Personal Safety User Guide for Apple devices



Contents

Personal safety at a glance 4

Personal safety at a glance 4

What's New 6

What's new in personal safety with Apple devices 6

Use Safety Check 8

How Safety Check works 8

Stop sharing with people and apps 13

Additional considerations when using Safety Check 19

Review and take action 21

Securely control whom you share content with from iPhone, iPad, and Apple Watch 21

Securely control whom you share content with from Mac 26

Safely manage how you forward content 30

Block unknown sign-in attempts 32

Record suspicious activity 33

Share or stop sharing your location 35

Manage automatic ETA sharing in Maps 38

Stay safe with AirTag 40

Store your data securely in iCloud 42

Control who can access your location 44

Delete suspicious content 47

Manage Family Sharing settings 51

Avoid fraudulent requests to share info 55

Securely control your Home accessories 56

How to erase all content and settings 57

Restore the data you backed up 59

Safety and privacy tools **62**

Update your Apple software 62

Set a unique passcode or password 66

Secure your iPhone or iPad with Face ID 68

Secure your devices with Touch ID 70

Delete unknown fingerprints from iPhone or iPad 71

Add or delete fingerprints on your Mac 71

Keep your Apple ID secure 72

Use two-factor authentication 75

If you get locked out of your device 77

Keep your device, app, and website passwords secure on iPhone and iPad 79

See how apps are accessing your data 81

Change your privacy settings 82

Harden your devices against mercenary spyware 83

Manage safety settings in iMessage 84

Block calls and messages 87

Keep your browsing history private 89

Make an emergency call on iPhone 93

Know how to obtain evidence related to another person’s account 97

Personal safety checklists **98**

See who has access to your iPhone or iPad 98

How to stop sharing your iPhone or iPad content 99

How to stop sharing your iPhone or iPad location 100

Copyright **101**

Personal safety at a glance

Personal safety at a glance

Apple makes it easy to connect with the people closest to you, while helping you stay aware of what you're sharing and with whom. If you gave someone access to your personal information and no longer want to—or if you're concerned someone who had access to your device or accounts made changes without your permission—this guide offers strategies and solutions to help you regain control.

This resource applies primarily to Apple devices running the latest operating systems (iOS 16, iPadOS 16.1, and macOS 13) but applies also to Apple Watch and HomePod.



In iOS 16, you can use Safety Check on iPhone to quickly view what you're sharing and whom you're sharing it with. You can then decide to stop sharing this information. If you haven't upgraded to iOS 16, Apple offers quick checklists and in-depth feature tasks designed to help you if you're experiencing technology-enabled abuse, stalking, or harassment. These tasks include step-by-step instructions on how to remove someone's access to information you previously granted—like location data in the Find My app, meetings you've shared in Calendar, and more. You'll also learn about features you can use to enhance your personal safety—like how to automatically let a friend know when you've arrived home safely and how to engage Emergency SOS.

This guide will be updated regularly to provide you with the information you need to feel safe and secure while using Apple products.

Tip: Where applicable, additional details for other products are provided or linked to, including links to user guides for Apple devices. You can download a PDF of this guide and print it for your convenience. All features, instructions, and settings can vary with the product model or software version. If you need assistance with a particular feature, search Apple Support at https://support.apple.com.

Additional safety resources

If you feel your safety is at risk, these additional resources might be helpful:

- *United States:* The Safety Net Project (https://www.techsafety.org/resources-survivors)
- *United States:* National Center for Victims of Crime (https://victimsofcrime.org/getting-help/)
- *United Kingdom:* Refuge UK (https://refuge.org.uk/i-need-help-now/how-we-can-help-you/national-domestic-abuse-helpline/)
- *Australia:* WESNET Safety Net Australia (https://techsafety.org.au/resources/resources-women/)

What's New

What's new in personal safety with Apple devices

Since the last release of this guide, the following features have been added to help users with their personal safety when using Apple devices.

Safety Check

Safety Check on iPhone can quickly stop sharing your information, or you can review and update sharing with individual people and apps. See How Safety Check works.

Manage forwarding content

You can review and manage how you forward content and whom you forward it to on an iPhone, iPad, or Mac. See Safely manage how you forward content.

ETA sharing in Maps

You can stop sharing your estimated time of arrival (ETA) with anyone in your Contacts. You can do this before you get started on your trip or during your trip. See Manage automatic ETA sharing in Maps.

Manage your passwords

On your iPhone or iPad, 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. See Keep your device, app, and website passwords secure on iPhone and iPad.

Turn on Lockdown Mode

Lockdown Mode is an extreme, optional protection for iPhone, iPad, and Mac 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. See Harden your devices against mercenary spyware.

iMessage safety settings

In iOS 16, iPadOS 16.1, and macOS 13, you can do the following using iMessage:

- Edit a recently sent message up to five times within 15 minutes of sending it.
- Unsend a recently sent message for up to 2 minutes after sending it.

See Manage safety settings in iMessage.

Clear recent information in Maps

You can clear recent directions and favorites in the Maps app. See Keep your browsing history private.

Obtain evidence related to another person's account

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. See Know how to obtain evidence related to another person's account.

Use Safety Check

How Safety Check on iPhone works to keep you safe

If your personal safety is at risk, you can use Safety Check on iPhone (running iOS 16 or later) to quickly stop sharing your information, or to review and update sharing with individual people and apps.

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).



If you need to immediately stop sharing information, see How do I use Emergency Reset in Safety Check?.

If you need to review or stop sharing information with specific people or apps, see How do I use Manage Sharing & Access in Safety Check?.

When using Safety Check, keep in mind that people may notice if you stop sharing your information with them. When you end sharing relationships, you may lose access to data such as shared photos and notes.

Safety Check is available only on iPhone and only if you have a personal Apple ID (not a Managed Apple ID) that uses two-factor authentication. You must also be signed in to Settings > [*Your Name*] on your iPhone. After you're signed in, you can go to Settings > Privacy & Security > Safety Check.



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.

What does Safety Check do?

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 ID password, and more.

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

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 functionality may not be available.

Which Apple apps stop sharing information with people using Safety Check?

Safety Check can turn off sharing information from the following Apple apps to other people:

App	Information
	Shared Calendars
	Health
	Home
	Shared Location using Find My
	Shared Notes
	Shared Photos (Including Shared Library and Shared Albums)

What information stops being shared with apps using Safety Check?

Safety Check removes from all apps on your iPhone any data gathered by the following apps, networks, and features:

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

Does Safety Check work with my Apple ID?

Safety Check can be used to modify information associated with your Apple ID. You can use Safety Check to:

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

What is Emergency Reset?

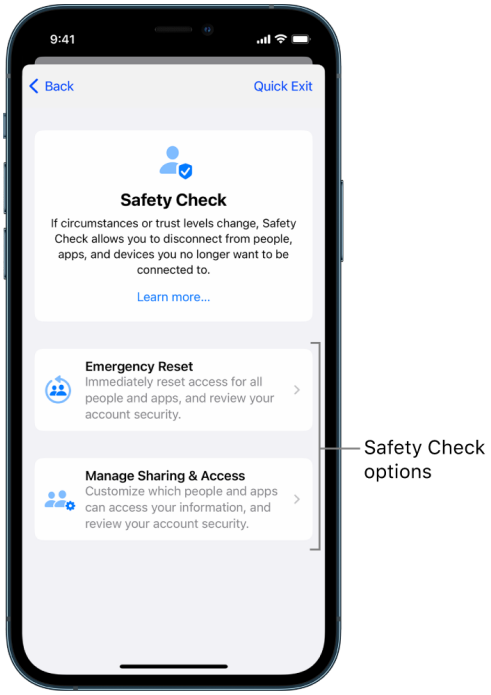
Safety Check has an option called Emergency Reset. You use it to immediately stop sharing the items listed above, which includes all types of sharing. Emergency Reset also allows you to review and reset settings associated with your Apple ID.

If you're unsure what you're sharing and whom you're sharing with, see How do I use Manage Sharing & Access.

Stop sharing with people and apps with Safety Check on iPhone

If your personal safety is at risk, you can use Safety Check on iPhone (running iOS 16 or later) to immediately stop all sharing and access, or to review and update sharing with individual people and apps. There are two ways to do this:

- Use Emergency Reset to immediately stop sharing the sharing types shown in How Safety Check works to keep you safe. Emergency Reset also allows you to review and reset settings associated with your Apple ID.
- Use Manage Sharing & Access to stop sharing information with specific people or apps. If you're not sure what you're sharing and whom you're sharing with, use this option.



When using Emergency Reset and Manage Sharing & Access, keep in mind that people may notice you've stopped sharing information with them. By ending sharing relationships, you may lose access to data such as shared photos and notes.

For more information about Safety Check, see How Safety Check works.

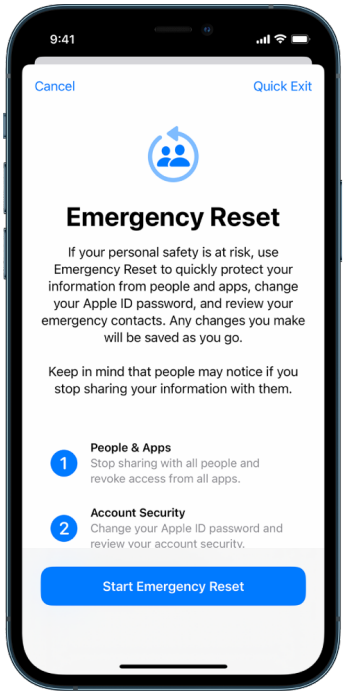
Quick Exit

A Quick Exit button is available if you need to quickly exit Safety Check. By tapping Quick Exit, Safety Check and the Settings app immediately close and return to the Home Screen. Any changes you made before using Quick Exit are saved.

How do I use Emergency Reset in Safety Check?

1. Go to Settings > Privacy & Security > Safety Check.
2. Tap Emergency Reset, then follow the onscreen instructions.

   Progress is saved as you go.



3. When you've finished, make sure you stopped all sharing and reset specific settings.

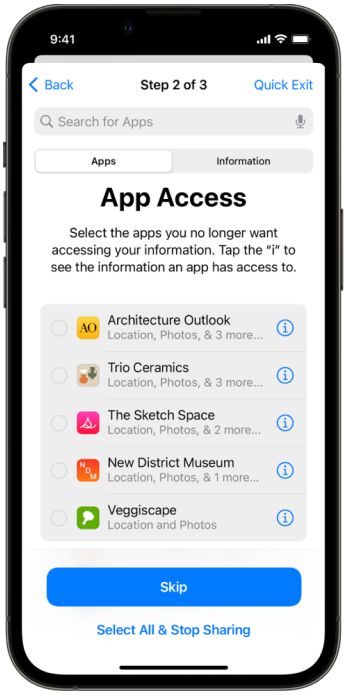
   See Verify you've stopped sharing.

How do I use Manage Sharing & Access in Safety Check?

When you want to explore sharing in more detail, use Manage Sharing & Access to review and reset information you're sharing with people, review and reset the information apps have access to, and update your device and Apple ID security.

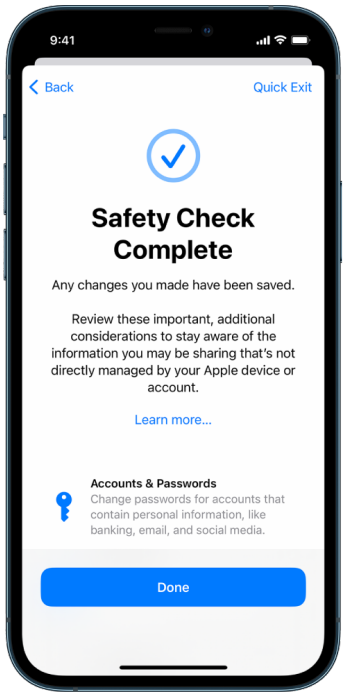
1. Go to Settings > Privacy & Security > Safety Check.
2. Tap Manage Sharing & Access.

   Progress is saved as you go.
3. Do one of the following to stop sharing information with other people:
   - 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.
4. Do one of the following to stop sharing information with other apps:
   - 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.
5. Tap Continue, then do any of the following:
   - Review and remove devices signed into your account.
   - Review and update trusted phone numbers.
   - Change your Apple ID password.
   - Update your emergency contacts.
   - Update your device passcode, or your Face ID or Touch ID information.

6. Click Done.



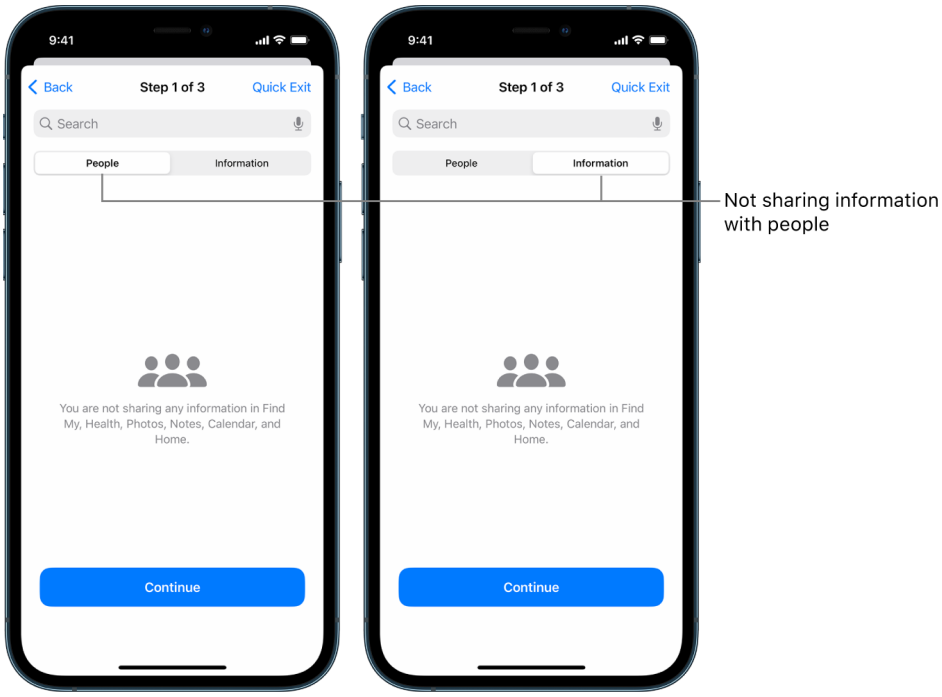
7. When you've finished, make sure you stopped certain sharing and reset specific settings. See Verify you've stopped sharing.

   Important: Review the list of "Additional considerations when using Safety Check" that isn't directly managed by your iPhone or Apple ID.

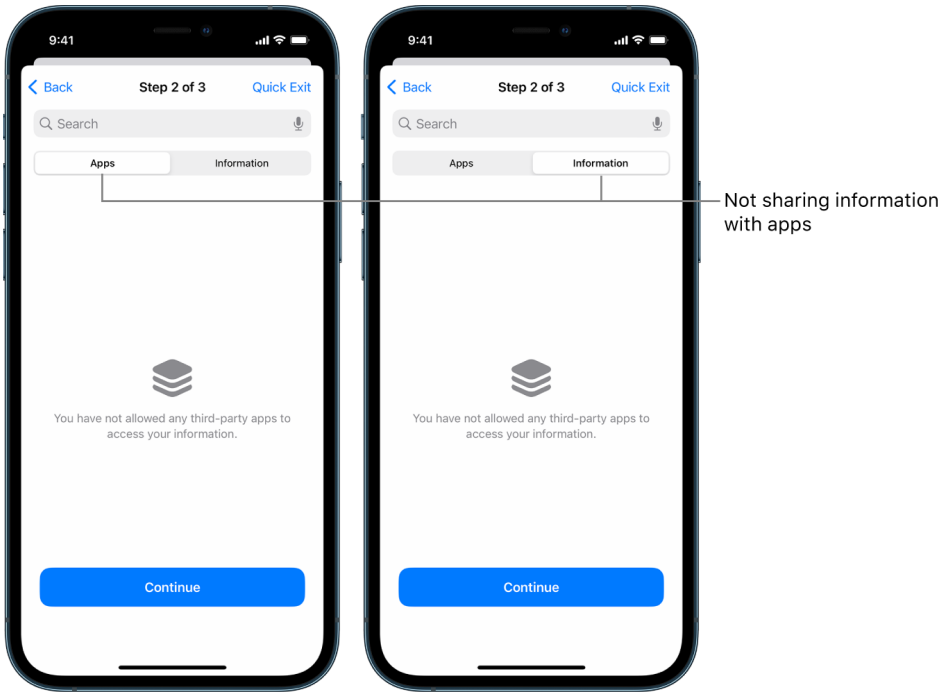
Verify you've stopped sharing

After using Safety Check, you can confirm that changes have been made. You can verify that sharing and information access has stopped. This has three steps:

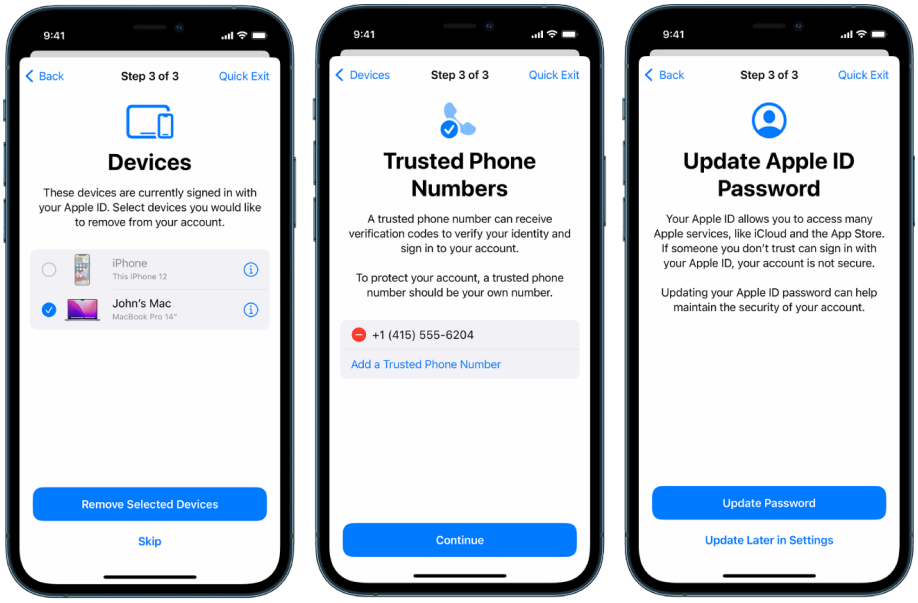
- *Step 1:* Verify that sharing has stopped for people and information shared to people has been stopped.



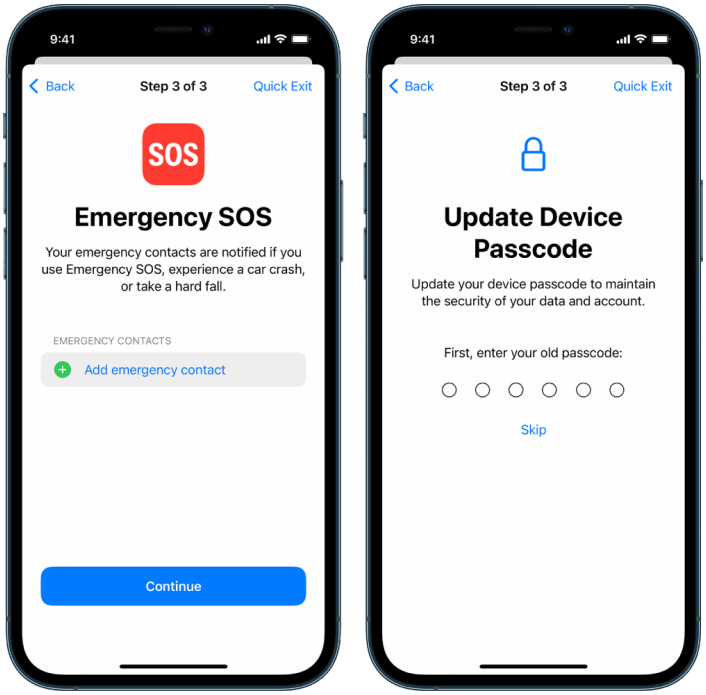
- *Step 2:* Verify that sharing has stopped for apps.



- *Step 3:* Verify that you may have changed the following:
  - Trusted devices may have been removed.
  - Trusted phone numbers may have been updated.
  - Your Apple ID password may have been updated.



  - Emergency contacts may have been added or changed.
  - The device passcode may have been updated.



Additional considerations when using Safety Check

Use Safety Check in iPhone (running iOS 16 or later) to quickly stop sharing and access to your information, or easily review and update sharing with individual people and apps.

In some cases, you may also be sharing information that Safety Check can't review or change—for example, accounts and passwords, social media sharing, or an iPad or Mac that may also have information you've shared. Carefully review the following to help you decide what additional steps you may want to take to reduce the amount of information you're sharing.

Accounts and passwords

Think about the accounts you use that may contain sensitive personal information you want to protect, like banking, shopping, email, social media, education, and others. Change the passwords for these accounts to help ensure no one else can access them. Check through each account's security and privacy settings to ensure that your information is protected. For accounts you use to communicate, like email, phone, and messaging, check to make sure nothing is being forwarded without your permission.

Social media

Remember that posting photos and other personal information on social media can reveal details about your location and personal life. Check your privacy settings, review your lists of connections and followers, and think carefully about what you post to ensure the level of privacy you need.

Other devices you own or use

Check the sharing and access settings for any other devices you use to make sure your information is secure. If anyone else is with you, like a child or friend, remember that their devices may also be sharing information.

Unwanted tracking

Unwanted tracking alerts were created to discourage people from trying to misuse AirTags and other small Find My accessories to track someone without their knowledge. To receive alerts if an unknown AirTag or other Find My network accessory is moving with you, make sure Bluetooth, Location Services, and Tracking Notifications are turned on. To turn on Tracking Notifications, open the Find My app, tap Me, scroll to Customize Tracking Notifications, then turn on Allow Notifications.

See the Apple Support article What to do if you get an alert that an AirTag, Find My network accessory, or set of AirPods is with you (https://support.apple.com/HT212227).

Home and HomeKit

If you're a member of an Apple home and decide to remove yourself, remember 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.

Apple Wallet

If you share cards or keys with someone in Wallet, the person you're sharing with may be able to view your transaction history or door lock history. To review your recent transactions, open the Wallet app. Remember that 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. Remember to update your passwords.

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 for more information 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. Remember to update your passwords.

Family Sharing

If you're a member of an Apple Family Sharing group, the Family Sharing organizer may be able to see your purchases 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.

Learn more about how to leave Family Sharing groups in steps 1 and 2 of the How to stop sharing your iPhone or iPad content checklist.

Review and take action

Securely control whom you share content with from iPhone, iPad, and Apple Watch

You can share content securely with others on your Apple devices using several different methods. With each method, you can view people you're sharing with. You can also remove them from shared content on your iPhone, iPad, iPod touch, and Apple Watch.



To control whom you share content with from a Mac, see Securely control whom you share content with from Mac.

How to manage file sharing settings for AirDrop

AirDrop is an easy way to share images, documents or other files between Apple devices that are near each other. You can set it up so that everyone near you can share, so that only your contacts can share, or so that no one can share.

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.

Manage AirDrop

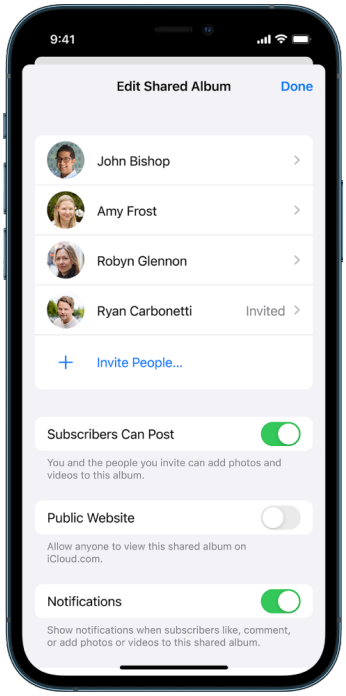
- On your iPhone, iPad, or iPod touch, go to Settings > General, tap AirDrop, then choose an option that works best for you.

To learn more, see:

- iPhone User Guide: Use AirDrop on iPhone to send items to nearby devices (https://support.apple.com/guide/iphone/iphcd8b9f0af)
- iPad User Guide: Use AirDrop on iPad to send items to nearby devices (https://support.apple.com/guide/ipad/ipadf0a1530e)

Manage sharing settings for photos and videos

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 anytime. If you stop sharing a photo or an album with someone, they won't receive a notification and 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.

1. Select a shared album on your iPhone, iPad, or iPod touch, then tap the Add Subscribers button .
2. Do any of the following:
   - *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.
   - *Remove subscribers:* Tap the name of the subscriber, then tap Remove Subscriber.
   - *Turn notifications off:* Tap the Notifications button. Tap again to turn Notifications on.

To learn more, see:

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

Manage calendar sharing settings

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.

If you're the Calendar owner and would like to stop sharing, tap the name of the subscriber for options. If you're a subscriber, select Delete Calendar to remove the shared calendar.

1. Tap Calendars on your iPhone, iPad, or iPod touch, then tap the Info button 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.

To learn more, see:

- iPhone User Guide: Share iCloud calendars on iPhone (https://support.apple.com/guide/iphone/iph7613c4fb)
- iPad User Guide: Share iCloud calendars on iPad (https://support.apple.com/guide/ipad/ipadc2a14a22)

Manage Shared with You settings by person

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. If there is 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, iPad, or iPod touch, then tap the conversation that has the content you don't want to be shared 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:

- iPhone User Guide: Use Messages to receive and share content with friends (https://support.apple.com/guide/iphone/iphb66cfeaad)
- iPad User Guide: Use Messages to receive and share content with friends (https://support.apple.com/guide/ipad/ipad5bf3d77b)

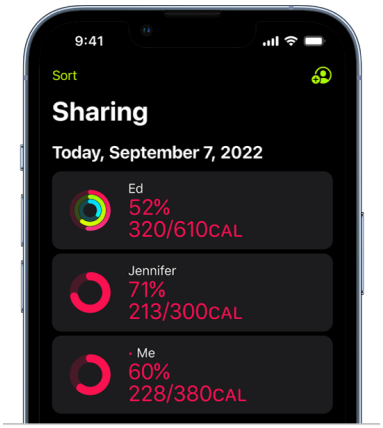
Manage Shared with You settings by app

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, iPad, or iPod touch, go to Settings > Messages > Shared with You, then turn off Automatic Sharing or turn off Shared with You for a specific app.

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.



You can hide your progress, or stop sharing your activity with a particular person entirely, from the Sharing tab in the Activity app. If you stop sharing your activity, that person isn't notified.

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:

- Apple Watch User Guide: Share your activity from Apple Watch (https://support.apple.com/guide/watch/apd68a69f5c7)

Securely control whom you share content with from Mac

You can share content securely with others on your Apple devices using any of several different methods. With each method, you can view people you're sharing with and you can also remove them from shared content on your Mac.

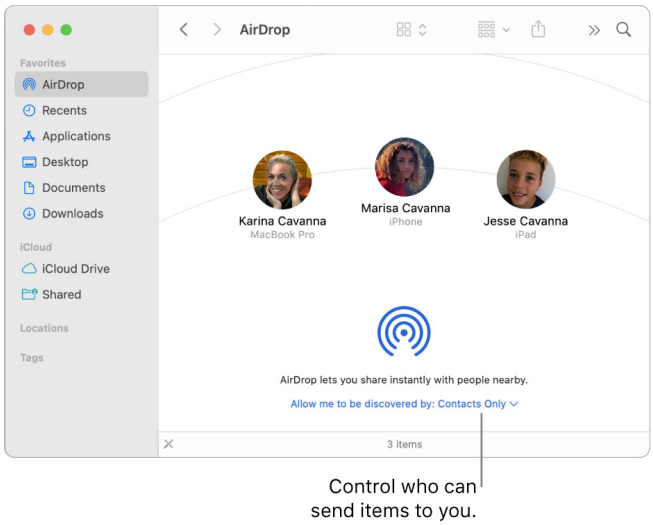


To control whom you share content with from an iPhone, iPad, iPod touch, and Apple Watch, see Securely control whom you share content with from iPhone, iPad, and Apple Watch.

How to manage file sharing settings for AirDrop

AirDrop is an easy way to share images, documents, or other files between Apple devices that are near each other. You can set it up so that everyone near you can share, so that only your contacts can share, or so that no one can share.

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 AirDrop on when you need it and then disable it when you don't.

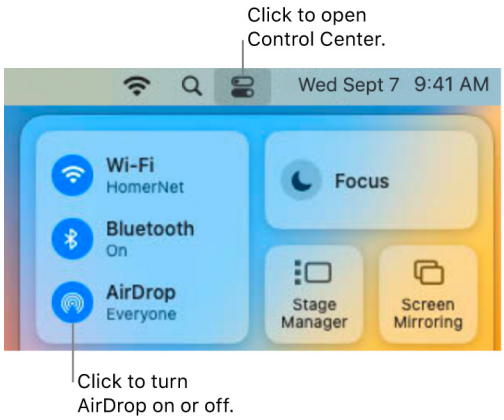


Use the Finder to manage AirDrop

1. On your Mac, 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.

Use Control Center to manage AirDrop

You can use Control Center to quickly turn AirDrop on or off and choose who can send items to you using AirDrop.



1. On your Mac, click Control Center in the menu bar.
2. Do any of the following:
   - *Turn AirDrop on or off:* Click the AirDrop icon.
   - *Choose who can send items to you:* Click the arrow button next to AirDrop, then choose an option that works best for you.

To learn more, see:

- macOS User Guide: Use AirDrop on your Mac to send files to devices near you (https://support.apple.com/guide/mac-help/mh35868)

Manage sharing settings for photos and videos

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, they won't receive a notification and 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.

1. Open the Photos app on your Mac, then click a shared album under Shared Albums in the sidebar.
2. Click the Collaborate button 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:

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

Manage calendar sharing settings

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.

If you're the Calendar owner and would like to stop sharing, tap the name of the subscriber for options. If you're a subscriber, you can select Delete Calendar to remove the shared calendar.

1. Open the Calendar app 📅 on your Mac.
2. Do one of the following:
   - If your Mac has macOS 13 or later: Choose Calendar > Settings.
   - If your Mac has macOS 12 or earlier: Choose Calendar > Preferences.
3. Click Accounts, select the calendar account, then click Delegation.

   A CalDAV account appears in the "Accounts I can access" list.

   Note: For a Microsoft Exchange account, click the Add button ＋, then enter the user name of the person who gave you access.

To learn more, see:

- Calendar User Guide: Share calendar accounts on Mac (https://support.apple.com/guide/calendar/icl27527)

Manage Shared with You settings by person

1. Open the Messages app 💬 on your Mac, then select the conversation.
2. Click the Details button ⓘ 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:

- iMessage User Guide: Keep track of shared content in Messages on Mac (https://support.apple.com/guide/messages/ichtdc9ebc32)

Manage Shared with You settings by app

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.
   - If your Mac has macOS 13 or later: Choose Messages > Settings.
   - If your Mac has macOS 12 or earlier: Choose Messages > Preferences.
2. Click Shared with You, then do one of the following:
   - *Turn off all apps:* Click Turn Off.
   - *Turn off selected apps:* Deselect apps.

Safely manage how you forward content

You can review and manage how you forward content and whom you forward it to on an iPhone, iPad, or Mac.



Manage mail forwarding in iCloud

You can see whether your messages in 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 ID user name and password. If necessary, enter the two-factor authentication code.
2. Click Mail, then click the Settings button at the top of the Mailboxes list, then choose Preferences.
3. In the General tab, see whether “Forward my email to” is selected and whom it’s 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 your iPhone

When you send a message to someone who uses a phone other than an iPhone, your message is sent as an SMS message. You can set up your iPhone so that when you send or receive an SMS message, it appears on other devices. You can review the device list and disable text message forwarding on specific devices.

1. On your iPhone, go to Settings > Messages.
2. Tap Text Message Forwarding to see which devices are able to send and receive text messages from your device.
3. Turn off certain devices.

Manage call forwarding in Phone

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 > Phone > Calls > 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.

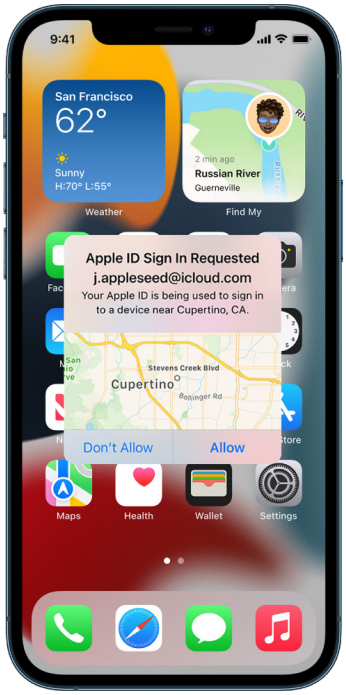
Block unknown sign-in attempts

When you sign in on a new device, you get a notification on your other trusted devices. The notification includes a map of the new device's location. This notification can appear on any trusted device; an iPhone, iPad, or Mac.



This is an approximate location based on the IP address or network that the device is currently using, rather than the exact location of the device.

If you see a notification that your Apple ID is being used to sign in on a new device and you're not signing in, tap Don't Allow to block the sign-in attempt. You may also want to capture a screenshot of the notification before dismissing it. See Record suspicious activity.



If you think your Apple ID might be compromised, see Keep your Apple ID secure and remove unknown devices.

Record suspicious activity

In some cases, such as if you see a notification that someone is attempting to use your Apple ID to sign in on a new device, you may want to take a screenshot or record video of the screen. You can then save these as image or video files on your iPhone, iPad, iPod touch, or Mac.



Take a screenshot or screen recording on your iPhone, iPad, or iPod touch

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, iPad, or iPod touch 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 (or use the Touch Bar).

   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 the Stop Recording button 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.

Share or stop sharing your location

The Find My app for iPhone, iPad, iPod touch, and Mac (and the Find People/Find Items apps in Apple Watch) helps keep you connected to your devices even if they are lost or stolen, and allows you and your family and friends to share locations with each other.



You can use Find My to locate your friends and family and to share your location with them (your location isn't shared by default). Share My Location—in the Me tab—must be on to share your location with friends, family, and contacts.

To see whom you're sharing your location with, go to the People tab in Find My. The people listed in this tab have either shared their location with you, or you've shared your location with them, or both. When someone shares their location with you, you can choose to share your location back, or not.



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.

Stop sharing your location using Find My

You can stop sharing your location with a particular person by choosing that person in the People tab, then scrolling down and choosing Stop Sharing My Location. Or you can stop sharing with everyone by turning off Share My Location in the Me tab.

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

Important: If you initially shared your location from iMessage rather than Find My and stop sharing, the person you stop sharing with may receive a banner in iMessage that you've stopped sharing your location. If you began sharing from Find My, and then stop sharing your location through Find My the person won't be able to see you on their list of friends. If you reenable sharing, they get a notification that you've started sharing your location with them.

Notify a friend when your location changes

You can use the Find My app to notify a friend when your location changes (https://support.apple.com/guide/iphone/iph9bfec93b1). Friends can also set up notifications for others to see when your location changes. To see all notifications about you:

1. Do one of the following:
   - On your iPhone, iPad, or iPod touch: Open the Find My app, then tap Me.
   - *On your Mac:* Open the Find My app, click Me, then click the Info button.
2. Look for a Notifications About You section to see a list of people who are notified when your location changes.
   - 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, you aren't notifying any friends when your location changes.

Turn off notifications about you

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

1. Do one of the following:
   - On your iPhone, iPad, or iPod touch: Open the Find My app, then tap Me.
   - *On your Mac:* Open the Find My app, click Me, then click the Info button.
2. Select a name, then select a notification.
3. Delete the notification, then confirm you want to delete the notification.

When to disable Find My for a lost or stolen device

To prevent theft, your device may be findable through the Find My network for up to 24 hours after it has been powered off or disconnected from the internet. The location is visible in Find My on your other devices, and to people 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 "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.

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

- On your iPhone, iPad, or iPod touch: 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.

- If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click Apple ID, click iCloud, then click Options next to Find My Mac.

- If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, click Apple ID, click iCloud, then click Options next to Find My Mac.

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 and 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 bar.
2. Select Favorites to open a window containing all of the locations you've designated as a Favorite.
3. Tap the Info button ⓘ next to the Favorite point of interest.
4. Scroll down to the Share ETA section to review whom you're automatically sharing your ETA with.
5. To remove someone, tap the Remove button beside the name of the person you want to remove.
6. To add someone, tap Add Person, then select the person from your Contacts 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.

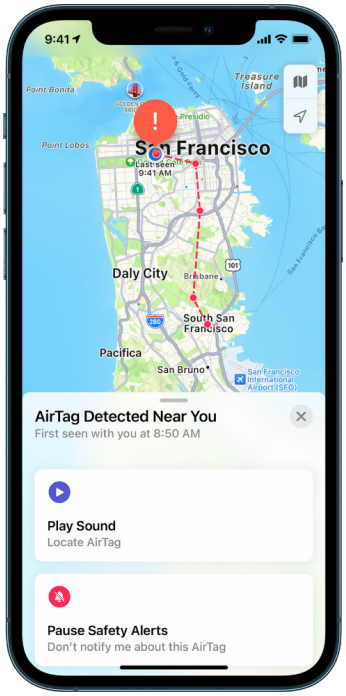
1. In the Maps app on your iPhone or iPad (Wi-Fi + Cellular), "Tap the Sharing with [*Name of Contact*]" at the bottom of the screen.
2. Identify the person on the list you no longer want to share your ETA with.
3. Select "Tap to stop," located under that person's name.

Stay safe with AirTag and other Find My accessories

AirTag lets you easily track things like your keys, wallet, purse, backpack, luggage, and more. If you find one that's not yours, you can view its serial number, help return it to its owner, or disable it. Use AirTag and the Find My network to discourage unwanted tracking on iPhone, iPad, iPod touch, and Mac.



Both AirTag and the Find My network are designed with privacy at their core. AirTag and Find My network accessories have unique Bluetooth identifiers that change frequently. To discourage unwanted tracking, Find My notifies you if an unknown AirTag or other Find My accessory is seen moving with you over time by sending you the message "[*AirTag*] or [*Item*] Detected Near You." (This feature is available on iPhone, iPad, or iPod touch running iOS 14.5 or iPadOS 14.5 or later).



If you see the above message on your device, it means that an AirTag or other Find My accessory has been separated from the person who registered it and is now moving with you. It's possible that the AirTag might be attached to an item you're borrowing. It's also possible that the owner might be tracking you without your knowledge.

View AirTag and Find My Network accessories that you've been recently notified about

1. Do one of the following:
   - On your iPhone, iPad, or iPod touch: 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 the option to play a sound isn't available, the item might not be with you anymore, might be near its owner, or if it was with you overnight, its identifier might have changed. To disable the AirTag, AirPods, or Find My network accessory and stop it from sharing its location, tap Instructions to Disable and follow the onscreen steps. After the AirTag, AirPods, or Find My network accessory is disabled, the owner can no longer get updates on its current location. You also no longer receive any unwanted tracking alerts for this item.

To learn more, see the Apple Support article What to do if you get an alert that an AirTag, Find My network accessory, or set of AirPods is with you (https://support.apple.com/HT212227).

Check for AirTags using an Android device

You can check for nearby AirTag or Find My network accessories using the Tracker Detect app (https://play.google.com/store/apps/details?id=com.apple.trackerdetect) from the Google Play Store. Tracker Detect looks for item trackers within Bluetooth range that are separated from their owner and that are compatible with Apple's Find My network. These include AirTag and compatible item trackers that use the Find My network. If you think someone is using an AirTag or another item tracker to track your location, you can scan to try to find it. If the app detects an AirTag or compatible item tracker near you for at least 10 minutes, you can play a sound to help locate it.

If you hear an AirTag make a sound

When moved, any AirTag separated for a period of time from the person who registered it makes a sound to alert 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. 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). You might need to provide the AirTag or its serial number.

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 with friends and family—such things as photos, calendars, and your location. You can sign in to iCloud on your device or the web with your Apple ID.

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



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, iPad, or iPod touch: 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.

- If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click Apple ID, then click iCloud.
- If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, click Apple ID, 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, iPad, or iPod touch: Go to Settings > [*your name*] > scroll down, then tap Sign Out.
- If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click Apple ID , click Overview, then click Sign Out.
- If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, click Apple ID , click Overview, then click Sign Out.

Control who can access your location

With your permission, Location Services allows apps (including Maps, Camera, Weather, and others) and websites to use information from various kinds of networks to determine your approximate location. You can find Location Services on iPhone, iPad, iPod touch, and Mac.



When an app is using Location Services, the Location Services icon appears on iPhone, iPad, and iPod touch (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 Mac computer's location information may be used for emergency calls to aid response efforts regardless of whether you enable Location Services.

Turn on Location Services

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.

If you didn't turn on Location Services at setup:

- On your iPhone, iPad, or iPod touch: Go to Settings > Privacy > Location Services and turn on Location Services.
- If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click Privacy & Security, click Location Services, turn on Location Services, enter your password, then click Unlock.
- If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, click Security & Privacy, then click Privacy. Click Location Services. If the lock at the bottom left is locked, click it to unlock the preference pane. Select Enable Location Services.

Turn off Location Services

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, iPad, or iPod touch: Go to Settings > Privacy > Location Services and turn off location sharing.
- If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click Privacy & Security, click Location Services, turn off Location Services, enter your password, then click Unlock.
- If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, click Security & Privacy, then click Privacy. Click Location Services. If the lock at the bottom left is locked, click it to unlock the preference pane. Deselect Enable Location Services.

Specify which apps can use Location Services on iPhone, iPad, or iPod touch

You can also grant or revoke access to your location for individual apps and indicate how often it may use your location. Instructions follow for iPhone, iPad, and iPod touch.

1. Go to Settings > Privacy > Location Services and 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:
   - If your Mac has macOS 13 or later: Choose Apple menu , click System Settings, click Privacy & Security , click Location Services, turn off Location Services, enter your password, then click Unlock.
   - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences > Security & Privacy , click Location Services, then deselect Enable Location Services. You may need to first unlock System Preferences to make changes. To do this, click the Lock button 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 the Remove button —. To remove all the locations, click the More button , then click Clear History.

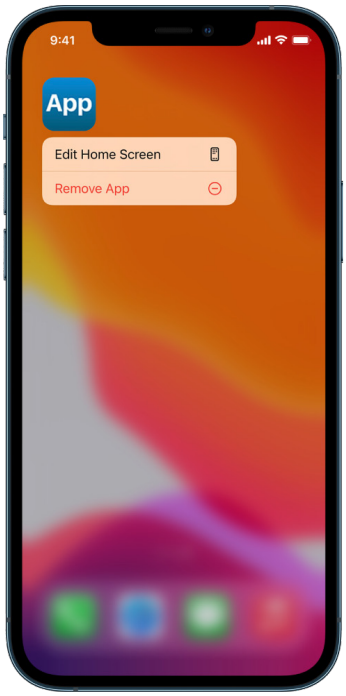
Delete suspicious content from your devices

You can delete any content you're concerned about or don't recognize, such as unknown apps and configuration files on your iPhone, iPad, iPod touch, or Mac.



Review and delete unknown apps from your iPhone, iPad, or iPod touch

If you're concerned someone you once trusted installed an app on your device without permission, you can review a list of all apps installed on the device and review or change how each app accesses information. If you notice an app has permission to access your data and you don't remember installing it or giving it permission to access your data, you may want to delete the app.



- *Delete an app from App Library and Home Screen:* Go to the Home Screen, swipe left past all your Home Screen pages to get to the App Library, touch and hold the app in the App Library, tap Delete App, then tap Delete.
- *Remove an app from the Home Screen:* Touch and hold the app on the Home Screen, tap Remove App, then tap Remove from Home Screen to keep it in the App Library, or tap Delete App to delete it.

Review and delete apps from your Mac

You can delete apps that may have been downloaded and installed from the internet or from a disc.

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:* 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.

Review 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 contain settings for a user's Mail account, Wi-Fi settings, VPN settings, and more. Configuration profiles can work on iPhone and iPad, Mac, and Apple TV.

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: 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, iPad, or iPod touch

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. Restart your device.

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.

Delete unknown configuration profiles from your Mac

1. Do one of the following:

   - If your Mac has macOS 13 or later: Choose Apple menu > System Settings > Privacy & Security, then click Profiles .
   - If your Mac has 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 the Remove button —.

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.

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. To change your Family Sharing status, it's good to know how the different roles within Family Sharing groups work. You can find Family Sharing on iPhone, iPad, iPod touch, and Mac.



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.



- *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 ID for a child who's too young to create their own.

In your household one adult, the *family organizer*, chooses the features the family will share 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 organizer can add anyone who has an Apple ID to their family and remove anyone over the age of 13 from the family group.

You can check to see if you're already part of a family in Settings > [*your name*]. If you see Set Up Family Sharing, you aren't using Family Sharing with this Apple ID. If you see an icon with Family Sharing, you can tap the icon to see your family members and roles.

Removing family members

The organizer of a Family Sharing group can remove other members.

Also, 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 ID website (https://appleid.apple.com) 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.

Note: The organizer can't remove themselves from the Family Sharing group. If you want to change the organizer, you must disband the group and have another adult create a new one.

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:

- Other family members' items no longer appear in the Purchased section of the iTunes Store, the App Store, and Apple Books.
- Protected (by copyright) music, movies, TV shows, books, and apps you previously downloaded are no longer usable if someone else originally purchased them. Other family members can no longer use this content downloaded from your collection.
- In-app purchases become unavailable if you bought them using an app someone else originally purchased. You can regain access to the in-app purchases by purchasing the app.
- Family members' device locations don't appear when you use the Find My app on iCloud.com or on your Mac, iOS, or iPadOS devices.

If Family Sharing is turned off

If the family organizer turns off Family Sharing, all family members are removed from the family group at once. If there are children under 13 in the family group, you must transfer them to another family before you can disband yours.

Remove members from a family group on your iPhone, iPad, or iPod touch

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 Family Sharing.

Remove members from a family group on your Mac

If you're the family organizer:

1. Do one of the following:
   - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click Family Sharing, then select Family Sharing in the sidebar.
   - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, click Family Sharing, then select Family Sharing.
2. Select the member in the list, then click the Remove button —.

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

Leave a Family Sharing group on your iPhone, iPad, or iPod touch

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:
   - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click Family Sharing, then select Family Sharing in the sidebar.
   - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, click Family Sharing, then select Family Sharing.
2. In the list of family members, click Details next to your name, click Stop Using Family Sharing, then follow the onscreen instructions.
3. Click Done.

Stop Family Sharing on your iPhone, iPad, or iPod touch

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

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

1. Do one of the following:
   - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click Family Sharing, then select Family Sharing in the sidebar.
   - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, click Family Sharing, then select Family Sharing.
2. Click the Details button next to your name, then click Stop Family Sharing.

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 ID 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/HT204759).

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

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, iPod touch, 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/ios/home/accessories/).

Stop sharing your home with someone

1. Tap or click 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, tap or click the user you want to remove from your home, then tap or click 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, tap or click 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 tap or click Leave Home. Tap or click 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, tap or click, then select Home Settings.
2. At the bottom of the dialog, tap or click Remove Home, then tap or click 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.

How to erase all content and settings

If you're concerned someone may have had physical access to your device and tampered with its built-in security, you can restore the device to its factory settings—even if you aren't running the latest version of iOS, iPadOS, and macOS. A factory restore erases 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. It also installs the latest version of the operating system.



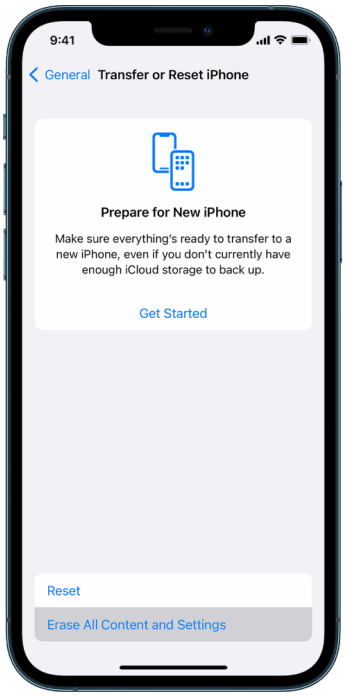
This process, known as *Erase All Content and Settings*, can take some time; however, it helps ensure that your device can be accessed only by you.

Important: When you use Erase All Content and Settings, all your data is erased.

If you want to use Erase All Content and Settings on your Mac, you must be running 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/HT212030) and Use Disk Utility to erase an Intel-based Mac (https://support.apple.com/HT208496).

Erase your iPhone, iPad, or iPod touch and restore it to factory settings

1. Go to Settings > General > Reset, then tap Erase all Contents and Settings.



2. Enter your passcode or Apple ID password.
3. Wait for all content to be safely removed from your device.

Erase your Mac and restore it to factory settings

1. Do one of the following:
   - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click General, click Transfer or Reset, then click Erase All Content and Settings.
   - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, then in the menu bar, choose System Preferences > Erase All Content and Settings.
2. In Erase Assistant, enter your administrator information (the password you use to log in to your Mac).
3. Review items that will be removed in addition to your content and settings.

   If your Mac has multiple user accounts, click the arrow next to your account name to review the items.
4. Click Continue, then follow the onscreen instructions.

Restore the data you backed up

If you backed up your Apple device before you erased it and before you restored it to factory settings, you can restore your data from a backup in iCloud or one on your computer. If you're concerned your backup may contain configurations or apps that you don't want on your device, you can review the App Library and settings after the backup has been restored. You can restore a Mac using Time Machine, or an iPhone, iPad, or iPod touch using a computer or iCloud.



Restore your iPhone, iPad, or iPod touch from an iCloud backup

1. Turn on your device. You should see a Hello screen. (If you already set up your device, you need to erase all of its content before you can use these steps to restore from your backup.)
2. Follow the onscreen setup steps until you reach the Apps & Data screen, then tap Restore from iCloud Backup.
3. Sign in to iCloud with your Apple ID.
4. Choose a backup.

   Look at the date and size of each backup and pick the most relevant. After you choose a backup, the transfer starts. If a message says that a newer version of software is required, follow the onscreen steps to update.
5. When asked, sign in with your Apple ID to restore your apps and purchases.

   If you've purchased iTunes or App Store content using multiple Apple IDs, you'll be asked to sign in to each. If you can't remember your password, you can tap Skip this Step and sign in later. You won't be able to use the apps until you sign in with your Apple ID.
6. Stay connected to Wi-Fi and wait for a progress bar to appear.

   Depending on the size of the backup and the network speed, the progress bar might need a few minutes to an hour to show that the networking process is complete. If you disconnect from Wi-Fi too soon, the progress pauses until you reconnect.
7. You can now finish setup.

   Content like your apps, photos, music, and other information continues to restore in the background for the next several hours or days, depending on the amount of information. Try to connect often to Wi-Fi and power to allow the restore to complete.

After the restore is complete:

- Go to the App Library and review the apps installed on your device. If you find any unknown third-party apps, you can delete them.

  See the Apple Support article Organize the Home Screen and App Library on your iPhone (https://support.apple.com/HT211345).

- Review and delete any device configuration profiles or mobile device management profiles that you didn't authorize. (Configuration profiles are used by schools and businesses to help ensure a consistent setup across devices. Be careful not to delete profiles installed by your school or workplace.)

Restore your iPhone, iPad, or iPod touch from a backup on your computer

1. On a Mac with macOS 10.15 or later, open the Finder. On a Mac with macOS 10.14, or earlier, or on a PC, open iTunes.
2. Connect your device to your computer with a USB cable. If a message asks for your device passcode or to Trust This Computer, follow the onscreen steps.
3. Select your iPhone, iPad, or iPod touch when it appears in the Finder window or iTunes.
4. Select Restore Backup.
5. Look at the date of each backup, and pick the most relevant.
6. Click Restore and wait for the restore to finish. If asked, enter the password for your encrypted backup.
7. Keep your device connected after it restarts and wait for it to sync with your computer. You can disconnect after the sync finishes.

After the restore is complete:

- Go to the App Library and review the apps installed on your device. If you find any unknown third-party apps, you can delete them.

  See the Apple Support article Organize the Home Screen and App Library on your iPhone (https://support.apple.com/HT211345).

- Review and delete any device configuration profiles or mobile device management profiles that you didn't authorize. (Configuration profiles are used by schools and businesses to help ensure a consistent setup across devices. Be careful not to delete profiles installed by your school or workplace.)

Restore items backed up with Time Machine on Mac

If you use Time Machine to back up the files on your Mac, you can easily get back lost items or recover older versions of files. You can use Time Machine within many apps.

1. On your Mac, open a window for the item you want to restore.

   For example, to recover a file you accidentally deleted from your Documents folder, open the Documents folder.

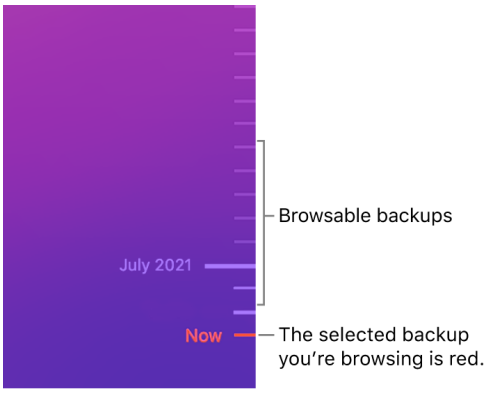
   If you're missing an item from the desktop, you don't need to open a window.

2. Use Launchpad to view and open apps on Mac and open Time Machine. A message may appear while your Mac connects to the backup disk.

   You can also open Time Machine by clicking the Time Machine icon in the menu bar, then choosing Enter Time Machine. If the Time Machine icon isn't in the menu bar, do one of the following:

   - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click Time Machine, then select "Show Time Machine in menu bar."
   - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, click Time Machine, then select "Show Time Machine in menu bar."

3. Use the arrows and timeline to browse the local snapshots and backups.



   If you see a pulsing light to semi-dark gray tick mark, it represents a backup that's still loading or validating on the backup disk.

4. Select one or more items you want to restore (these can include folders or your entire disk), then click Restore.

   Restored items return to their original location. For example, if an item was in the Documents folder, it's returned to the Documents folder.

After the restore is complete:

- Go to Launchpad and review the apps installed on your Mac. If you find any unknown third-party apps, delete them by pressing and holding the Option key, then clicking the X on the app you want to remove.
- Review and delete any device configuration profiles or mobile device management profiles that you didn't authorize. (Configuration profiles are used by schools and businesses to help ensure a consistent setup across devices. Be careful not to delete profiles installed by your school or workplace.)

Safety and privacy tools

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 ID. 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/HT201222#update).

Update iPhone, iPad, and iPod touch automatically

If you didn't turn on automatic updates when you first set up your device, you can now by doing the following:

1. Go to Settings > General > Software Update > Automatic Updates.
2. Turn on both options: Download [*iOS or iPadOS*] Updates and Install [*iOS or iPadOS*] Updates.

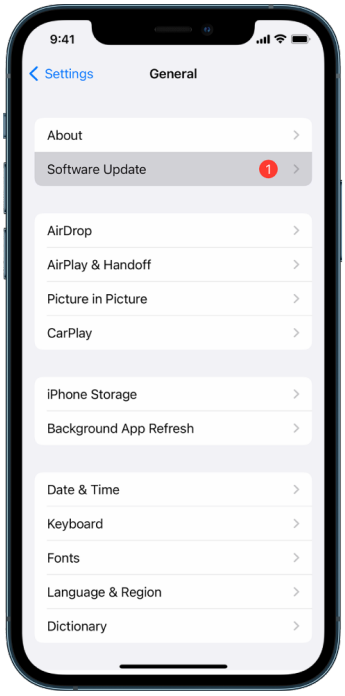
When an update is available, the device downloads and installs the update overnight while it's charging and connected to Wi-Fi. You're notified before an update is installed.

To turn off automatic updates, go to Settings > General > Software Update > Automatic Updates, then turn off both options.

Update iPhone, iPad, and iPod touch 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, iPad, and iPod touch 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 PC 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 be running macOS 10.15 or later. With earlier versions of macOS, use iTunes (https://support.apple.com/guide/itunes/itns3235/12.9/mac/10.14) to update your device.
   - *In the iTunes app on your Windows PC:* 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. Do one of the following:
   - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click General, then click Software Update.
   - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, 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 system data files and security updates.”
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.

- Do one of the following:
  - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click General, then click Software Update.
  - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, 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 .

Set a unique passcode or password on Apple devices

To prevent anyone except you from using your devices and accessing your information, use a unique passcode or password that only you know. If you share a device or if others know your passcode or password, remember that they can see the information on your device or account and can change the device's settings.

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. Your Mac password must have eight or more characters and include upper- and lowercase letters, and at least one number. You can also add extra characters and punctuation marks to make your password even stronger.

Set a passcode on your iPhone, iPad, or iPod touch

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

- 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.
  - On your iPod touch: 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 login password on your Mac

It’s important to change your login password from time to time 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. It is not your Apple ID password, which provides access to the iTunes Store, App Store, Apple Books, iCloud, and other Apple services.

1. Do one of the following:
   - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click General, click Users & Groups , then click the Info button .
   - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, click Users & Groups , then click Change Password.
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 the Key button 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.

Change when to automatically lock your iPhone, iPad, or iPod touch

- Go to Settings > Display & Brightness > Auto-Lock, then set a length of time.

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 ensures 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/HT209183).

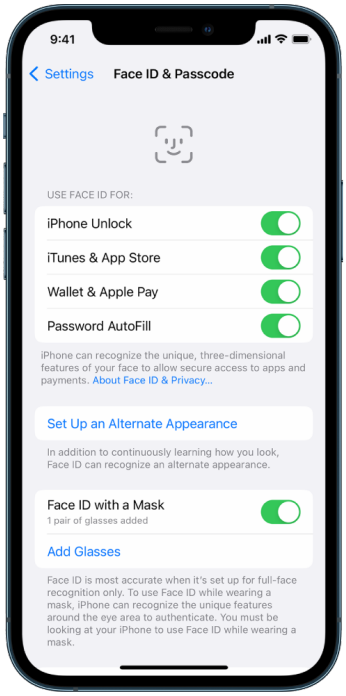


Set up Face ID

- 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 during Face ID set up. 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) 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.

Reset Face ID

If there is an alternate appearance that you don't want to keep or if you believe someone may have added an alternate appearance on your device without your permission, you can reset Face ID, 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.

Secure your devices with Touch ID

Use Touch ID to securely and conveniently unlock iPhone or iPad, 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 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.

   If you see existing fingerprints you don't recall adding, see Delete unknown fingerprints from iPhone or iPad.

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 (https://support.apple.com/HT207537).

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. Do one of the following:
   - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, then click Touch ID.
   - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, then click Touch ID.
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 fingerprints from iPhone or iPad

If there are multiple fingerprints on your iPhone or iPad and you want to remove the possibility that someone else can access your device using an additional fingerprint, you can reset fingerprints so that only your fingerprint is available on the device.

1. Go to Settings > Touch ID & Passcode.
2. If more than one fingerprint is available, place a finger on the Home button to identify its print.
3. Tap the fingerprint, then do any of the following:
   - Enter a name (such as “Thumb”).
   - Tap Delete Fingerprint.

Add or delete fingerprints on your Mac

If there are multiple fingerprints on your Mac or Magic Keyboard with Touch ID and you’re concerned one or more may not be yours, you can delete the fingerprints and then add back your own fingerprint.

1. Do one of the following:
   - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, then click Touch ID.
   - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, then click Touch ID.
2. Do any of the following:
   - *Add a fingerprint:* Click Add Fingerprint to add new fingerprint, then choose which options you’d like to use with Touch ID.
   - *Delete a fingerprint:* Click a fingerprint, enter your password, click OK, then click Delete.

Keep your Apple ID secure

Your Apple ID 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 ID, 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 ID on iPad, iPhone, iPod touch, and Mac.



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

Secure your Apple ID

1. Don’t share your Apple ID with anyone, even family members, partners, and close friends. If you share an Apple ID, you’re giving someone else access to all your personal data and your content. If someone else set up your Apple ID and password for you, or has had access to your password, you should change your password.
2. Use two-factor authentication for your Apple ID. 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.

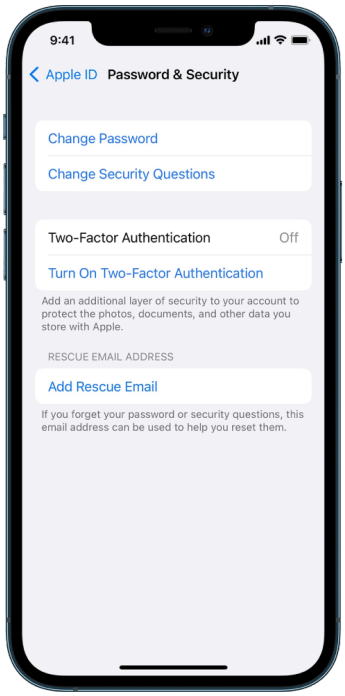
   You must verify at least one trusted phone number—a number where you can receive verification codes by text message or automated phone call—to enroll in two-factor authentication.
3. Pay attention to notifications about your Apple ID. Apple notifies you by email, text, or push notification when changes are made to your account, such as when there is a sign in for the first time on a new device or when your password is changed, so it’s important to keep your contact information up to date.

   See Block unknown sign-in attempts.
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 ID security information

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

1. Do one of the following:
   - On your iPhone, iPad, or iPod touch: Go to Settings > [*your name*].
   - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, then click Apple ID.
   - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, then click Apple ID.
   - *In a web browser on your Mac or PC:* Go to the Apple ID account page (https://appleid.apple.com/).
2. In the Name, Phone Numbers, Email 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 to remove them from your account.
   - If you haven't yet set up two-factor authentication, see Use two-factor authentication.

Secure your account and remove unknown devices

If there are devices connected to your Apple ID 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 these steps to review your account information and protect your account:

1. If you want to change your password:
    - On your iPhone, iPad, or iPod touch: Go to Settings > [*your name*] > Password & Security > Change Password. Choose a strong password (eight or more characters, including upper and lowercase letters, and at least one number).
    - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, then click Apple ID > Password > Security > Change Password. Choose a strong password (eight or more characters, including upper and lowercase letters, and at least one number).
    - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, then click Apple ID > Password > Security > Change Password. Choose a strong password (eight or more characters, including upper and lowercase letters, and at least one number).
    - If you want to remove the devices you don't want connected to your account, go to Settings > Apple ID. Scroll down to the list of devices, tap the device you want to remove, then tap Remove from Account.
2. If you want to change the email address associated with your Apple ID for added safety, open Safari and sign in to your account at https://appleid.apple.com. Select Account and under your current Apple ID, select Change Apple ID, then enter the new email address you would like to use.
3. If you want to remove the devices you don't want connected to your account:
    - On your iPhone, iPad, or iPod touch: Go to Settings > [*your name*], scroll down to the list of devices, tap the device you want to remove, then tap Remove from Account.
    - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click Apple ID, scroll down to the list of devices, click the device you want to remove, then click Remove from Account.
    - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, click Apple ID, 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 ID 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, iPod touch, and Mac.



Set up two-factor authentication on your iPhone, iPad, or iPod touch

1. Go to Settings > [*your name*] > Password & 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 sign out completely, erase your iPhone, sign in to your Apple ID account page in a web browser, or need to change your Apple ID 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 period, 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

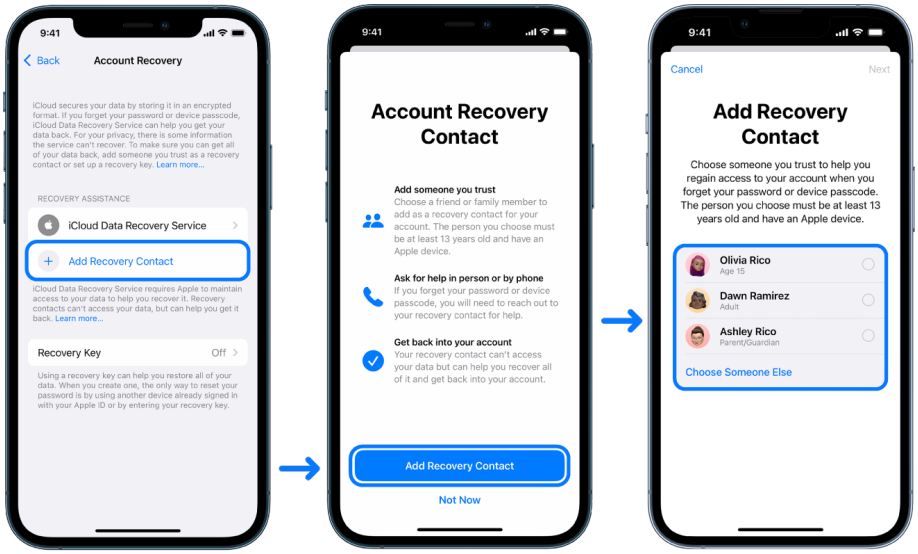
1. Do one of the following:
   - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click Apple ID , then select Password & Security in the sidebar.
   - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, click Apple ID , then select Password & Security.
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 your Apple ID completely, erase your Mac, or need to change your password for security reasons.

If you get locked out of your Apple device

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, iPod touch, or Mac so that you can regain access to your data if you ever get locked out.



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



Set up an account recovery contact

If you're concerned that someone may use access to 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, iPad, or iPod touch: Go to Settings > [*your name*], then tap Password & Security.
   - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click Apple ID, then select Password & Security in the sidebar.
   - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, click Apple ID, then select Password & 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 have been added as your account recovery contact.

Remove a recovery contact

If the person set as your recovery contact is someone you no longer trust and you would like to remove them as your recovery contact, you can remove that contact.

1. Do one of the following:
   - On your iPhone, iPad, or iPod touch: Go to Settings > [*your name*], then tap Password & Security.
   - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click Apple ID, then select Password & Security in the sidebar.
   - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, click Apple ID, then select Password & Security.
2. Under Recovery Assistance, choose the Recovery Contact you would like to remove, then remove the contact.

Keep your device, app, and website passwords secure on iPhone and iPad

On your iPhone or iPad, 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.



Manage passwords

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

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.

See how apps are accessing your data

If you're concerned that someone close to you installed apps on your iPhone, iPad, or iPod touch 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.

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.

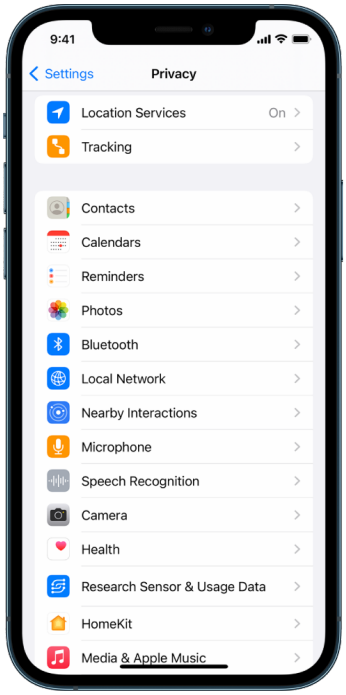
Turn on App Privacy Report

1. On your iPhone, iPad, or iPod touch, go to Settings > Privacy.
2. Scroll down and tap App Privacy Report.
3. Tap Turn on App Privacy Report.

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

Change your 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, iPad, or iPod touch: Go to Settings > [*your name*] > Password & Security.
   - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, Privacy & Security, then click Privacy.
   - If your Mac has macOS 12 or earlier: Choose Apple menu > System Preferences, click Security & Privacy, then click Privacy.

     You can change each setting in the list of options that appears.

2. To see which apps that have access to various types of information on your device, select a type of data from the list.

   You'll see which apps have asked for permission to use that data. 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. An app can use the data type in the setting only if you have given the app permission.

Changing the privacy settings on your Apple device only changes how those apps can access your device. If you want to change the 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.

Harden your devices against mercenary spyware with Lockdown Mode

Lockdown Mode is an extreme, optional protection for iPhone, iPad, and Mac (running iOS 16, iPadOS 16.1, and macOS 13) 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 won'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.

To learn more about Lockdown Mode:

- *On your iPhone or iPad:* Go to Settings > Privacy & Security > Lockdown Mode, then tap Learn More.
- *On your Mac:* Choose Apple menu > System Settings, Privacy & Security > Lockdown Mode, then click Learn More.

Manage safety settings in iMessage

You can use iMessage to send messages, photos, or videos to another iPhone, iPad, iPod touch, 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.



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.

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, iPad, or iPod touch: Go to Settings > Messages, then turn iMessage on or off.
- If your Mac has macOS 13 or later: Open Messages go to Messages > Settings, click the iMessage tab, then sign in or out using your Apple ID.
- If your Mac has macOS 12 or earlier: Open Messages go to Messages > Preferences, click the iMessage tab, then sign in or out using your Apple ID.

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, iPad, or iPod touch: Go to Settings > Messages, then turn Read Receipts on or off.
- If your Mac has macOS 13 or later: Open Messages go to Messages > Settings, click the iMessage tab, then select or deselect Send Read Receipts.
- If your Mac has 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, 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 running macOS 13: 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, and macOS 13, 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, iPad, or iPod touch: 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 running macOS 13 or later: 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.

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 ID.

Important: The person you block won'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 have 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 emails from certain people

- *Phone app on your iPhone:* In the Phone app, tap Favorites, Recents, or Voicemail, tap the Info button ⓘ 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, iPad, or iPod touch: In your FaceTime call history, tap the Info button ⓘ 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 on the name, phone number, or email address of the contact you want to block, then select Block this Caller.
- Messages app on your iPhone, iPad, or iPod touch: In Messages, tap a conversation, tap the name or number at the top of the conversation, tap the Info button ⓘ, 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 Conversations menu, select Block Person, then click Block.
- Mail app on your iPhone, iPad, or iPod touch: Tap Mail, 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:* Open Mail, select an email message from the sender, click their name at the top of the email, then from the dropdown select Block this Contact.

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, iPad, iPod touch: Go to Settings > FaceTime, then under Calls, tap Blocked Contacts.
- *FaceTime on your Mac:* Open FaceTime, go to FaceTime > Settings (or FaceTime > Preferences), then click Blocked.
- Messages app on your iPhone, iPad, or iPod touch: 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, iPad, or iPod touch: 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.

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 use Private Browsing mode. When you use Private Browsing, the details of your browsing aren't saved, and they aren't shared across your devices. You can clear your browsing history and open a Private Browsing window on iPhone, iPad, iPod touch, and Mac.



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.

Clear your browsing history in Safari

- On your iPhone, iPad, or iPod touch: 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 and iPad

1. Tap Maps, 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 the Remove button to remove multiple Favorites.

Clear recent directions and favorites in Maps on Mac

1. Open the Maps app, the 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 or iPod touch

1. Tap the Tabs button.
2. Tap the Tab Groups button 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 the Tabs button, then tap the Tab Groups button 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 the Tabs button, then swipe left each of the tabs you want to close.

Open a Private Browsing window on iPad

- Tap the Show Sidebar button, 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 the Show Sidebar button, 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.

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:

   - If your Mac has macOS 13 or later: Choose Apple menu > System Settings, click Desktop & Dock, then make sure “Close windows when quitting an app” is selected.
   - If your Mac has 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.

Make an emergency call on iPhone

In case of emergency, you can use iPhone to quickly call 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 (https://support.apple.com/guide/iphone/iph08022b194/#iphbcea12902) in the iPhone User Guide.

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/HT210894).

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

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 (https://support.apple.com/guide/iphone/iph08022b192) in the iPhone User Guide.

Set up or change emergency contacts

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. Tap Edit, then scroll to Emergency Contacts.
4. Add or delete a contact.
   - *Add a contact:* Tap the Add button to add an emergency contact (You can't set emergency services as an SOS contact).
   - *Delete a contact:* Tap the Delete button 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

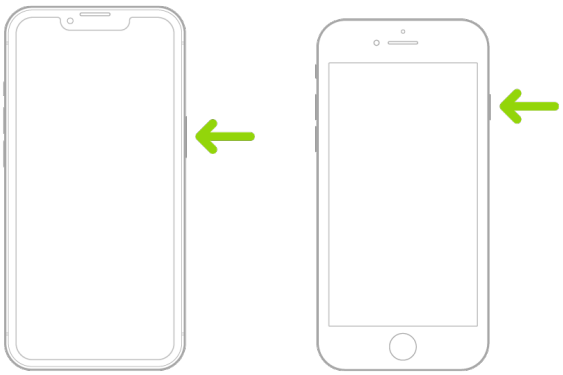
1. On the Passcode screen, tap Emergency.
2. Dial the emergency number (for example, 911 in the U.S.), then tap the Call button.

Use Emergency SOS (all countries or regions except India)

When you make a call with Emergency SOS, your iPhone can quickly call the local emergency number. After the call ends, your iPhone sends your emergency contacts a text message with your current location, unless you choose to cancel. If Location Services is off, it temporarily turns itself on. If your location changes, your contacts get an update and you get a notification about 10 minutes later. (When your location is being shared through this feature, you get a reminder every 4 hours for 24 hours. To stop sharing your location, you can tap the status bar at the top of your screen and select Stop Sharing Emergency Location.)

- On an iPhone with
  Face ID, iPhone SE (2nd generation and later), iPhone 8, and iPhone 8 Plus: Press and hold the side button and either volume button. Continue to hold the buttons when the Emergency SOS slider appears, until iPhone plays a warning sound and starts a countdown. (To skip the countdown, drag the Emergency SOS slider.) When the countdown ends, iPhone calls emergency services.

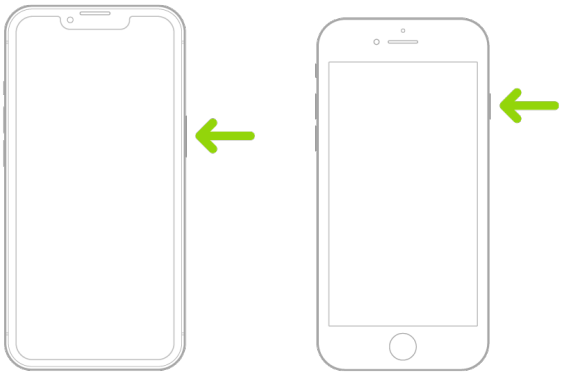
  Or, you can enable iPhone to start Emergency SOS when you press the side button five times. Go to Settings > Emergency SOS, then turn on Call with 5 Presses.
- *On other iPhone models:* Press the side button five times, then drag the Emergency SOS slider.



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.

Use Emergency SOS (India)

- *On an iPhone with Face ID:* Triple-click the side button. Or, if the Accessibility Shortcut is turned on, press and hold the side button and either volume button until the sliders appear, then drag Emergency SOS.
- *On an iPhone with a Home button:* Triple-click the side button.



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.

Important information about emergency calls on iPhone

- Some cellular networks may not accept an emergency call from iPhone if iPhone isn't activated, if iPhone isn't compatible with or configured to operate on a particular cellular network, or (when applicable) if iPhone doesn't have a SIM card or the SIM card is PIN-locked.
- In certain countries or regions, your location information (if determinable) may be accessed by emergency service providers when you make an emergency call.
- Review your carrier's emergency calling information to understand the limits of emergency calling over Wi-Fi.
- With CDMA, when an emergency call ends, iPhone enters *emergency call mode* for a few minutes to allow a callback from emergency services. During this time, data transmission and text messages are blocked.
- After making an emergency call, certain call features that block or silence incoming calls may be disabled for a short period of time to allow a callback from emergency services. These include Do Not Disturb, Silence Unknown Callers, and Screen Time.
- On an iPhone with Dual SIM, if you don't turn on Wi-Fi Calling for a line, any incoming phone calls on that line (including calls from emergency services) go directly to voicemail (if available from your carrier) when the other line is in use; you won't receive missed call notifications.

  If you set up conditional call forwarding (if available from your carrier) from one line to another when a line is busy or not in service, the calls don't go to voicemail; contact your carrier for setup information.

Know how to obtain evidence related to another person's 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:* Legal Process Guidelines (https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf)
- *Outside the United States:* Legal Process Guidelines (https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf)

Personal safety checklists

See who has access to your iPhone or iPad

If you're running iOS 15 or earlier, use this checklist to see who has access to your device or accounts. If you're running iOS 16 or later, see How Safety Check works.

1. Check which devices are signed in to your account by going to Settings > [*your name*]. If you see a device you don't recognize, tap on that device name and select "Remove from Account."
2. Check to see if there is an unexpected alternate Face ID appearance or additional Touch ID fingerprint set up on your device by following these instructions: Set up Face ID and Set up Touch ID on your iPhone or iPad.
3. Sign in to the Apple ID website (https://appleid.apple.com) and review all the personal and security information in your account to see if there is any information that someone else has added.
4. If you have two-factor authentication turned on, review trusted devices for any devices that you don't recognize. If you don't have it turned on, you can turn it on by following these instructions: Set up two-factor authentication on your iPhone, iPad, or iPod touch.
5. Review the installed apps on your device and look for apps you don't recognize or don't remember installing. You can look up any apps you find in the App Store to see what their purpose is.
6. Mobile device management (MDM) configuration profiles—typically installed by employers, schools, or other official organizations—allow additional privileges and access to a user's devices. To look for an unknown MDM configuration profile on your devices, see Delete unknown configuration profiles from your iPhone, iPad, or iPod touch.
7. To see if anything has been changed in or added to your sharing permissions, see the checklist How to stop sharing your iPhone or iPad content.

How to stop sharing your iPhone or iPad content

If you're running iOS 15 or earlier, use this checklist to learn how to stop sharing with someone you previously shared with. If you're running iOS 16 or later, see How Safety Check works.

1. Check to see if you're part of a Family Sharing group by going to Settings > [*your name*] and look for the Family Sharing tab. If you're in a Family Sharing group, the names of the family members are visible.
2. If you're part of a Family and no longer want to share information, you can remove yourself (as long as you're 13 or older). If you're the one who set the Family up (the word *Organizer* appears under your name), you can remove anyone over the age of 13 from the Family.
3. In the Find My app, tap the People tab to see whom you share your location with. If you want to stop sharing with an individual, select the person, then tap Stop Sharing My Location. To stop sharing with everyone, tap Me, then turn off Share My Location..
4. In the Photos app, tap Albums, then go to Shared Albums. Select a shared album, and tap People to see the owner of the shared album and whom it's shared with.
   - If you're the album owner and would like to stop sharing, tap the name of the subscriber you want to stop sharing with, then select that option.
   - If you're a subscriber, you can tap Unsubscribe from the bottom of the screen. You can also delete any photos that you shared.
5. In the Calendar app, tap Calendars. Select a shared calendar and tap the Info button to see whom the calendar is shared with.
   - If you're the Calendar owner and would like to stop sharing, tap the name of the subscriber you want to stop sharing with, then select that option.
   - If you're a subscriber, you can tap Delete Calendar from the bottom of the screen.
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 Securely control whom you share content with from iPhone, iPad, and Apple Watch.

How to stop sharing your iPhone or iPad location

If you're running iOS 15 or earlier, use this checklist to limit who can see your location or to stop sharing your location entirely. If you're running iOS 16 or later, see How Safety Check works.

1. If you aren't running 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. It also installs the latest version of the operating system. To restore it to factory settings, see How to erase all content and 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, such as 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. You can share your location with just certain apps. Go to Settings > Privacy > Location Services, then choose the apps you want to have use Location Services, from the list near the bottom of the screen.

4. Stop sharing your location with a particular person. In 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. Stop sharing your estimated time of arrival (ETA) in Maps. In Maps, select Favorites to open a window containing all of the locations you've designated as a Favorite. Tap the Info button, then scroll down to the Share ETA section and remove the person you're sharing with.

6. See whether any third-party apps are sharing your location with others. With Location Services turned on, review the list of apps you've installed on your device to see if any of them are sharing your location. Then select one and follow the relevant instructions to stop sharing.

7. You can track the location of your accessories to make sure that only the devices you configured for personal use are paired with your device.

   - *Track using AirTags:* Use AirTags to connect accessories to the Find My network and track their location. See the Apple Support article Use the Find My app to locate a missing device or item (https://support.apple.com/HT210515).
   - *Find out if an unpaired device is moving with you:* In Find My, tap Devices at the bottom of the screen. If you use an Android device, download the Tracker Detect app (https://play.google.com/store/apps/details?id=com.apple.trackerdetect) from the Google Play Store to help identify hidden AirTags or other accessories on the Find My network.

© 2022 Apple Inc. All rights reserved.

Apple, the Apple logo, AirDrop, AirPods, Apple Books, Apple Music, Apple Pay, Apple TV, Apple Watch, Digital Crown, Face ID, FaceTime, FileVault, Finder, HomeKit, HomePod, iMac, iMessage, iPad, iPadOS, iPad Pro, iPhone, iPod touch, iTunes, Launchpad, Lightning, Mac, MacBook Air, MacBook Pro, macOS, Magic Keyboard, OS X, Safari, Siri, Time Machine, and Touch ID are trademarks of Apple Inc., registered in the U.S. and other countries and regions.

AirTag, Find My, and Touch Bar are trademarks of Apple Inc.

App Store, iCloud, 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

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 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.

028-00570