App Privacy Report.

You'll find details about how often each app accesses your data (for example, your location, camera, and microphone).

1. Go to Settings  > Privacy & Security.
2. Scroll down and tap App Privacy Report.
3. Turn on App Privacy Report.

You can turn off App Privacy Report at any time by going to Settings > Privacy & Security > App Privacy Report. Doing so also clears the report data from your device.

*Note:* App Privacy Report starts gathering information only after you turn it on, so it may take a while for details to appear. You'll see more info as you continue using apps on your device. The data in your App Privacy Report is encrypted and stored only on your device. The report shows how many times—and when—an app accessed privacy-sensitive data or device sensors in the past 7 days. You can tap each app and data type to learn more.

## Review and delete apps

If you're concerned someone may have installed an app on your device without your permission, you can review a list of your apps to make sure you don't have anything you don't want (instructions begin in next section below).

If you're unsure what an app's purpose is, you can look it up in the App Store.

You can review and change the type of data each app has permission to access (like location, photos, etc.) You can do this through the [Safety Check](#) feature in iOS 16 or later.

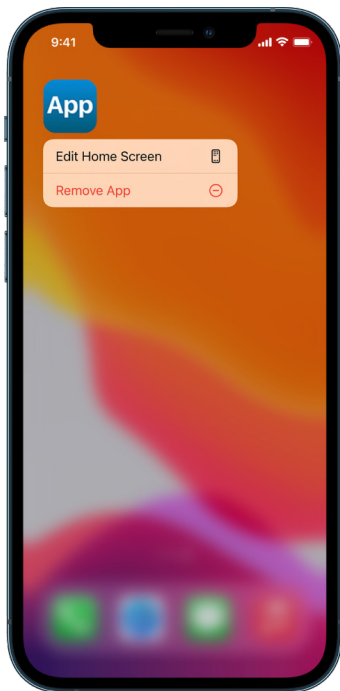
You may also want to review [Third-party app settings](#) only available in-app that cannot be managed through Apple.

⚠️ **IMPORTANT:** Before making changes or deleting information, [consider potential impacts to your safety](#) and privacy.





## To delete an app from App Library on iPhone or iPad



1. Go to the Home Screen, then swipe left past all your Home Screen pages to get to App Library.
2. Tap in the search field. An alphabetized list of all apps on the device appears.
3. If you see an app you want to remove, touch and hold the app's icon until the menu appears.
4. Tap Delete App to delete it.

To learn more, see [Remove or delete apps from iPhone](https://support.apple.com/guide/iphone/iph248b543ca) in the iPhone User Guide.  
(<https://support.apple.com/guide/iphone/iph248b543ca>)


## To delete an app from the Home Screen

1. Touch and hold the app on the Home Screen.
2. Tap Remove App, then tap Delete App to delete it.

To learn more, see [Remove or delete apps from iPhone](https://support.apple.com/guide/iphone/iph248b543ca) in the iPhone User Guide.  
(<https://support.apple.com/guide/iphone/iph248b543ca>)

## Delete an app from a Mac

You can delete apps that may have been downloaded and installed from the internet or from an external device, such as a USB device.

1. Click the Finder icon  in the Dock, then click Applications in the Finder sidebar.
2. Do one of the following:
  - *If an app is in a folder:* Open the app's folder to check for an Uninstaller. If Uninstall [App] or [App] Uninstaller is shown, double-click it, then follow the onscreen instructions.
  - *If an app isn't in a folder or doesn't have an Uninstaller:* If an app isn't in a folder or doesn't have an Uninstaller: Drag the app from the Applications folder to the Trash (at the end of the Dock).

**WARNING:** The app is permanently removed from your Mac the next time you or the Finder empties the Trash. If you have files that you created with the app, you may not be able to open them again. If you decide you want to keep the app, get it back before emptying the Trash. Select the app in the Trash, then choose File > Put Back.

To uninstall apps downloaded from the App Store, use Launchpad.

## Lock or hide apps on your iPhone

If you want to show someone something on your iPhone but want peace of mind that they can't get into certain apps, you can lock or hide the apps.

- *Locking an app:* The app requires Face ID, Touch ID, or your passcode to open. Information inside a locked app won't appear in some locations on your iPhone—for example, in notification previews, search, Siri suggestions, or your call history.
- *Hiding an app:* The app is locked as described above; it also disappears from your Home Screen and moves to the Hidden folder at the bottom of App Library. The app is still visible in other places on your iPhone.

🚩 **IMPORTANT:** When you lock or hide an app on your device, it's only locked or hidden on that device. The locked or hidden status of an app doesn't sync with iCloud.

*Note:* Children under 13 in a Family Sharing group can't lock or hide apps. Anyone aged 13 to 17 in a Family Sharing group can lock or hide an app, but a parent or guardian in the family group can see that the app was downloaded and how much time it's used, and restrict access to it using Screen Time. (These ages vary by country or region.)



### Lock an app

*Note:* Some of the apps that come with iPhone can't be locked—including Calculator, Camera, Clock, Contacts, Find My, Maps, Shortcuts, and Settings.

1. Go to the Home Screen on your iPhone, then locate the app you want to lock.
2. Touch and hold the app icon until the quick actions menu opens.
3. Tap Require Face ID (or Touch ID or Passcode).
4. Tap Require Face ID (or Touch ID or Passcode) again, then authenticate using Face ID (or Touch ID or a passcode).

## Hide an app




*Note:* Apps that come installed with iOS 18 or later can't be hidden—only apps you download separately can be hidden.

1. Go to the Home Screen on your iPhone, then locate the app you want to hide.
2. Touch and hold the app icon until the quick actions menu opens.
3. Tap Require Face ID (or Touch ID or Passcode).
4. Tap Hide and Require Face ID (or Touch ID or Passcode) again, authenticate using Face ID (or Touch ID or a passcode), then tap Hide App.

## Where are hidden apps visible?

To use your hidden apps, go to the Home Screen, swipe left past all your Home Screen pages to get to App Library, tap the Hidden folder, then authenticate using Face ID, Touch ID, or a passcode.

There are a few other places you may be able to see the names of hidden apps:

- Settings  > Apps > Hidden Apps (requires authentication using Face ID, Touch ID, or a passcode)
- Settings  > Screen Time
- Settings  > Battery > Battery Health & Charging
- App Store purchase history. See the Apple Support article [Hide purchases from the App Store](https://support.apple.com/108091) (<https://support.apple.com/108091>).

## Unhide apps

You can stop hiding an app so that you can see it on the Home Screen again.

1. Go to the Home Screen on your iPhone.
2. Swipe left past all your Home Screen pages to go to App Library.
3. Tap the Hidden folder at the bottom of App Library, then authenticate using Face ID (or Touch ID or a passcode).
4. To move the app out of the Hidden folder, touch and hold the app, tap Don't Require Face ID (or Touch ID or Passcode), then authenticate using Face ID (or Touch ID or a passcode).

The app appears on your Home Screen and near the top of App Library.

# Third-party app settings

## Introduction to third-party apps

In the Apple ecosystem, there are two kinds of apps available:

- *First-party apps*: Developed by Apple, such as Messages, Calendar, Safari, or FaceTime.
- *Third-party apps*: Developed by companies and organizations other than Apple, such as Instagram, YouTube, Threads, or Google.

Third-party apps are available on the App Store or alternative app stores. Their account settings and controls may vary from apps developed by Apple, and some of those controls may only be accessible inside the app or through the third-party app developer's website. This distinction is important, because third-party apps generally require extra steps to manage sharing and privacy settings.

## Apple settings for third-party apps

Some settings for third-party apps can be managed in the Settings app. These settings include what Apple device functionality the app can access and use. Some examples include access to Location, Contacts, Photos, or the ability to send notifications.

To manage these settings, go to Settings , scroll down, then tap the app you want to manage.

## Third-party settings only available in-app

Some third-party app settings cannot be managed through Apple, and instead can only be managed directly in-app. To manage how third-party apps are sharing information with others, open the app and navigate to account settings. These settings may be listed under another name such as "Preferences," and some settings may be listed in different sections of account settings. Important areas to review are any safety, security, privacy, data sharing, and discoverability settings. For some apps, searching their support articles or FAQs will be necessary to find all the available settings to manage.

*Note:* In some cases, certain settings, such as deleting your account or requesting a copy of your data, may only be available to manage through the third-party app developer's website. If you want to change account settings you must sign in to the third-party app's website and update the settings from there.

## Blocking, muting, and unfriending

Managing relationships within the Apple ecosystem does not extend to individuals and communications in a third-party app. For example, blocking someone in Messages, Phone, or FaceTime don't result in them being blocked in Instagram. Those relationships must be managed from within the third-party app itself. Check the third-party app's support site for more information on temporarily or permanently blocking, muting, or unfriending a user.

## Review forwarding settings


You can review and manage how you forward content and whom you forward it to.

▼ **IMPORTANT:** Before making changes or deleting information, [consider potential impacts to your safety](#) and privacy.




### Manage iCloud Mail forwarding

You can see whether your messages in iCloud Mail are being automatically forwarded to another email address and easily disable forwarding.

1. Sign in to iCloud at <https://www.icloud.com> with your Apple Account user name and password. If necessary, enter the two-factor authentication code.
2. Click Mail, then click  at the top of the Mailboxes list, then choose Preferences.
3. In the General tab, see whether "Forward my email to" is selected and which addresses your email is being forwarded to. If necessary, remove the forwarding address and stop forwarding mail messages.
4. In the Rules tab, review any rules where the "Then" option is set to "Forward to" or "Forward to an Email Address and Mark as Read," and if necessary, change the rule accordingly.
5. Sign out of iCloud.

### Manage text message forwarding on iPhone

When you send a message to someone who uses a phone other than an iPhone, your message is sent as a text message. You can set up your iPhone so that when you send or receive a text message, it appears on other devices where you're signed in to your Apple Account. Those devices can also send new text messages. If you're concerned that your messages are being forwarded to other devices, you can review the device list and disable text message forwarding.

1. On your iPhone, go to Settings  > Apps > Messages.
2. Tap Text Message Forwarding to see which devices are able to send and receive text messages from your device.
3. Turn off any devices you don't want to receive or send text messages from.

## Manage call forwarding and calls on other devices on iPhone

Depending on your cellular carrier, your iPhone may be able to forward calls you receive to another phone number. You can check to see if calls you receive are being forwarded to another phone number and turn off this feature.

1. On your iPhone, go to Settings  > Apps > Phone > Call Forwarding.

If the slider bar is green, it means that call forwarding is turned on and you can see which phone number your calls are being forwarded to.

*Note:* If you don't see this option, call forwarding is unavailable on your iPhone. Call your cellular carrier for more information.

2. If necessary, turn off call forwarding.

Turning off call forwarding doesn't notify the phone number that was receiving forwarded calls.

## Hide photos and videos on Apple devices

In Photos on your iPhone, iPad, or Mac, you can hide photos that you don't want to display. The hidden photos remain in your library, and you can reveal them later if you want to.



### Hide photos temporarily on iPhone or iPad

1. Go to the Photos app 📷 on your iPhone or iPad.
2. Touch and hold the photo that you want to hide.
3. Tap Hide, then confirm that you want to hide the photo.  
The selected photo disappears from view but isn't deleted.

### Hide photos temporarily on Mac


1. Go to the Photos app 📷 on your Mac.
2. Click Library in the sidebar, then select the photos that you want to hide.
3. Choose Image > Hide [number] Photos, then click Hide.  
The selected photos disappear from view but aren't deleted.

### Show photos that you've hidden on iPhone or iPad

1. Go to the Photos app 📷 on your iPhone or iPad.
2. Scroll down and tap Hidden (below Utilities).  
**💡 Tip:** On iPad, you may need to tap the sidebar icon in the upper-left corner first to see your albums.
3. Tap View Album, then use Face ID or Touch ID to unlock your Hidden album.
4. Touch and hold the photo or video that you want to unhide, then tap Unhide.



### Show photos that you've hidden on Mac

1. Go to the Photos app  on your Mac.
2. Click Library in the sidebar, then choose View > Show Hidden Photo Album.  
The Hidden album appears in the sidebar, in Utilities. If the Hidden album is locked, use Touch ID or enter your password to unlock it. To hide the Hidden Album, choose View > Hide Hidden Photo Album.
3. Select the photos you want to display, then choose Image > Unhide [number] Photos.

### Show or hide the Hidden collection on iPhone or iPad


By default, the Hidden album is visible in the Utilities collection. You can hide it from view at any time.

1. On your iPhone or iPad, go to Settings > Apps > Photos.
2. Scroll down, then do any of the following:
  - *Show the Hidden Album in Utilities:* Turn on Show Hidden Album.
  - *Hide the Hidden Album:* Turn off Show Hidden Album.

The Hidden album requires Face ID, Touch ID, or a passcode to unlock it. To change that setting, see Photos settings.

### Show or hide the Hidden collection on Mac

By default, the Hidden album is locked and hidden from view. You can allow it to be visible in the Utilities collection, and hide it from view at any time.

1. Go to the Photos app  on your Mac.
2. Click Library in the sidebar, then do any of the following:
  - *Show the Hidden Album in Utilities:* Choose View > Show Hidden Photo Album.
  - *Hide the Hidden Album:* Choose View > Hide Hidden Photo Album.





The Hidden album requires a password or Touch ID to unlock it. To change that setting, see Photos settings.

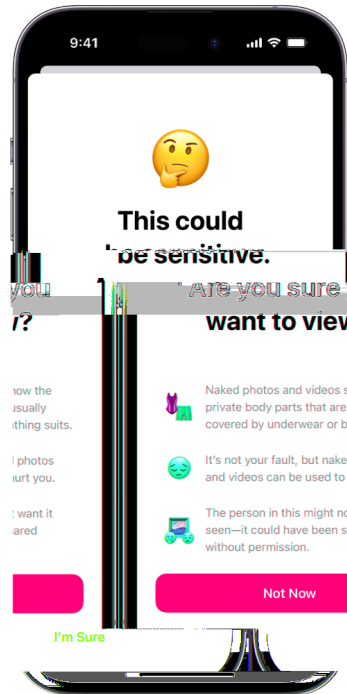
## Sensitive image and video warnings

The Sensitive Content Warning helps adult users avoid seeing unwanted nude images and videos when receiving them in Messages, in AirDrop, in a FaceTime video message, and in the Phone app when receiving a Contact Poster—all using the same privacy-preserving technology at the core of Communication Safety. The feature is optional and can be turned on by the user in Privacy & Security settings.



## Set up a Sensitive Content Warning on iPhone, iPad, or Mac

1. Do one of the following:
  - *On your iPhone or iPad:* Go to Settings  > Privacy & Security , then tap Sensitive Content Warning.
  - *On your Mac:* Choose Apple menu  > System Settings, click Privacy & Security  in the sidebar, then click Sensitive Content Warning.



2. Turn on Sensitive Content Warning.

If Sensitive Content Warning determines that you've received a photo or video that appears to contain nudity, it blurs the image, displays a warning that the content appears to be sensitive, and offers ways to get help.

## Obtain evidence related to another Apple Account

Apple is committed to protecting the security and privacy of our users. If you're experiencing technology-enabled abuse, stalking, or harassment and want to request evidence related to another person's account, you should partner with local law enforcement or courts to submit the request. In recognizing the ongoing digital evidence needs of law enforcement agencies, we have a team of dedicated professionals within our legal department who manage and respond to all legal requests received from law enforcement agencies globally.

All other requests for information regarding Apple customers, including customer questions about information disclosure, should be directed to <https://www.apple.com/privacy/contact/>.

### Apple's guidelines for law enforcement requests

See the following guidelines for law enforcement requests, for inside and outside the United States:

- *Inside the United States:* [The Legal Process Guidelines](https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf)  
(<https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>)
- *Outside the United States:* [The Legal Process Guidelines](https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf)  
(<https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf>)

## Record suspicious activity

If you're experiencing harassment or are concerned about suspicious activity on your account or device, you can take a screenshot or screen recording of the related content. A screenshot is a picture of what appears on your device's screen. A screen recording is a video of what appears on your device's screen, and includes any related audio playing through the device at the time of the recording. You can save these as image or video files on your iPhone, iPad, or Mac.

If you want to request information from Apple about another person's account related to a stalking or harassment case, see [Obtain evidence related to another Apple Account](#) later in this guide.



### Take a screenshot or screen recording on your iPhone or iPad

1. Do one of the following:
  - On your iPhone or iPad with Face ID: Simultaneously press and then release the side button and volume up button.
  - *On your iPhone or iPad with a Home button:* Simultaneously press and then release the Home button and the side button or Sleep/Wake button (depending on your model).
2. Tap the screenshot in the lower-left corner, then tap Done.
3. Choose Save to Photos, Save to Files, or Delete Screenshot.

If you choose Save to Photos, you can view it in the Screenshots album in the Photos app, or in the All Photos album if iCloud Photos is turned on in Settings > Photos.

## Take pictures or screen recordings on your Mac

1. Press Shift-Command-5 (or use Launchpad) to open the Screenshot app and display the tools.



2. Click a tool to use to select what you want to capture or record.

For a portion of the screen, drag the frame to reposition it or drag its edges to adjust the size of the area you want to capture or record.


Action	Tool
Capture the entire screen	
Capture a window	
Capture a portion of the screen	
Record the entire screen	
Record a portion of the screen	

3. Select any options you want.

The available options vary based on whether you're taking a screenshot or a screen recording. For example, you can choose to set a timed delay or show the mouse pointer or clicks, and specify where to save the file.

The Show Floating Thumbnail option helps you work more easily with a completed shot or recording. It floats in the bottom-right corner of the screen for a few seconds so you have time to drag it into a document, mark it up, or share it before it's saved to the location you specified.

4. Start the screenshot or screen recording:

- *For the entire screen or a portion of it:* Click Capture.
- *For a window:* Move the pointer to the window, then click the window.
- *For recordings:* Click Record. To stop recording, click  in the menu bar.

When the Show Floating Thumbnail option is set, you can do any of the following while the thumbnail is briefly displayed in the bottom-right corner of the screen:

- Swipe right to immediately save the file and make it disappear.
- Drag the thumbnail into a document, an email, a note, or a Finder window.
- Click the thumbnail to open a window; there you can mark up the screenshot—or trim the recording—and share your result.

Depending on where you chose to save the screenshot or recording, an app may open.

## Restore device to factory settings

If you're concerned someone may have had physical access to your device, tampered with its built-in security, and installed malicious software like stalkerware, you can restore the device to its factory settings. This helps ensure that your device can be accessed only by you.

### ⚠️ IMPORTANT:

- A factory reset erases all content and settings. Before restoring the device to factory settings, run Safety Check's [Manage Sharing & Access \(option two\)](#). The issues you're concerned about may be related to sharing settings or app access that you didn't realize were in place.
- If you're erasing all content and settings because you're concerned your device was tampered with and had malicious software installed, don't restore from a backup. Restoring from a backup may reinstall the malicious software you're trying to remove.

A factory restore:

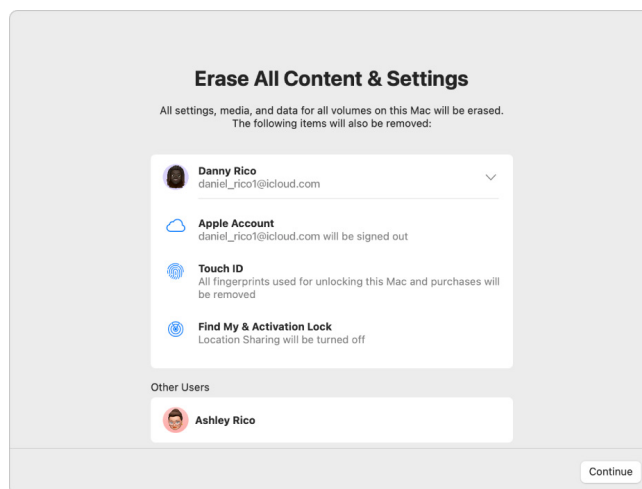
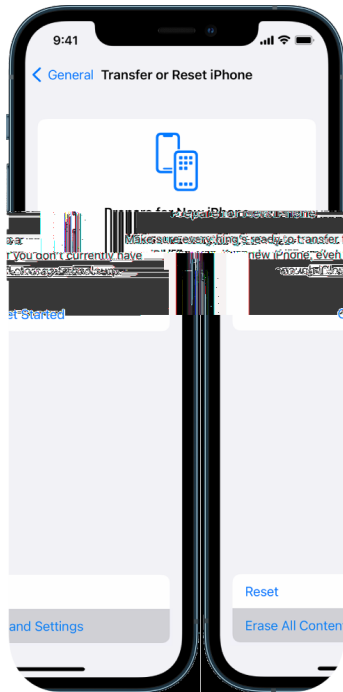
- Erases all data stored on the device, including Face ID and Touch ID data, passcode and passwords, messages, emails, photos, files, media, and more
- Removes all apps, including any installed without your knowledge
- Resets your privacy settings so you aren't sharing location with any people or apps
- Installs the latest version of the operating system software (regardless of the previously installed version)



Requirements:

- Internet access
- Device passcode or password
- Apple Account password
- Time

If you want to use Erase All Content and Settings on your Mac, you must have macOS 12.0.1 or later. Alternatively, you can erase your Mac. See the Apple Support articles “[Use Disk Utility to erase a Mac with Apple silicon](https://support.apple.com/102506)” (https://support.apple.com/102506) and “[Use Disk Utility to erase an Intel-based Mac](https://support.apple.com/102639)” (https://support.apple.com/102639).



### For iPhone and iPad

- “[Restore your iPhone or iPad to factory settings using a computer](https://support.apple.com/108931)” (https://support.apple.com/108931) — Apple Support article



### **Erase all content and settings on Mac**

- Erase your Mac (macOS 12.0.1 or later)—Remove your content, settings, and any apps you installed without reinstalling macOS in order to restore it to factory settings.
  - ["Erase your Mac"](https://support.apple.com/guide/mac-help/mchl7676b710) to erase your content (apps, data) and settings (for example, before you sell, trade, or give it away) (<https://support.apple.com/guide/mac-help/mchl7676b710>).
  - ["Erase and reinstall macOS"](https://support.apple.com/guide/mac-help/mh27903) for a Mac with Apple silicon or an Intel-based Mac. (<https://support.apple.com/guide/mac-help/mh27903>)
- ["Use Disk Utility to erase a Mac with Apple silicon"](https://support.apple.com/102506) — Apple Support article (<https://support.apple.com/102506>)
- ["Use Disk Utility to erase an Intel-based Mac"](https://support.apple.com/102639) — Apple Support article (<https://support.apple.com/102639>)

## Specific apps and features

### Make an emergency call or text on iPhone or Apple Watch

In case of emergency, you can use iPhone or Apple Watch to quickly call or text for help.




If you choose to share your Medical ID, iPhone can send your medical information to emergency services when you call or text 911 or use Emergency SOS (U.S. only). To learn more about Medical ID, see ["Create a Medical ID"](#) in the iPhone User Guide (<https://support.apple.com/guide/iphone/iph08022b194/#iphbcea12902>).

*Note:* For emergency help in some areas, you can also send a text message to 911. In places that don't offer this, you might receive a "bounce-back" message indicating that the text didn't go through. See the Apple Support article ["Text 911 on iPhone or Apple Watch"](#) (<https://support.apple.com/101996>).

With Emergency SOS, you can quickly and easily call for help and alert your emergency contacts. Because of this, it's important to make sure that the person or people assigned as emergency contacts are people you trust.




## Change your Emergency SOS settings on iPhone

1. Go to Settings  > Emergency SOS.
2. Do any of the following:
  - *Turn Call with Hold on or off:* Press and hold the side and volume buttons to start a countdown to call emergency services.
  - *Turn Call with 5 presses on or off:* Rapidly press the side button five times to start a countdown to call emergency services.
  - *Manage your emergency contacts:* In Health, tap Set Up Emergency Contacts or Edit Emergency Contacts. See “[Set up and view your Medical ID](#)” in the iPhone User Guide (<https://support.apple.com/guide/iphone/iph08022b192>).


## Set up or change emergency contacts on iPhone

Emergency contacts can be set up so that if you call an emergency number, iPhone sends those contacts a notice that you’ve called for help, shares your location with those contacts, and notifies them if your location changes. If you previously added someone as an emergency contact and want to remove them, you can delete them.

To add or delete emergency contacts:

1. Open the Health app , then tap your profile picture.
2. Tap Medical ID.
3. Scroll to Emergency Contacts, then tap Edit.
4. Add or delete a contact.
  - *Add a contact:* Tap  to add an emergency contact (You can’t set emergency services as an SOS contact).
  - *Delete a contact:* Tap  next to the contact you want to delete, then tap Delete.
5. Tap Done to save your changes.

## Make an Emergency call when iPhone is locked


1. On the Passcode screen, tap Emergency.
2. Dial the emergency number (for example, 911 in the U.S.), then tap .

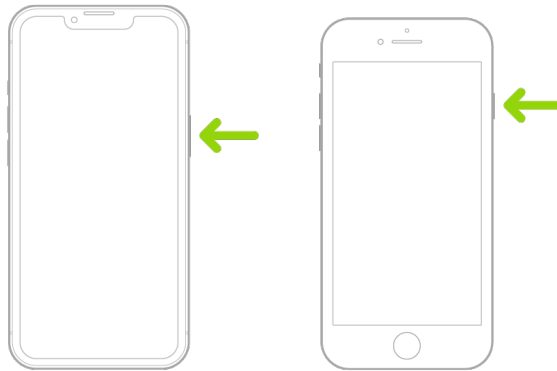
## Use Emergency SOS with iPhone (all countries or regions except India)

In case of emergency, use your iPhone to quickly and easily call for help and alert your emergency contacts (provided that cellular service is available). After an emergency call ends, your iPhone alerts your emergency contacts with a text message, unless you choose to cancel. Your iPhone sends your current location (if available) and—for a period of time after you enter SOS mode—your emergency contacts receive updates when your location changes.

*Note:* If you have iPhone 14 or later (any model), you may be able to contact emergency services through satellite if cell service isn't available. See ["Use Emergency SOS via satellite on your iPhone"](#) later in this guide.

- Simultaneously press and hold the side button and either volume button until the sliders appear and the countdown on Emergency SOS ends, then release the buttons.

Or you can enable iPhone to start Emergency SOS when you quickly press the side button five times. Go to Settings  > Emergency SOS, then turn on Call with 5 Presses.



## Use Emergency SOS with iPhone (India)

- Quickly press the side button three times until the sliders appear and the countdown on Emergency SOS ends.
- If you've turned on Accessibility Shortcut, simultaneously press and hold the side button and either volume button until the sliders appear and the countdown on Emergency SOS ends, then release the buttons.

By default, iPhone plays a warning sound, starts a countdown, and then calls the emergency services.

After an emergency call ends, your iPhone alerts your emergency contacts with a text message, unless you choose to cancel. Your iPhone sends your current location (if available) and—for a period of time after you enter SOS mode—your emergency contacts receive updates when your location changes.

## Contact emergency services with Apple Watch

Do one of the following:

- Press and hold the side button until the sliders appear, then drag the Emergency Call slider to the right.



Your Apple Watch calls the emergency services in your region—for example, 911. (In some regions, you may be required to press a keypad number to complete the call.)

- Press and keep holding the side button until your Apple Watch issues a warning sound and starts a countdown. When the countdown ends, your Apple Watch calls emergency services. The Apple Watch makes the warning sound even if it's in silent mode, so if you're in an emergency situation where you don't want to make noise, use the Emergency Call slider to call emergency services without a countdown.

If you don't want your Apple Watch to automatically start the emergency countdown when you press and hold the side button, turn off Automatic Dialing. Open the Settings app on your Apple Watch, tap SOS, tap Hold Side Button, then turn off Hold Side Button. (Or open the Apple Watch app on your iPhone, tap My Watch, tap Emergency SOS, then turn off Hold Side Button to Dial.) You can still make an emergency call with the Emergency Call slider.




- Say "Hey Siri, call 911."

## Text Emergency Services from your iPhone (not available in all countries or regions)

1. Open the Messages app , then type 911 or your local emergency services number in the To field.
2. In the Text Message field, type your emergency.
3. Tap .

**Important:** After you text 911, your iPhone enters emergency mode for 30 minutes. To get out of emergency mode, restart your iPhone.

## Text Emergency Services from your Apple Watch (not available in all countries or regions)

1. Open the Messages app , then tap New Message.
2. Tap Add Contact.
3. Tap , type 911, then tap OK.
4. Tap Create Message, then tap SMS.
5. Write a message with your finger, tap  to dictate a message, or type a message with the keyboard.
6. Tap Done, then tap Send.

**Important:** After you text 911, your Apple Watch enters emergency mode for 30 minutes. To get out of emergency mode, restart your Apple Watch.

## Use Emergency SOS via satellite on your iPhone

On iPhone 14 and later (any model) with iOS 16.1 or later, you can use Emergency SOS via satellite to text emergency services when you're outside cellular and Wi-Fi coverage. To learn more, see the Apple Support article "[Use Emergency SOS via satellite on your iPhone 14](https://support.apple.com/101573)" (<https://support.apple.com/101573>).

You can also use the Find My app to share your location with people via satellite. See "[Send your location via satellite in Find My on iPhone](https://support.apple.com/guide/iphone/iph2aac8ae20)" in the iPhone User Guide (<https://support.apple.com/guide/iphone/iph2aac8ae20>).




For more information, see [Important information about emergency calls on iPhone](#) in the iPhone User Guide.

## Manage Screen Sharing and Screen Control in FaceTime

During a one-to-one FaceTime video or audio call, you can share your screen with another person, or they can request to see your screen. After you share your screen, they can request or you can allow them to remotely control your screen.



### How can you tell if screen sharing or screen control is on?

- *Screen sharing:* On an iPhone or iPad,  appears at the top of the screen. You can also tap the screen to show FaceTime controls, then check for “Viewing My Screen” below a person’s name or contact information.  
On a Mac,  appears in the menu bar.
- *Screen control:* On an iPhone or iPad, “Remote Control Active” appears at the bottom of the screen.  
On a Mac,  appears in the menu bar.

### **What can the other person do during screen sharing?**

The person you're sharing your screen with can:

- See most of the content on your screen.
- Tap, draw, or write on your screen (the circle, drawing, or writing disappears after a few seconds).
- Request remote control of your device (you can accept or deny).

The person you're sharing your screen with with *cannot*:

- See any notifications you get.
- See the keypad when you enter your passcode. (By default, passcodes and passwords appear as dots.)
- See content that requires a subscription, a free trial, or a purchase or rental to view.

### **What can the other person do during screen control?**

The person remotely controlling your screen can:

- Open and close apps, windows, or files.
- Change settings.
- Delete items.
- Send messages.
- Shut down your device or restart your Mac (this ends the FaceTime call and screen control).



The person remotely controlling your screen *cannot*:

- Change certain Apple Account or Face ID & Passcode settings.
- Use Apple Pay. (They may be able to make payments with third-party apps; see [Introduction to third-party apps](#).)
- Erase your device.

Your Face ID is disabled during a remote control session. You can still navigate your device while your screen is remotely controlled—your actions take priority over remote actions.



### **Stop screen sharing**


- *iPhone or iPad:* Tap .
- *Mac:* Click  in the menu bar, then click Stop Sharing.

Ending a FaceTime call also ends screen sharing.

### **Decline a remote control request**

If you receive a remote control request that you want to decline, tap or click Don't Allow. Screen sharing continues. The other person doesn't receive a notification that you declined.

### **Stop remote control**

- *iPhone or iPad:* Tap Stop at the bottom of the screen sharing window.
- *Mac:* Click  in the menu bar, then click Allow Control. (The button is dimmed.)

Ending a FaceTime call also ends remote control.

## Manage Activity sharing on Apple Watch


If you have an Apple Watch and previously shared your Activity rings with someone, they can see information about your activity level and workouts. It doesn't give them any information about your location.



### Use your Apple Watch to stop sharing

You can hide your progress, or stop sharing your activity with a particular person entirely, from the Sharing tab in the Activity app.

To stop sharing Activity rings with someone using your Apple Watch.

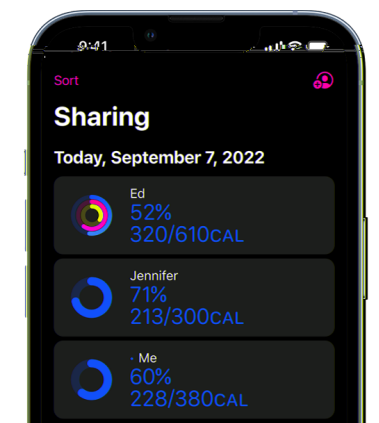
1. Open the Activity app  on your Apple Watch.
2. Swipe left, then turn the Digital Crown to scroll to the bottom of the screen.
3. To remove someone you're sharing with, tap their name, then tap Remove.


To learn more, see:

- ["Share your activity from Apple Watch"](https://support.apple.com/guide/watch/apd68a69f5c7) in the Apple Watch User Guide (<https://support.apple.com/guide/watch/apd68a69f5c7>)

## Use your iPhone to stop sharing

You can stop sharing Activity rings with someone using your iPhone.




1. Open the Fitness app  on your iPhone, then tap Sharing.
2. Tap a person you share with.
3. Tap the Share button in the top-right hand corner of the screen.
4. Tap either Remove Friend or Hide my Activity.

To learn more, see:

- ["Share your activity from Apple Watch"](https://support.apple.com/guide/watch/apd68a69f5c7) in the Apple Watch User Guide (<https://support.apple.com/guide/watch/apd68a69f5c7>)

# Secure AirDrop

## What is AirDrop?

AirDrop  is an easy way to share images, documents, or other files between Apple devices that are near each other. You can enable your device to share with everyone near you, limit sharing to only your contacts, or share with no one.

*Note:* The Contacts Only option is available on devices with iOS 10, iPadOS 13.1, and macOS 10.12, or later. If your device uses an earlier software version and you want to limit who can send files to you over AirDrop, you can turn it on when you need it and then disable it when not in use.



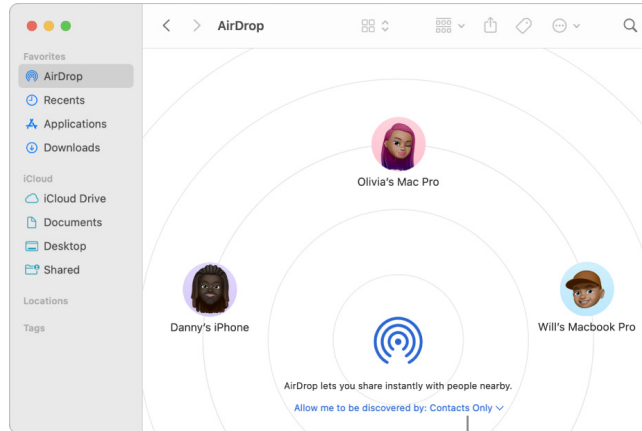
## iPhone or iPad

- On your iPhone or iPad, go to Settings  > General, tap AirDrop, then choose an option that works best for you.


To learn more, see:

- ["Use AirDrop on iPhone to send items to nearby devices"](https://support.apple.com/guide/iphone/iphcd8b9f0af) in the iPhone User Guide (<https://support.apple.com/guide/iphone/iphcd8b9f0af>)
- ["Use AirDrop on iPad to send items to nearby devices"](https://support.apple.com/guide/ipad/ipadf0a1530e) in the iPad User Guide (<https://support.apple.com/guide/ipad/ipadf0a1530e>)

## On a Mac using the Finder



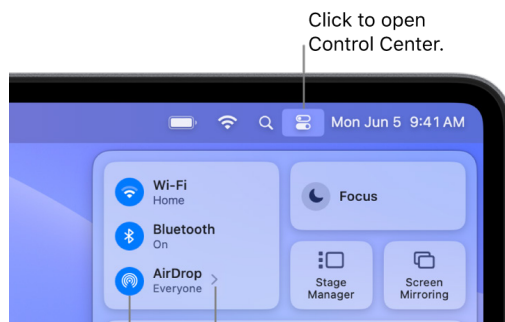
Control who can send items to you.

1. Click the Finder icon  in the Dock to open a Finder window.
2. In the Finder sidebar, click AirDrop.
3. In the AirDrop window, click the "Allow me to be discovered by" pop-up menu, then choose an option that works best for you.

To learn more, see:

- [Use AirDrop on your Mac to send items to nearby devices](https://support.apple.com/guide/mac-help/mh35868) in the Mac User Guide (<https://support.apple.com/guide/mac-help/mh35868>)




## On a Mac using Control Center



Click to turn AirDrop on or off.

Click to choose who can send items to you.

Click to open Control Center.

1. On a Mac, click  in the menu bar, then click . When it's blue, it's on.
2. Click  next to AirDrop, then choose an option that works best for you.

To learn more, see:

- [Use AirDrop on your Mac to send items to nearby devices](https://support.apple.com/guide/mac-help/mh35868) in the Mac User Guide (<https://support.apple.com/guide/mac-help/mh35868>)



## Manage Calendar sharing settings on Apple devices

If you previously invited a person to share your calendar, you can manage their ability to edit the calendar, or you can stop sharing the calendar with that person.

**IMPORTANT:** When you delete or stop sharing a calendar, other participants may be notified about the changes.




### Manage calendar sharing settings on iPhone or iPad

1. Tap Calendar  on your iPhone or iPad, then tap  next to the shared calendar you want to edit.
2. Tap a person, then do any of the following:
  - Turn Allow Editing on or off.
  - Tap Stop Sharing.

### Delete a calendar on Mac

Some calendars can't be deleted.

- You can't delete delegated calendars, but you can stop showing them in the main Calendar window. See [Unpublish a calendar on Mac](#).
- If you can't delete a calendar for a particular calendar account, try deleting the calendar on the account provider's website. For example, to delete a Google calendar, go to [google.com](https://google.com).
- If a calendar account has only one calendar (not counting other people's calendars you're sharing), you can't delete that last calendar.

1. Open the Calendar app  on your Mac, then click the calendar's name in the calendar list.

If you don't see the calendar list on the left, choose View > Show Calendar List.


2. Choose Edit > Delete.

To learn more, see:

- ["Add or delete calendars on Mac"](#) in the Calendar User Guide (<https://support.apple.com/guide/calendar/icl1005>)

## Unsubscribe from a calendar on Mac

If you want to stop subscribing to someone else's calendar, you can unsubscribe from it.

- Open the Calendar app  on your Mac, control-click the calendar in the calendar list, then choose Unsubscribe.

If you don't see the calendar list on the left, choose View > Show Calendar List.

*Note:* When unsubscribing from a calendar, you can also report it as junk. Reporting junk helps Calendar better identify junk subscriptions.


To learn more, see:

- "[Subscribe to calendars on Mac](https://support.apple.com/guide/calendar/icl1022)" in the Calendar User Guide (<https://support.apple.com/guide/calendar/icl1022>)


## Unpublish a calendar on Mac

If your calendar list has an On My Mac section, you can publish a calendar in that section on a WebDAV server you have access to. Other people can subscribe to your published calendar or view it in a web browser. At any time, you can stop publishing a calendar without deleting it from your Mac.

*Note:* Unpublished calendars aren't deleted from your Mac.

1. Open the Calendar app  on your Mac, then click the name of the calendar or calendar group in the calendar list.

If you don't see the calendar list on the left, choose View > Show Calendar List.

A published calendar has  next to its name.

2. Choose Edit > Stop Publishing.

After you unpublish a calendar, new users aren't able to subscribe to it. Users who are already subscribed to it see the last published copy until they delete it.


To learn more, see:

- "[Publish or unpublish calendars on Mac](https://support.apple.com/guide/calendar/icl1017)" in the Calendar User Guide (<https://support.apple.com/guide/calendar/icl1017>)

## Stop sharing an iCloud calendar on Mac


If you [set up iCloud on your Mac](#), you can use Calendar to manage your shared iCloud calendars. If you share an iCloud calendar or join someone else's shared iCloud calendar, you may receive email whenever the shared calendar is updated. You can stop receiving these emails by changing a setting in Calendar settings on iCloud.com.

If you receive an invitation to join an iCloud shared calendar, you can accept the invitation on your iPhone, iPad, or Mac where you're signed in to the same Apple Account, or on iCloud Calendar, or on iCloud.com.

1. Open the Calendar app  on your Mac.

If you don't see the calendar list on the left, choose View > Show Calendar List.

2. Do any of the following:

- *Stop sharing your calendar with specific people:* Place the pointer over the calendar's name in the calendar list, then click . Click a person's name, then press Delete.
- *Stop sharing your calendar with everyone:* Control-click the calendar in the calendar list, then choose Stop Sharing.
- *Stop subscribing to someone else's calendar:* Control-click the calendar in the calendar list, then choose Unsubscribe.

When unsubscribing from a calendar, you can also report it as junk. Reporting junk helps Calendar better identify junk subscriptions.


To learn more, see:

- ["Receive updates to calendars on iCloud.com"](#) in the Calendar User Guide (<https://support.apple.com/guide/icloud/mm8074582205>)



## Manage Family Sharing settings

Family Sharing can be used by up to five family members to share subscriptions, purchases, photos, photo albums, a calendar, and more, all without sharing each other's Apple Accounts. If you're sharing an iCloud storage plan, each person's files and documents remain private, while the amount of storage space being used by each person is visible to all members.

To see if you're part of a Family Sharing group, go to Settings  > [your name] > Family. If you see Set Up Family Sharing, you aren't using Family Sharing with this Apple Account. If you see an icon with Family Sharing, you can tap the icon to see your family members and roles.



### Who can leave a Family Sharing group?

The ability to change or leave a Family Sharing group varies.

- An organizer can leave a Family Sharing group by turning off Family Sharing. When Family Sharing is turned off, all family members are removed from the family group at once. If there are children under 13 in the family group, the organizer must transfer them to another Family Sharing group. Family members will no longer be able to share access to subscriptions, purchases, and other services enabled through Family Sharing.
- Any family member over the age of 13 can remove themselves from a family group at any time. Just select your name and then select Leave Family. You can also sign in to the Apple Account website and choose Remove Account in the Family Sharing section.
- For security reasons, a child (under 13) account can't remove themselves from a family and can't stop sharing details such as Screen Time without the Screen Time passcode. The organizer has access to shared family content on your device, such as shared photo albums and shared calendars, and can view Screen Time activity.

## Types of Family Sharing members

Members of a Family Sharing group can have different roles depending on their age.

*Note:* The age at which someone is considered an adult or child varies by country or region.



To change your Family Sharing status, it's good to know how the different roles within Family Sharing groups work.

- *Organizer:* An adult who sets up a Family Sharing group. The organizer can invite family members, remove family members, and disband the group.
- *Adult:* A member of the Family Sharing group who's 18 years or older.
- *Parent/Guardian:* An adult member of the Family Sharing group who can help manage parental controls for children in the group. When the organizer adds an adult to the Family Sharing group, they can designate them as a parent or guardian.
- *Child or teen:* A member of the Family Sharing group under the age of 18. The organizer, parent, or guardian can create an Apple Account for a child who's too young to create their own.

In your household one adult, the *family organizer*, chooses the features the family shares and invites up to five additional members to join. After the invitations are accepted, Family Sharing is set up on everyone's devices automatically—including a shared calendar and shared photo album. The family organizer can add anyone who has an Apple Account to their family and remove anyone over the age of 13 from the family group.


## What happens when you leave a Family Sharing group

If a member is removed or leaves the Family Sharing group, they keep purchases paid for using the shared credit card but they immediately lose access to other things the family members share:

- Former family members' device locations don't appear in the Find My app on iCloud.com or on the Mac, iPhone, or iPad.
- Former family members' items no longer appear in the Purchased section of the iTunes Store, the App Store, and Apple Books.
- Music, movies, TV shows, books, and apps previously downloaded are no longer usable if someone else originally purchased them. Former family members can no longer use this content downloaded from your collection.
- In-app purchases become unavailable if they were purchased using an app someone else originally purchased. You can regain access to the in-app purchases by purchasing the app.


### Leave a Family Sharing group on your iPhone or iPad with iOS 18, iPadOS 18, or later

If you're over the age of 13 and are a member of a Family Sharing group:

1. Go to Settings  > Family (below your name).
2. Tap your name, then tap Stop Using Family Sharing.




### Leave a Family Sharing group on your iPhone or iPad with iOS 17, iPadOS 17, or earlier

If you're over the age of 13 and are a member of a Family Sharing group:

1. Go to Settings  > [your name] > Family Sharing.
2. Tap your name, then tap Stop Using Family Sharing.


### Leave a Family Sharing group on your Mac

If you're over the age of 13 and are a member of a family sharing group:

1. Do one of the following:
  - On your Mac with macOS 13 or later: Choose Apple menu  > System Settings, then click Family in the sidebar (below your name).
  - On your Mac with macOS 12 or earlier: Choose Apple menu  > System Preferences, click Family Sharing , then click Family Sharing.
2. In the list of family members, click your name or Details next to your name, click Stop Using Family Sharing, then follow the onscreen instructions.
3. Click Done.


### Stop Family Sharing on your iPhone or iPad with iOS 18, iPadOS 18, or later

You must be the family organizer to turn off Family Sharing.

1. Go to Settings  > Family (below your name).
2. Tap your name, then tap Stop Using Family Sharing.





## Stop Family Sharing on your iPhone or iPad with iOS 17, iPadOS 17, or earlier

You must be the family organizer to turn off Family Sharing.

1. Go to Settings  > [your name] > Family Sharing.
2. Tap your name, then tap Stop Using Family Sharing.


## Stop Family Sharing on your Mac

To stop Family Sharing, you must:

- Be the family organizer.
  - Transfer child accounts to another family.
1. Do one of the following:
    - On your Mac with macOS 13 or later: Choose Apple menu  > System Settings, then click Family in the sidebar (below your name).
    - On your Mac with macOS 12 or earlier: Choose Apple menu  > System Preferences, click Family Sharing , then click Family Sharing.
  2. Click  next to your name, then click Stop Family Sharing.

## Remove members from a family group on your iPhone or iPad with iOS 18, iPadOS 18, or later


If you're the family organizer:

1. Go to Settings  > Family (below your name).
2. Tap [member's name], tap Remove [member's name] from Family, then tap Remove [member's name] again.

*Note:* If you're the family organizer, you can't remove yourself from the Family Sharing group.

## Remove members from a family group on your iPhone or iPad with iOS 17, iPadOS 17, or earlier





If you're the family organizer:

1. Go to Settings  > [your name] > Family Sharing.
2. Tap [member's name], then tap Remove [member's name] from Family.

*Note:* If you're the family organizer, you can't remove yourself from the Family Sharing group.

## Remove members from a family group on your Mac

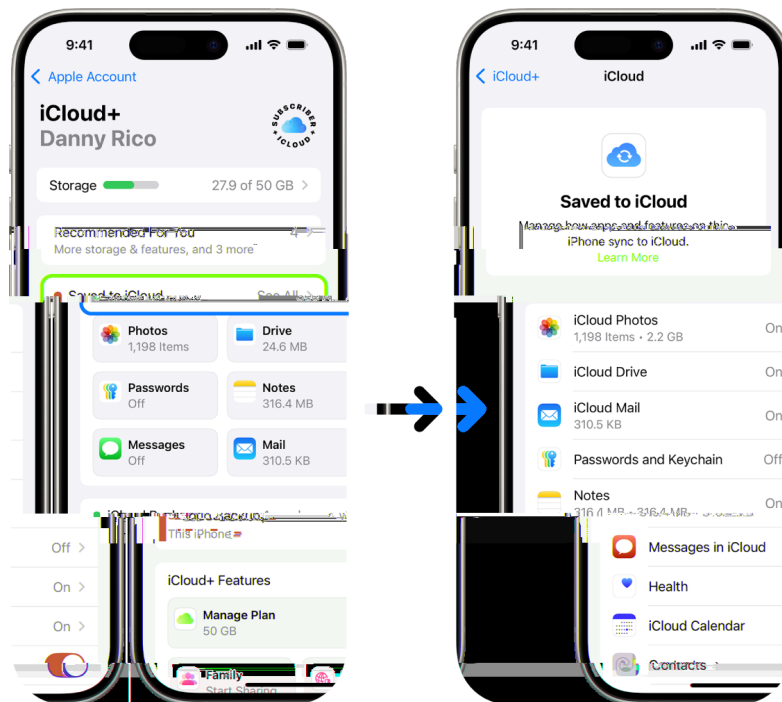
If you're the family organizer, you can remove members from a family group but you can't remove yourself.

1. Do one of the following:
  - On your Mac with macOS 13 or later: Choose Apple menu  > System Settings, then click Family in the sidebar (below your name).
  - On your Mac with macOS 12 or earlier: Choose Apple menu  > System Preferences, click Family Sharing , then click Family Sharing.
2. Do one of the following:
  - On your Mac with macOS 13 or later: Select the member in the list, click Remove [member's name] from Family, then click Remove [member's name] again.
  - On your Mac with macOS 12 or earlier: Select the member in the list, click , then click to confirm you want to remove them.

## Store your data securely in iCloud

iCloud securely stores your photos, videos, documents, music, apps, device backups, and more—and keeps them updated across all your devices. iCloud also allows you to share photos, calendars, location, and more with friends and family. You can sign in to iCloud on your device or through the web with your Apple Account.

See the [iCloud User Guide](https://support.apple.com/guide/icloud/) for more detailed information about what's stored in iCloud (<https://support.apple.com/guide/icloud/>).



### iCloud security options

Apple offers users two options to encrypt and protect the data stored in iCloud:

- *Standard data protection (the default setting):* Your iCloud data is encrypted, the encryption keys are secured in Apple data centers, and Apple can assist you with data and account recovery. Only certain iCloud data—14 data categories, including Health data and passwords in iCloud Keychain—is end-to-end encrypted.
- *Advanced Data Protection for iCloud:* An optional setting that offers you Apple's highest level of cloud data security. If you choose to turn on Advanced Data Protection, your trusted devices retain sole access to the encryption keys for the majority of your iCloud data, protecting it using end-to-end encryption. And with the Advanced Data Protection, the number of data categories that use end-to-end encryption rises to 23 and includes your iCloud Backup, Photos, Notes, and more.


For more information, see the Apple Support articles "[How to turn on Advanced Data Protection for iCloud](https://support.apple.com/108756)" (<https://support.apple.com/108756>) and "[iCloud data security overview](https://support.apple.com/102651)," the table on Data categories and encryption (<https://support.apple.com/102651>).

## View and change iCloud settings

You can view and change your iCloud settings on each device, including which apps (Apple and third-party) use iCloud, iCloud backups, and more:



- *On your iPhone or iPad:* Go to Settings  > [your name] > iCloud.

Disabling this feature means you can't use it if your device is lost or stolen and powered down.

- *On your Mac:* Choose Apple menu  > System Settings, click your name at the top of the sidebar, then click iCloud.

## Sign out of iCloud

You can also sign out of iCloud completely on a device. If you sign out of iCloud, it no longer backs up the information on that device.

- *On your iPhone or iPad:* Go to Settings  > [your name], scroll down, then tap Sign Out.
- *On your Mac:* Choose Apple menu  > System Settings, click your name at the top of the sidebar, scroll down, then click Sign Out.

## Manage safety settings in Messages

In the Messages app , you can send text messages in two different ways:

- Over Wi-Fi or cellular service, using iMessage with others who also use iMessage on an iPhone, iPad, or Mac. Your iMessage texts appear in blue bubbles.
- With SMS/MMS messages forwarded from your iPhone to other devices. Your SMS/MMS messages appear in green bubbles.



You can use iMessage to send messages, photos, or videos to another iPhone, iPad, or Mac over Wi-Fi or cellular networks. These messages are always encrypted and appear in blue text bubbles on your iPhone, iPad, and Mac.



### Limit Messages to one device


If you want to limit Messages to one device, you must sign the account out of Messages on the devices you no longer want to receive messages on, and turn off Messages in iCloud.

Do one of the following:

- *On your iPhone or iPad:* Go to Settings  > Messages, then turn iMessage on or off.
- *On your Mac:* Open Messages , choose Messages > Settings, click iMessage, then click "Sign out." Confirm you want to sign out, then click "Sign out" again.

### Turn off Messages in iCloud from iPhone or iPad


When you use Messages in iCloud, all the messages you send, receive, and delete are updated on all your Apple devices automatically.

1. Go to Settings  > [your name], then tap iCloud.
2. Under Apps using iCloud, tap Show All.
3. Tap Messages, then turn off Sync this [device].
4. Repeat this task on each device to remove the messages from iCloud.



## Turn off Messages in iCloud from Mac

When you use Messages in iCloud, all the messages you send, receive, and delete are updated on all your Apple devices automatically.

1. Open Messages  on your Mac, choose Messages > Settings, then click iMessage.
2. Click Settings, then deselect Enable Messages in iCloud.
3. Choose one of the following:
  - *Disable All*: Turns off Messages in iCloud on all your devices. Messages are no longer stored in iCloud and are instead stored on each device.
  - *Disable This Device*: Turns off Messages in iCloud on your Mac only. Messages on your Mac are no longer stored in iCloud; on any other device where Messages in iCloud is turned on, messages continue to be stored in iCloud.

## Turn iMessage on and off

iMessage uses end-to-end encryption, protecting your messages across all of your devices so they can't be accessed without your passcode by anyone, including Apple. Because iMessage conversations take place over Wi-Fi and cellular networks, information related to the person you message doesn't appear on your phone bill. iMessages can be backed up, so that if your device is lost or stolen, you can still reproduce important message threads.

**Important:** For Messages to be saved to iCloud, you must have enabled backup. If you haven't, your messages won't be restored. See "[Set up iCloud for Messages on all your devices](https://support.apple.com/guide/icloud/mm0de0d4528d)" in the iCloud User Guide (<https://support.apple.com/guide/icloud/mm0de0d4528d>).



## When iMessage is on

You can send an iMessage using a Wi-Fi connection when you don't have access to cellular service. The Recently Deleted feature saves deleted messages for up to 30 days, so if you're concerned someone may have deleted messages from your device, those messages may still be in this tab.

## When iMessage is off

When iMessage is turned off, features like message editing, message unsend, and read receipts aren't available. Messages are sent using SMS/MMS instead.

**Important:** When using SMS/MMS, records of these messages may appear in your phone bill and those message records may be released through the cellular provider to the account owner for that phone number.




- *On your iPhone or iPad:* Go to Settings  > Messages, then turn iMessage on or off.
- *On your Mac:* Open Messages , choose Messages > Settings, click iMessage, then click "Sign out." Confirm you want to sign out, then click Sign out again.

## Turn read receipts on and off

iMessage read receipts let iMessage users know when their messages have been read. With read receipts on, the person who sent you the iMessage gets a Read indicator below the message after you've read it. With read receipts off, they see only that the message has been delivered.

You have the option to send read receipts for all conversations, or only for individual ones. If you've turned on read receipts for all conversations, you can still turn them off for individual ones—and vice versa.

*Note:* Read receipts aren't supported with SMS messaging and with group texts.



- *On your iPhone or iPad:* Go to Settings  > Messages, then turn Read Receipts on or off.
- *On your Mac with macOS 13 or later:* Open Messages , go to Messages > Settings, click the iMessage tab, then select or deselect Send Read Receipts.
- *On your Mac with macOS 12 or earlier:* Open Messages , go to Messages > Preferences, click the iMessage tab, then select or deselect Send Read Receipts.

## Edit a sent message

In iOS 16, iPadOS 16.1, and macOS 13, or later, you can edit a recently sent message up to five times within 15 minutes of sending it. This allows you the opportunity to fix a typo. Recipients see that a message was edited and are able to view the edit history.

*Note:* SMS messages can't be edited.


If your recipients have Apple devices with earlier versions of iOS, iPadOS or macOS, they receive follow-up messages with the preface "Edited to" and your new message in quotation marks.

- *On your iPhone or iPad:* Tap Messages , touch and hold the message bubble, tap Edit, then edit the message and send it again.
- *On your Mac:* Open Messages , Control-click the message bubble, select Edit, then edit the message and send it again.


## Unsend a message

In iOS 16, iPadOS 16.1, macOS 13, or later, you can unsend a recently sent message for up to 2 minutes after sending it. This allows you the opportunity to pull back a message that was accidentally sent to the wrong person. Recipients see that a message was unsent.

*Note:* SMS messages can't be unsent.

- *On your iPhone or iPad:* Tap Messages , touch and hold the message bubble, then tap Undo Send.

A note confirming that you unsent the message appears in both conversation transcripts—yours and your recipient's.

- *On your Mac:* Open Messages , Control-click the message bubble, then select Undo Send.

A note confirming that you unsent the message appears in both conversation transcripts—yours and your recipient's.

## Avoid fraudulent requests to share info

Use caution if you receive unsolicited messages prompting you to accept gifts, download documents, install software, or follow suspicious links. People who want to access your personal information use any means they can—spoofed emails and texts, misleading pop-up ads, fake downloads, calendar spam, even phony phone calls—to trick you into sharing information, such as your Apple Account or password, or to get you to provide a verification code for two-factor authentication.

For tips on how to avoid being tricked into compromising your accounts or personal information, see the Apple Support article “[Recognize and avoid phishing messages, phony support calls, and other scams](https://support.apple.com/102568)” (<https://support.apple.com/102568>).

*Note:* Phishing refers to fraudulent attempts to get personal information from you.

## Block calls and messages from certain people

If you’re receiving calls, FaceTime calls, messages, or emails from someone you don’t want to hear from, you can block them from contacting you in the future. If you block someone on one device, they’re blocked on all Apple devices signed in with the same Apple Account.


⚠ **IMPORTANT:** The person you block doesn’t receive a notification that they’ve been blocked, and you can still call, message, or email a blocked contact without unblocking them. However, if you were sharing your location with them, they *do* receive a notification that you’ve stopped sharing your location after you block them.

Blocking a contact in Phone, FaceTime, Messages, or Mail blocks them across all four apps.



## Block voice calls, FaceTime calls, Messages, and Mail from certain people





- *Phone app on your iPhone:* In the Phone app, tap Favorites, Recents, or Voicemail, tap ⓘ next to the name, phone number, or email address of the contact you want to block, scroll down, tap Block this Caller, then tap Block Contact.
- *FaceTime app on your iPhone or iPad:* In your FaceTime call history, tap ⓘ next to the name, phone number, or email address of the contact you want to block, scroll down, tap Block this Caller, then tap Block Contact.
- *FaceTime app on your Mac:* In your FaceTime call history, Control-click the name, phone number, or email address of the contact you want to block, then select Block this Caller.
- *Messages app on your iPhone or iPad:* In the Messages app, tap a conversation, tap the name or number at the top of the conversation, tap ⓘ, scroll down, then tap Block this Caller.
- *Messages app on your Mac:* In your Messages history, select the name, phone number, or email address of the person you want to block. From the Conversation menu, choose Block Person, then click Block.
- *Mail app on your iPhone or iPad:* In the Mail app, select an email message from the sender, tap their name at the top of the email, select Block this Contact, then tap Block this Contact.
- *Mail app on your Mac:* In the Mail app, select an email message from the sender, click the arrow next to their name at the top of the email, then from the pop-up menu choose Block this Contact.

The Blocked icon  appears next to the sender's name in the message list and a banner is added to their messages to indicate they're blocked. The banner also provides a link to the Blocked pane of Mail settings, where you can manage blocked senders.

*Note:* If the sender has previously been marked as a VIP in mail, you must first tap Remove from VIP before you can block them.

## Manage your blocked contacts

You can manage your blocked contacts through any of the four apps that allow blocking—Phone, FaceTime, Messages, and Mail. Unblocking in one app unblocks across all four apps. Do any of the following to see the list of numbers you have blocked:

- *iPhone:* Go to Settings  > Phone, then tap Blocked Contacts.
- *FaceTime on your iPhone or iPad:* Go to Settings  > FaceTime, then under Calls, tap Blocked Contacts.
- *FaceTime on your Mac:* Open FaceTime, go to FaceTime > Settings (or FaceTime > Preferences) in the menu bar, then click Blocked.
- *Messages app on your iPhone or iPad:* Go to Settings  > Messages, then under SMS/MMS, tap Blocked Contacts.
- *Messages app on your Mac:* Open Messages, go to Messages > Settings (or Messages > Preferences), click iMessage, then click Blocked.
- *Mail app on your iPhone or iPad:* Go to Settings > Mail, then under Threading, tap Blocked.
- *Mail app on your Mac:* Open Mail, go to Mail > Settings  (or Mail > Preferences), click Junk Mail, then click Blocked.

# Secure NameDrop

## What is NameDrop?

NameDrop (part of AirDrop) allows iPhone and Apple Watch users to easily share their contact information by simply bringing their devices together. You can choose the specific contact details that you want—or don't want—to share.

NameDrop works automatically. If you need to turn NameDrop off, see [Turn Off NameDrop](#) later in this guide.


*Note:* NameDrop requires iOS 17.1, watchOS 10.1, or later on both devices; NameDrop is supported on Apple Watch SE 2nd generation, Apple Watch Series 7 and later, and Apple Watch Ultra models.



## Review and update your Contact Card

You can update the information that you share in NameDrop by updating your Contact Card—for example, if you only want to share your first name or your initials.

*Note:* NameDrop shares only your name, the phone number or email address you choose, and Contact Poster information associated with your Contact Card. It doesn't share other information in your Contact Card, like your home address or birthday. When you share your contact information through Contacts or NameDrop, by default your pronouns aren't shared. When you're sharing another contact's information, their pronouns are never shared.


1. Open the Contacts app .
2. Tap My Card > Edit.
3. Review and update your name, phone numbers, and email addresses that you want to share through NameDrop.


To learn more, see:

- [Add or edit your contact info and photo on iPhone](https://support.apple.com/guide/iphone/iph18b749db1) in the iPhone User Guide (https://support.apple.com/guide/iphone/iph18b749db1)
- [Add or edit your contact info and photo on iPad](https://support.apple.com/guide/ipad/ipadfcfa2d42) in the iPad User Guide (https://support.apple.com/guide/ipad/ipadfcfa2d42)

## Share your contact info

You can share your contact info with another person.

1. Do one of the following:
  - *Share from iPhone or iPad:* Hold your iPhone a few centimeters above the other person's iPhone or Apple Watch.
  - *Share from Apple Watch to Apple Watch:* Open the Contacts app  on your Apple Watch, tap your picture in the top-right corner, tap Share, then bring your watch to the other person's Apple Watch.
  - A glow emerges from both devices, and Apple Watch vibrates to indicate that a connection is being made.
2. Continue holding your devices near each other until NameDrop appears on both screens.
3. Choose to share your contact card (or a specific phone number or email address) and receive the other person's, or choose to receive only the other person's.


If you're sharing your contact card, tap , select the fields you want to include, then tap Save. The same fields are selected by default next the time you use NameDrop.

To cancel, move the two devices away from each other or lock your iPhone before the NameDrop transfer is complete.

To learn more, see:

- [Use NameDrop to share your contact information with new people](https://support.apple.com/guide/watch/apd8ebed6c09#apdd22da5d51) in the Apple Watch User Guide  
(<https://support.apple.com/guide/watch/apd8ebed6c09#apdd22da5d51>)

## Turn Off NameDrop

1. Open the Settings app .
2. Tap General > AirDrop.
3. Turn off Bringing Devices Together.

## Manage Photos sharing settings on Apple devices

With Shared Albums in Photos, you choose the photos and videos you want to share and the people you want to share them with. You can also change your sharing settings at any time. If you stop sharing a photo or an album with someone, their access to the shared album and its contents is removed.

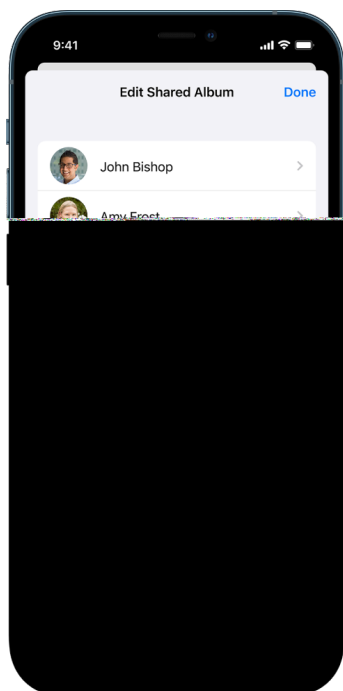
If you're a subscriber to a shared album, you can delete any photos that you shared. You can also select Unsubscribe to unsubscribe from the shared album.



To control whom you share content with from a Mac, see [“Manage Shared with You settings”](#) later in this guide.



## Manage sharing settings for Shared Albums in Photos on iPhone or iPad



1. Select a shared album on your iPhone or iPad, then tap Invite People.
2. Do any of the following:
  - *To invite new subscribers:* Tap Invite People, then enter the names of the subscribers you want to add.  
Subscribers can add photos and videos to the album. Turn off the Subscribers Can Post button so only you can add photos and videos.
  - *To remove subscribers:* Tap the name of the subscriber, then tap Remove Subscriber.
  - *To remove yourself from a Shared Album:* Do one of the following:
    - Tap the ellipsis in the top-right corner, then tap Unsubscribe.
    - Tap the iCloud account icon in the top-right corner, then tap Unsubscribe.
  - *To turn notifications off:* Slide to turn off Notifications.

To learn more, see:

- "[Share photos and videos on iPhone](https://support.apple.com/guide/iphone/iphf28f17237)" in the iPhone User Guide (https://support.apple.com/guide/iphone/iphf28f17237)
- "[Share photos and videos on iPad](https://support.apple.com/guide/ipad/ipad4f44c78f)" in the iPad User Guide (https://support.apple.com/guide/ipad/ipad4f44c78f)


## Manage iCloud Shared Photo Library settings on iPhone or iPad

iCloud Shared Photo Library lets you share photos and videos seamlessly with up to five other people. When you contribute photos and videos to iCloud Shared Photo Library, they move out of your Personal Library and into the Shared Library. With Shared Library you can choose what to share, or automatically share content straight from the camera. All participants have equal permissions to add, edit, and delete content in the Shared Library, while the person who set up the Shared Library, the library creator, provides iCloud storage for all of the content.

Participants can choose to leave a Shared Library at any time.

If you're the library creator, you can remove participants from the Shared Library or delete your shared library at any time. When you remove a participant from your Shared Library, they receive a notification and can copy all of the items in the Shared Library to their Personal Library. A participant can't remove other participants.

*Note:* Shared Libraries in Photos require iOS 16 or iPadOS 16.1 or later. To find the software version installed on your device, go to Settings > General, then tap About.

- Go to Settings  > Photos > Shared Library, then do any of the following:
  - *To remove participants from a Shared Library:* Tap Delete Participants.
  - *To leave a Shared Library:* Tap Leave Shared Library.

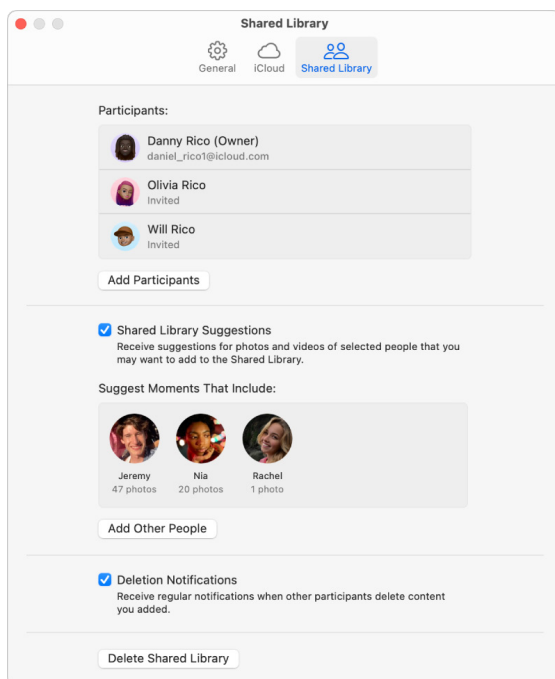
When you leave a Shared Library, you can copy everything from the Shared Library into your own library, or just the content you contributed.



- *To delete a Shared Library (you must be the organizer):* Tap Delete Shared Library. All participants are notified that the Shared Library has been deleted.

To learn more, see:

- ["Set up or join an iCloud Shared Photo Library in Photos"](https://support.apple.com/guide/iphone/iph28ac9ea81) in the iPhone User Guide (https://support.apple.com/guide/iphone/iph28ac9ea81)
- ["Set up or join an iCloud Shared Photo Library in Photos"](https://support.apple.com/guide/ipad/ipad94c5ed43) in the iPad User Guide (https://support.apple.com/guide/ipad/ipad94c5ed43)

## Manage sharing settings for Shared Albums in Photos on Mac




1. Open the Photos app  on your Mac, then click a shared album under Shared Albums in the sidebar.
2. Click  in the toolbar.
3. In the Invite People field, do one of the following:
  - *Invite new subscribers:* Enter an email address.  
If the person you're inviting doesn't use iCloud, you can select the Public Website checkbox to create a URL for your shared album. Anyone with this URL can view and download the shared album's contents.
  - *Remove subscribers:* Select the subscriber's email address, then press Delete.
  - *Reinvite a subscriber:* Click the down arrow beside the subscriber's name and choose Resend Invitation.



To learn more, see:

- ["What are shared albums in Photos on Mac?"](https://support.apple.com/guide/photos/pht7a4c765b) in the Photos User Guide (https://support.apple.com/guide/photos/pht7a4c765b)
- ["Subscribe to shared albums in Photos on Mac"](https://support.apple.com/guide/photos/pht884a8908) in the Photos User Guide (https://support.apple.com/guide/photos/pht884a8908)

## Remove participants from an iCloud Shared Photo Library on Mac

*Note:* Shared Libraries in Photos on Mac requires macOS 13 or later. To find the software version installed on your device, from the Apple menu  in the upper-left corner of your screen, choose About This Mac.

If a participant has been part of the Shared Library for less than 7 days, they can retrieve only the items they contributed.

1. In the Photos app  on your Mac, choose Photos > Settings, then click Shared Library.
2. Click  next to the person you want to remove, then choose Remove.
3. Click Remove from Shared Library.


To learn more, see:


- ["What is iCloud Shared Photo Library in Photos on Mac?"](https://support.apple.com/guide/photos/pht153ab3a01) in the Photos User Guide <https://support.apple.com/guide/photos/pht153ab3a01>

## Leave or delete an iCloud Shared Photos Library in Photos on Mac

Participants can choose to leave a Shared Library at any time. If you're the organizer of a Shared Library, you can delete it. When you delete the Shared Library, all participants receive a notification and can choose to keep all of the items in the Shared Library in their Personal Library.

If you leave a Shared Library less than 7 days after joining, you can keep only the items you contributed.

*Note:* Shared Libraries in Photos on Mac requires macOS 13 or later. To find the software version installed on your device, from the Apple menu  in the upper-left corner of your screen, choose About This Mac.

1. In the Photos app  on your Mac, choose Photos > Settings, then click Shared Library.
2. Click Leave Shared Library (if you're a participant) or Delete Shared Library (if you're the organizer).
3. Select one of the following options:
  - *Keep everything:* Add all the photos in the Shared Library to your Personal Library.
  - *Keep only what I contributed:* Add only photos that you contributed to the Shared Library to your Personal Library.
4. Click Delete Shared Library, then click Delete Shared Library again to confirm the deletion.

To learn more, see:

- ["What is iCloud Shared Photo Library in Photos on Mac?"](https://support.apple.com/guide/photos/pht153ab3a01) in the Photos User Guide <https://support.apple.com/guide/photos/pht153ab3a01>
- ["Leave or delete a Shared Library"](https://support.apple.com/guide/photos/pht4dd77b3aa#pht82b300b22) in the Photos User Guide (<https://support.apple.com/guide/photos/pht4dd77b3aa#pht82b300b22>)

## Manage shared Tab Groups in Safari



You can share a Tab Group and collaborate with people who use iCloud. A shared tab group can have a total of 100 participants. Participants can add and remove tabs from the Tab Group, and everyone sees updates in real time.

Everyone you collaborate with must be signed in to their Apple Account, have Safari turned on in iCloud settings (<https://support.apple.com/guide/iphone/iphde0f868fd>), and have two-factor authentication turned on.



### Manage shared Tab Groups in Safari on iPhone or iPad

If you don't see the Collaborate button, you don't have any shared Tab Groups.



1. Tap Safari , then tap  at the top-right corner.
2. Tap Manage Shared Tab Group, then do any of the following:
  - *Remove someone*: Tap a name, then tap Remove Access.
  - *Stop sharing with everyone*: Tap Stop Sharing.
  - *Add someone*: Tap Share With More People, then invite them.

To learn more, see:

- ["Add and remove people from a shared Tab Group"](https://support.apple.com/guide/iphone/iph4a323d663#iph5f23c7659) in the iPhone User Guide (<https://support.apple.com/guide/iphone/iph4a323d663#iph5f23c7659>)
- ["Add and remove people from a shared Tab Group"](https://support.apple.com/guide/ipad/ipad76b9549e#iPad252604e8) in the iPad User Guide (<https://support.apple.com/guide/ipad/ipad76b9549e#iPad252604e8>)

## Manage shared Tab Groups in Safari on Mac

If you don't see the Collaborate button, you don't have any shared Tab Groups.

1. In the Safari app  on your Mac, click  in the toolbar.
2. Click Manage Shared Tab Group, then do any of the following:
  - *Remove someone*: Click a name, click Remove Access, then click Continue.
  - *Stop Sharing with everyone*: Click Stop Sharing, then click Continue.
  - *Add someone*: Click Share With More People, then click Messages to invite them.

To learn more, see:

- ["Add and remove people from a shared Tab Group"](https://support.apple.com/guide/iphone/iph4a323d663#iph5f23c7659) in the Safari User Guide (<https://support.apple.com/guide/iphone/iph4a323d663#iph5f23c7659>)

## Keep your browsing history private in Safari and Maps

Reviewing and clearing search history and caches for browsers and other apps may be a good practice if you're concerned someone has access to your device. Many apps store information about what you've searched for and what you've looked at so that it's easy for you to rediscover it in the future. For example, when you use the Maps app, having a history of locations you've searched for or navigated to can make it easier to navigate back to a place you recently visited.



If you're in an unsafe personal situation and need to look up safety strategies online but don't want Safari to keep a record of what you've viewed, you can open a Private Browsing window on [iPhone](#), [iPad](#), and [Mac](#). When you use Private Browsing, the details of your browsing aren't saved, and they aren't shared across your devices. Additionally, if you've updated your devices to iOS 17, iPadOS 17, macOS 14, or later, Safari locks Private Browsing tabs after a period of inactivity so that they can be opened only with your password, passcode, Face ID or Touch ID, protecting your privacy when you're away from your device. You can clear your browsing history and open a Private Browsing window on iPhone, iPad, and Mac.

See how to open a Privacy window on an iPhone, iPad, or Mac later in this guide.



## Clear your browsing history in Safari



If you've been looking up information about safety strategies online and are concerned someone may see your browsing history, you can remove all records that Safari keeps about where you've browsed.

- *On your iPhone or iPad:* Go to Settings  > Safari > Clear History and Website Data.
- *On your Mac:* Open the Safari app , choose History > Clear History, click the pop-up menu, then choose how far back you want your browsing history cleared.

When you clear your history, Safari removes data it saves as a result of your browsing, including:


- A history of the webpages you visited
- The back and forward list for open webpages
- A list of frequently visited sites
- Recent searches
- Icons for webpages
- Snapshots saved for open webpages
- A list of items you downloaded (downloaded files aren't removed)
- Websites you added for a Quick Website Search
- Websites that asked to use your location
- Websites that asked to send you notifications

## Clear recent directions and favorites in Maps on iPhone or iPad




1. Open the Maps app , then scroll down in the search field to Recents.
2. Do one of the following:
  - Swipe a recent route left.
  - Tap More directly above the list, then swipe a recent route left; or to delete a group of routes, tap Clear above the group.
3. If you want to remove a Favorite location, scroll to Favorites, then tap More. Swipe from right to left on the Favorite location you want to delete, or tap Edit and tap  to remove multiple Favorites.





### **Clear recent directions and favorites in Maps on Mac**

1. Open the Maps app , then scroll to Recents in the sidebar.
2. Below Recents, click Clear Recents.
3. If you want to remove a Favorite location, Control-click a location (in the sidebar below Favorites), then choose Remove from Favorites.

### **Open a Private Browsing window on iPhone**

1. Open the Safari app , then tap .
2. Tap  in the bottom center of the Tab bar at the bottom of the screen, then tap Private.  
The tab is automatically added to a Tab Group called Private. You can open multiple private tabs in the group.

You can easily confirm that you're in Private Browsing Mode by checking that the search field bar is gray or that it displays the word Private.


To hide the sites and exit Private Browsing Mode, tap , then tap  to open a different Tab Group from the menu at the bottom of your screen. The private sites reappear the next time you use Private Browsing Mode.

To close private tabs, tap , then swipe left each of the tabs you want to close.


### **Open a Private Browsing window on iPad**

- In the Safari app, tap , then tap Private.

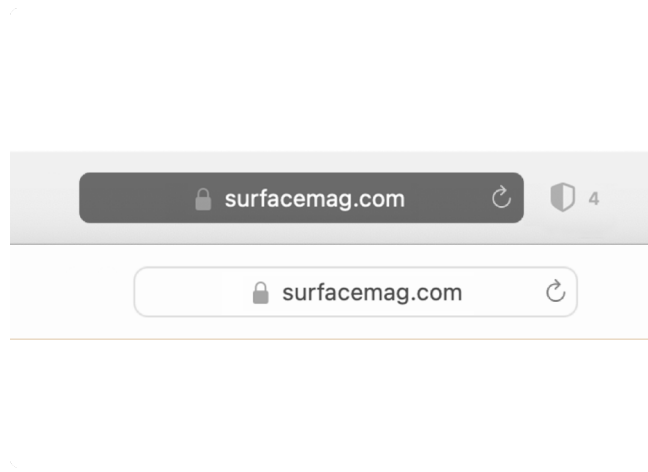
While Private Browsing Mode is on, the search field background is black instead of white and sites you visit don't appear in History on iPad or in the list of tabs on your other devices. You can open multiple private tabs in the Private Tab Group.

To hide the sites and exit Private Browsing Mode, tap , then switch to a different tab group. The tabs reappear the next time you use Private Browsing Mode.

## Open a Private Browsing window on Mac

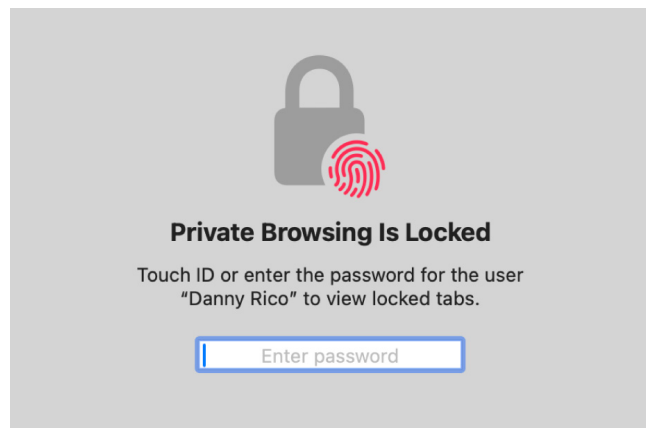
1. In the Safari app , choose File > New Private Window, or switch to a Safari window that's already using Private Browsing.

A window using Private Browsing has a dark Smart Search field with white text.




2. Browse as you normally would.





*Note:* When your device is locked or asleep, or if you aren't actively using Safari, your private windows in Safari will lock. When you unlock or wake up your device, or start using Safari again, just unlock your private window with Face ID, Touch ID, or your device passcode or password.



### **If you want to always open windows with Private Browsing on Mac**

1. In the Safari app , choose Safari > Preferences, then click General.
2. Click the "Safari opens with" pop-up menu, then choose "A new private window."

If you don't see this option, do one of the following:

- On your Mac with macOS 13 or later: Choose Apple menu  > System Settings, click Desktop & Dock  in the sidebar, then make sure "Close windows when quitting an app" is selected.
- On your Mac with macOS 12 or earlier: Choose Apple menu  > System Preferences, click General , then make sure "Close windows when quitting an app" is selected.

### **To further enhance Safari privacy**

- In your Downloads folder, delete any items that were downloaded while you were using Private Browsing windows.
- Close any other Private Browsing windows that are still open, to prevent other people from using the Back and Forward buttons to see pages you visited.


## Manage Shared with You settings on Apple devices

When someone shares content with you from the Music, Apple TV, News, Photos, Podcasts, and Safari apps, Shared with You can automatically organize it into a Shared with You section for easy access. Content that's shared with you in the Messages app is automatically organized in a Shared with You section in the Music, Apple TV, News, Photos, Podcasts, and Safari apps.



### Manage by person on iPhone or iPad

If there's content shared with you through Messages that you don't want to appear in associated apps, you can turn off this feature by person.



1. Tap Messages  on your iPhone or iPad, then tap the conversation whose content you don't want to share across apps.
2. When the thread opens, tap the person's name at the top.
3. Turn off Show in Shared with You, then tap Done.

To learn more, see:

- ["Use Messages to receive and share content with friends"](https://support.apple.com/guide/iphone/iphb66cfeaad) in the iPhone User Guide (https://support.apple.com/guide/iphone/iphb66cfeaad)
- ["Use Messages to receive and share content with friends"](https://support.apple.com/guide/ipad/ipad5bf3d77b) in the iPad User Guide (https://support.apple.com/guide/ipad/ipad5bf3d77b)

## Manage by person on Mac

If there's content shared with you through Messages that you don't want to appear in associated apps, you can turn off this feature by person.

1. Open the Messages app  on your Mac, then select the conversation.
2. Click  in the top-right corner of a conversation, then deselect Show in Shared with You to remove shared content from the Shared with You section.

When Shared with You is turned off, you can still pin shared content to show it in the corresponding app.

To learn more, see:

- ["Keep track of shared content in Messages on Mac"](https://support.apple.com/guide/messages/ichtdc9ebc32) in the Mac User Guide (<https://support.apple.com/guide/messages/ichtdc9ebc32>)


## Manage by app on iPhone or iPad

If you want to turn Shared with You on or off within the Music, Apple TV, News, Photos, Podcasts, or Safari apps, you can adjust your settings.

- On your iPhone or iPad, go to Settings  > Messages > Shared with You, then turn off Automatic Sharing or turn off Shared with You for a specific app.

## Manage by app on Mac

If you want to turn Shared with You on or off within the Music, Apple TV, News, Photos, Podcasts, or Safari apps, you can adjust your settings.

1. Open the Messages app  on your Mac.
2. Choose Messages > *Settings* or *Preferences*.
3. Click Shared with You, then do one of the following:
  - *To turn off all apps:* Click Turn Off.
  - *To turn off selected apps:* Deselect apps.


To learn more, see:

- ["Keep track of shared content in Messages on Mac"](https://support.apple.com/guide/messages/ichtdc9ebc32) in the Mac User Guide (<https://support.apple.com/guide/messages/ichtdc9ebc32>)

# Additional information

## Safety considerations

Before making changes or deleting information, keep in mind:

- You may want to record suspicious activity. See also [Obtain evidence related to another Apple Account](#).
- Changes you make to sharing or access may be noticed by others. Look for this icon throughout the guide for safety-related information you may want to consider before taking action: .
- When you change a sharing relationship, you may lose access to tools and information that could be important to you.
- Apps developed by other companies (like Youtube or Instagram) have their own individual settings that Apple cannot control. See each individual app's directions to review, manage, or check whether those apps send notifications when altered. See [Third-party app settings](#) for more information.

## Other technology safety resources

If you need more information or support regarding technology-related safety, you can visit the websites below.

### United States

- [The Safety Net Project](#) at the National Network to End Domestic Violence
- [National Center for Victims of Crime](#)

### United Kingdom

- [Refuge UK](#)

### Australia

- [WESNET Safety Net Australia](#)

## Other support resources

For other Apple related concerns, consider the resources below.

### Apple Support

General Apple-related assistance through self-help resources or to connect to an expert. Apple Support has extremely limited access to your information without your explicit permission and no access to your data and/or passwords.

- [Apple Support](https://support.apple.com) (https://support.apple.com)
- US – 1-800-275-2273; In Canada – 1-800-263-3394

### Apple Platform Security

Search [Apple Platform Security](#) for information on hardware and system security, encryption and data protection, and services security—including Apple Account, iCloud, Sign in with Apple, Apple Pay, Messages, FaceTime and Find My.

### Apple Privacy

Explore the [Apple Privacy](#) webpage for features that protect your data and settings that put you in control, review nutrition labels for apps and transparency reports for government requests, and familiarize yourself with Apple's Privacy Policies.

### Your Data and Privacy

Sign in to the [Data and Privacy web portal](#) with your Apple Account to learn more about what Apple collects, get or transfer a copy of your data, and correct, deactivate, or delete your data.

### Apple Support Community

Search the [Apple Support Community](#) for answers and ask questions from other Apple customers (globally).

© 2024 Apple Inc. All rights reserved.

Use of the “keyboard” Apple logo (Option-Shift-K) for commercial purposes without the prior written consent of Apple may constitute trademark infringement and unfair competition in violation of federal and state laws.

Apple, the Apple logo, AirDrop, AirPods, AirTag, Apple Books, Apple Music, Apple Pay, Apple TV, Apple Wallet, Apple Watch, Apple Watch SE, Apple Watch Series, Apple Watch Ultra, Digital Crown, Face ID, FaceTime, FileVault, Finder, Find My, HomeKit, HomePod, HomePod mini, iMac, iMessage, iPad, iPadOS, iPad Pro, iPhone, iTunes, Launchpad, Lightning, Mac, MacBook, MacBook Air, MacBook Pro, macOS, Magic Keyboard, Magic Mouse, Magic Trackpad, NameDrop, OS X, Safari, Siri, Time Machine, and Touch ID are trademarks of Apple Inc., registered in the U.S. and other countries and regions.

App Store, iCloud, iCloud+, iCloud Keychain, and iTunes Store are service marks of Apple Inc., registered in the U.S. and other countries and regions.

Apple  
One Apple Park Way  
Cupertino, CA 95014  
[apple.com](https://apple.com)

IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license.

The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Apple is under license.

Other company and product names and logos mentioned herein may be trademarks of their respective companies.

Every effort has been made to ensure that the information in this manual is accurate. Apple is not responsible for printing or clerical errors.

Some apps are not available in all areas. App availability is subject to change.

028-00803