



Device and Data Access when Personal Safety is At Risk

What's in this guide?

Apple makes it easy to connect and share your life with the people closest to you. What you share, and whom you share it with, is up to you — including the decision to make changes to better protect your information or personal safety.

If you'd like to revisit what you share with other people, or restore your device's original settings for any reason, this guide can help you understand what information you are sharing via your Apple devices, and how to make changes to protect your safety. It includes step-by-step instructions on how to remove someone's access to information you've previously granted: from location data on the Find My app, to meetings you've scheduled via Calendar.

If you're concerned that someone is accessing information you did not share from your Apple device, this guide will also help you identify risks, and walk you through the steps to help make the technology you rely on as private and secure as you want it to be.

Contents

Update your software	3
Restoring your device to factory settings	3
Protect your device	4
Protect your Apple ID	5
If you don't recognize a sign-in location	7
Check privacy settings	8
Using the Find My app	9
Sharing your location	10
Sharing with iCloud	11
Shared Albums in Photos	12
Shared Calendars	12
Sharing your Activity with Apple Watch	13
Delete unknown third-party apps	14
Delete unknown configuration profiles	15
If you use Family Sharing	16
Phishing and fraudulent requests to share info	17
Checklist: If you want to see if anyone else has access to your device or accounts	18
Checklist: If you want to stop sharing with someone whom you previously shared with	19
Checklist: If you want to make sure no one else can see your location	20

Update your software

Updating your software is one of the most important things you can do to protect your device and your information.

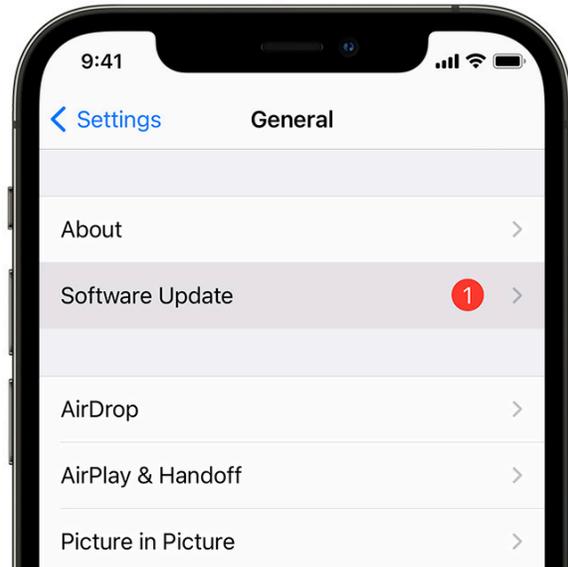
- On iPhone, iPad, or iPod touch, you can see the software version you are running by going to Settings > General > Software Update.
- On your Mac, go to System Preferences > Software Update.

If there is a software update [available for your device](#), download and install it.

If you have iOS 12 or later, you can also enable automatic updates from the Software Updates menu.

[Update your iPhone, iPad, or iPod touch](#)

[How to update the software on your Mac](#)



Restoring your device to factory settings

If you are not running the latest version of iOS and have concerns that someone else may have had physical access to your device, you should back up the information from your device and restore the device to factory settings. This process can take some time, but it will ensure that your device is accessible only by you, while preserving all of your information.

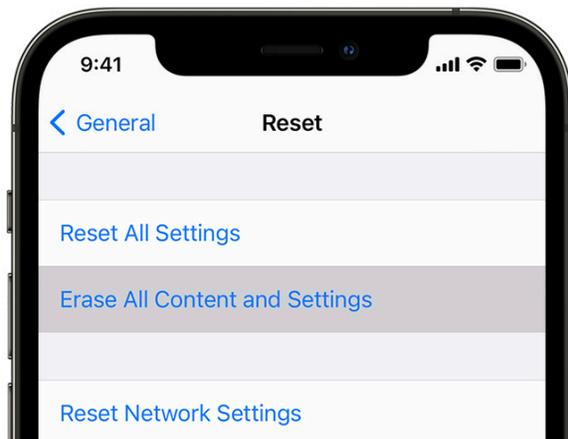
To erase your device and restore it to factory settings:

1. Go to Settings > General > Reset then tap Erase all Contents and Settings.
2. Enter your passcode or Apple ID password.
3. Wait for your device to erase.

[How to back up your iPhone, iPad, and iPod touch](#)

[How to erase your iPhone, iPad, or iPod touch](#)

[How to erase a disk for Mac](#)



Protect your device

To prevent anyone except you from using your devices and accessing your information, make sure you use unique passcodes or passwords **that only you know**, and use Touch ID or Face ID on your iPhone or iPad.

Face ID allows you to set up an alternate appearance, so that Face ID still recognizes you if you have an appearance that can look vastly different. Touch ID allows you to add additional fingerprints.

If you believe someone else knows your device passcode or may have added an alternate appearance or fingerprint on your device, you can reset or remove these in Settings using the instructions at these pages:

[Use a passcode with your iPhone, iPad, or iPod touch](#)

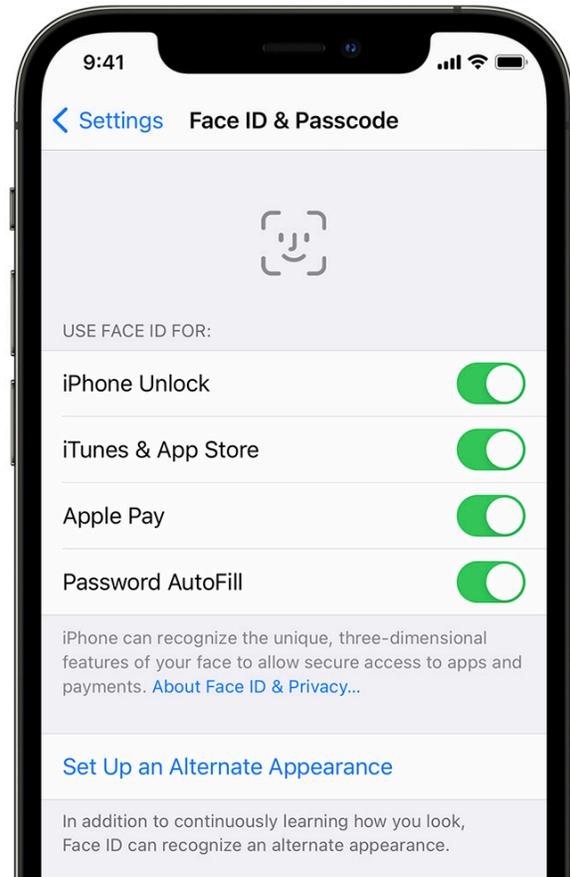
[Use Face ID on your iPhone or iPad Pro](#)

[If Face ID isn't working on your iPhone or iPad Pro](#)

[Use Touch ID on iPhone and iPad](#)

[Change or reset the password of a macOS user account](#)

[Use Touch ID on your Mac](#)



Protect your Apple ID

Your Apple ID is the personal account that you use to sign into your device and access Apple services. This includes services like the App Store, iCloud, iMessage, FaceTime, and Find My, and personal information that you store with Apple and share across devices, like contacts, payment info, photos, device backups, and much more.

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

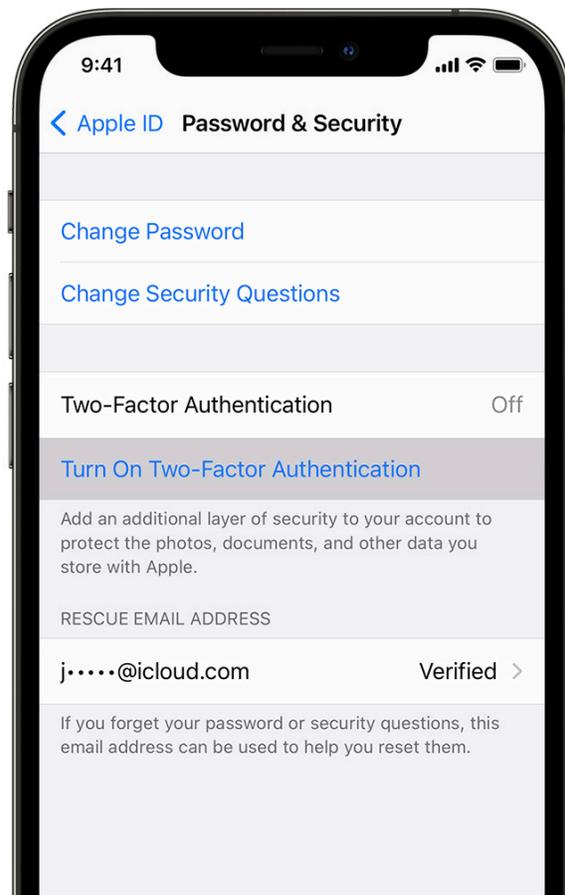
1. Don't share your Apple ID password with anyone, even family members. If you share an Apple ID, you're giving someone else access to all your personal data and your content. If someone else set up your Apple ID and password, you should change your password. You can use [Family Sharing](#) to share information and services without sharing accounts.
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 knows your password. With two-factor authentication, you'll need to provide your password and a six-digit verification code that automatically appears on your trusted device(s) 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 you 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.

To check and update your Apple ID security information, go to Settings > [your name].

Tap Name, Phone Numbers, Email to see and update personal information. Tap Password & Security to see your trusted phone numbers, whether two-factor authentication is on, and trusted devices. You can also view and update this info at your Apple ID account page: appleid.apple.com.



If you think your Apple ID has been compromised, follow these steps to review your account information and protect your account:

1. Change your Apple ID password and choose a strong password—eight or more characters, including upper and lowercase letters, and at least one number.
2. Review all the personal and security information in your account. Update any information that isn't correct or that you don't recognize, including your name, your primary Apple ID email address, and phone number(s).
3. If you have two-factor authentication enabled, review your trusted devices on iOS, by going to Settings > [your name] and review the devices listed. If you see a device that you don't recognize or haven't authorized to use your account, you can select it and tap Remove from Account.
4. If you haven't yet, set up two-factor authentication by going to Settings > [your name] > Password & Security. You may be asked to enter your Apple ID password to access these features. Tap Turn On Two-Factor Authentication.

[Sign in with your Apple ID](#)

[Change your Apple ID password](#)

[If you forgot your Apple ID password](#)

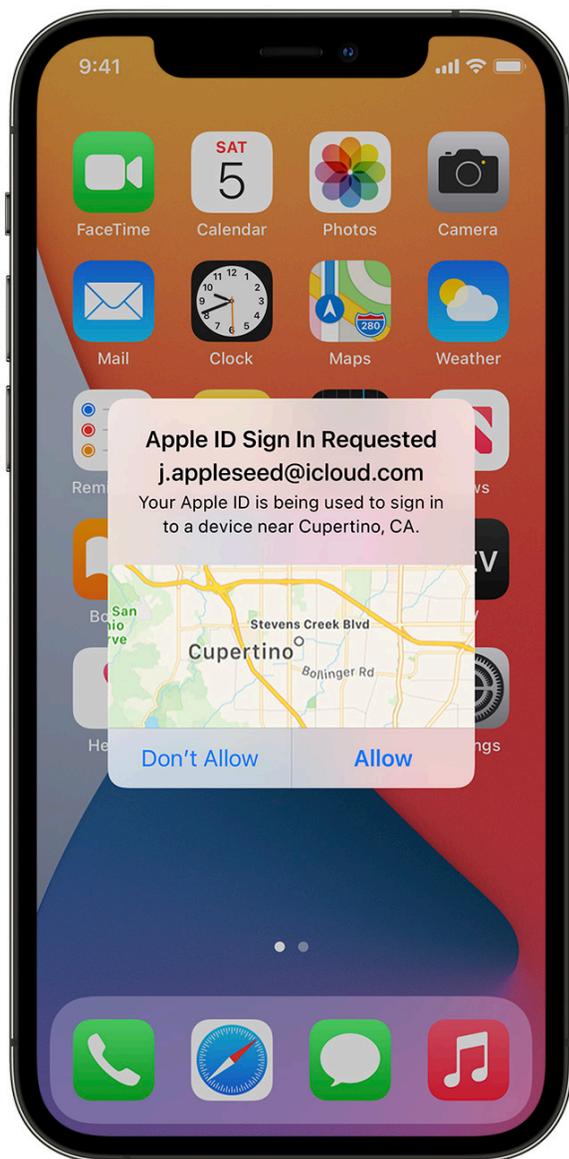
[Two-factor authentication for Apple ID](#)

[If you think your Apple ID has been compromised](#)

If you don't recognize a sign-in location

When you sign in on a new device, you get a notification on your other trusted devices. The notification includes a map of the location of the new device. 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.

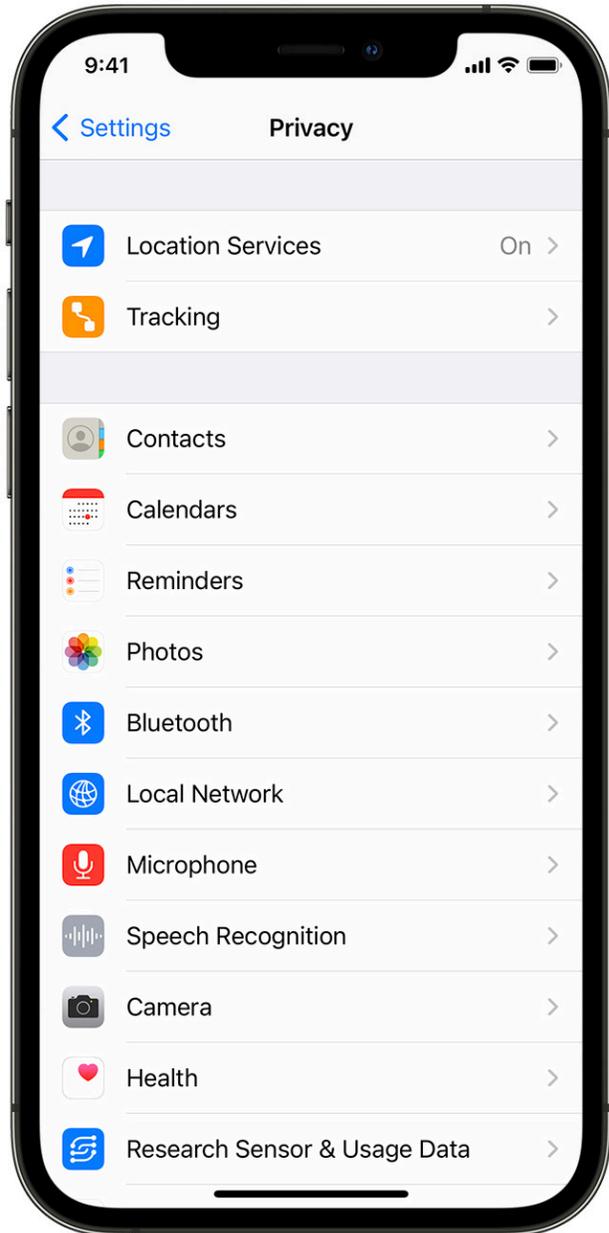


Check privacy settings

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. You can also grant access to Contacts so a messaging app can find any friends that are already using the same app.

In Settings > Privacy, you can see the apps you have allowed to access certain information—such as Location Services, Contacts, Camera, Files & Folders, and more—as well as grant or revoke any future access to this info.

Select a type of data from the list to see which apps have asked for permission to use that data. An app won'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.



Using the Find My app

The Find My app for iPhone, iPad, and Mac helps keep you connected to your device even if it's lost or stolen and allows you to share your location with friends and family members.

You can use Find My to locate your friends and family and to share your location—your location is not shared by default. Share My Location, in the Me tab, must be on to share your location with friends, family, and contacts.

To see people with whom you are sharing your location, go to the People tab. When someone shares their location with you, you can choose to share your location back, or not.

You can stop sharing your location with a particular person in the People tab. Just choose the person, scroll down and select Stop Sharing My Location. Or you can stop sharing with everyone by turning off Share My Location in the Me tab.

If you stop sharing your location in Find My, the person will not receive a notification, but they will not be able to see you on their list of friends. If you re-enable sharing, they get a notification that you have started sharing your location with them.

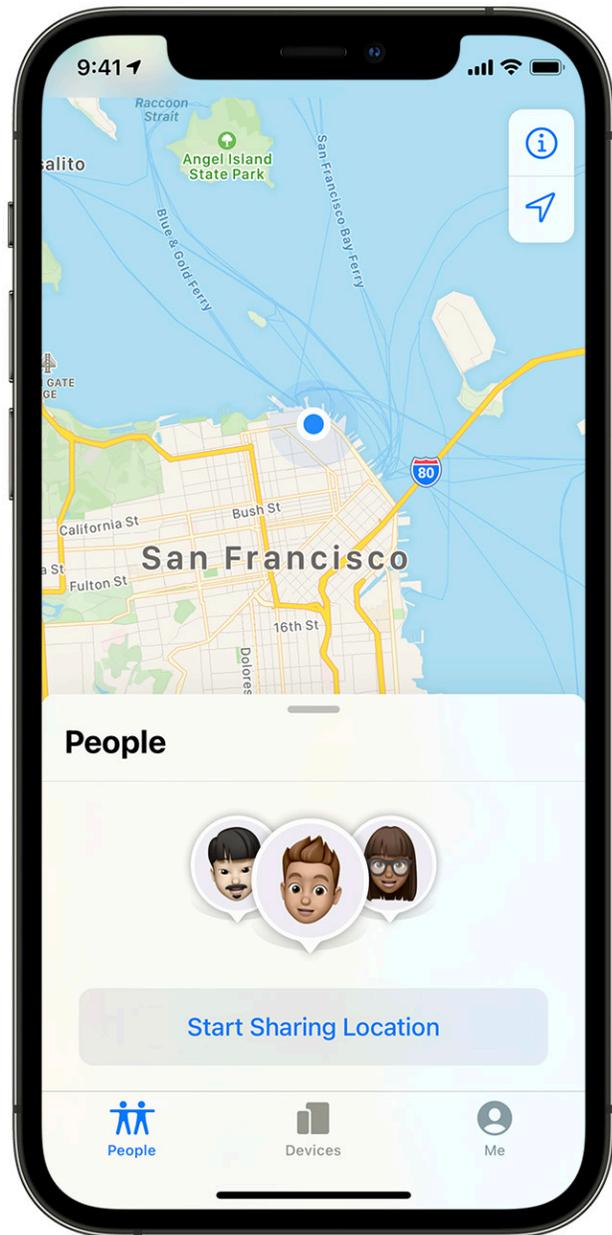
If you shared your location from iMessage rather than the Find My app, and you stop sharing, the person you stop sharing with sees a notification that you have stopped sharing your location.

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.

[Set up Find My on your iPhone, Mac, and other devices](#)

[Locate a lost or stolen device](#)

[Find friends and share your location with Find My](#)



Sharing your location

With your permission, Location Services allows apps and websites (including Maps, Camera, Weather, and other apps) to use location information, such as from cellular, Wi-Fi, Global Positioning System (GPS) networks, and Bluetooth to determine your approximate location. The first time an app tries to access your location, it must ask for your permission. You see a prompt explaining which app is asking for permission to use your location as well as the app developer's reason for requesting it.



To stop sharing your location with 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 features may not work as expected without access to your location.

In Settings > Privacy > Location Services, you can also grant access to your location for individual apps and indicate how often the app may use your location.

To stop sharing your location with friends through the Find My app, turn off the Location Sharing option in the Me tab in Find My.

Note: Your device's location information may be used for emergency calls to aid response efforts, regardless of whether Location Services is on.

[About privacy and Location Services in iOS and iPadOS](#)

[Manage which apps can detect your Mac location](#)

Sharing with iCloud

iCloud securely stores your photos, videos, documents, music, apps, and more and keeps them updated across all your devices. iCloud also allows you to share photos, calendars, your location, and more with friends and family.

You sign in to iCloud—on your device or the web— with your Apple ID. See detailed information about [what is stored in iCloud](#).

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

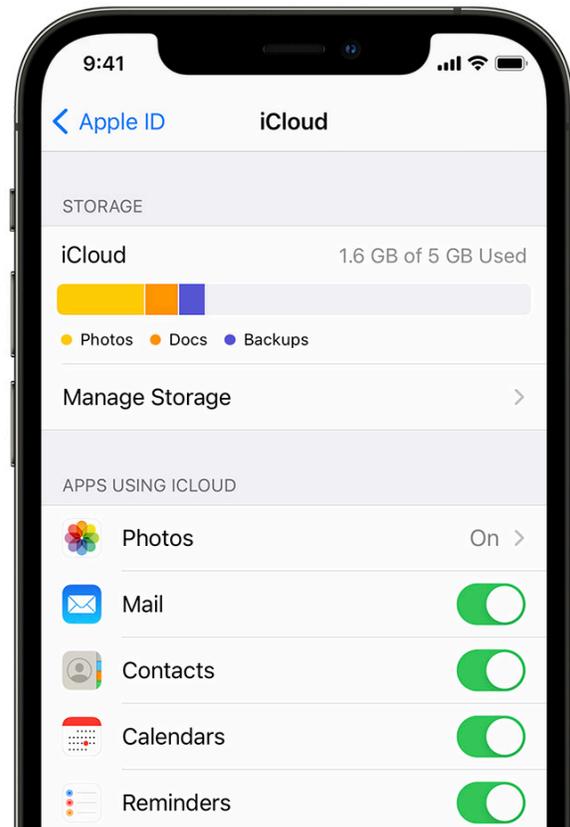
- On your iPhone, iPad, or iPod touch, go to Settings > [your name] > iCloud.
- On your Mac, go to System Preferences > Apple ID > iCloud.

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, go to Settings > [your name], scroll down and tap Sign Out.
- On your Mac, choose Apple menu > System Preferences. Click Apple ID, then click Overview, then click Sign Out.

[Change your iCloud feature settings](#)

[Sign out of iCloud on your iPhone, iPad, iPod touch, Apple TV, or Mac](#)



Shared Albums in Photos

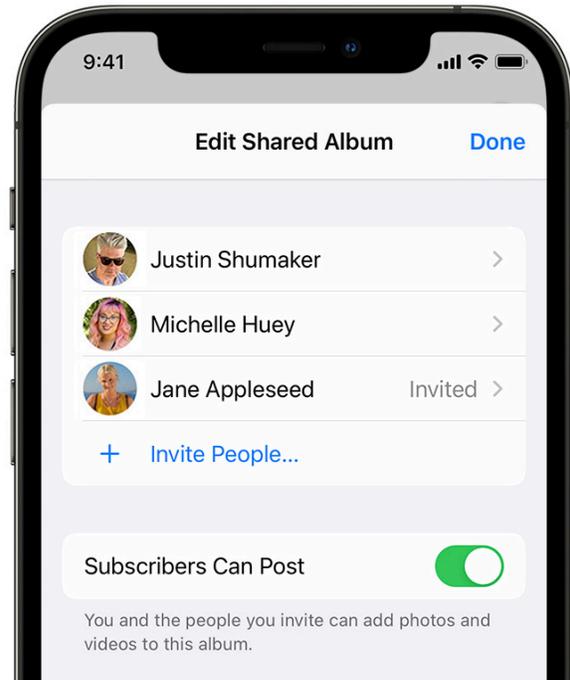
With Shared Albums in Photos, you choose the photos and videos you want to share, and the people you want to share them with. You can change your sharing settings anytime.

To see who you have shared albums with, go to Photos > Albums > Shared Albums. Select a shared album and tap the People tab to see the owner of the shared album and who the album is shared with.

If you are the album owner and would like to stop sharing, tap the name of the subscriber for options.

If you are a subscriber to a shared album, you can delete any photos that you shared. You can also select Unsubscribe from the bottom of the screen. If you stop sharing a photo or an album with someone, they will not receive a notification.

[How to share albums in Photos](#)



Shared Calendars

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

To see who you have shared a Calendar with, go to Calendar > Calendars. Select a shared calendar and tap the Info icon to see who the album is shared with.

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 from the bottom of the screen.

[Share iCloud calendars on iPhone](#)

[Share iCloud calendars on Mac](#)

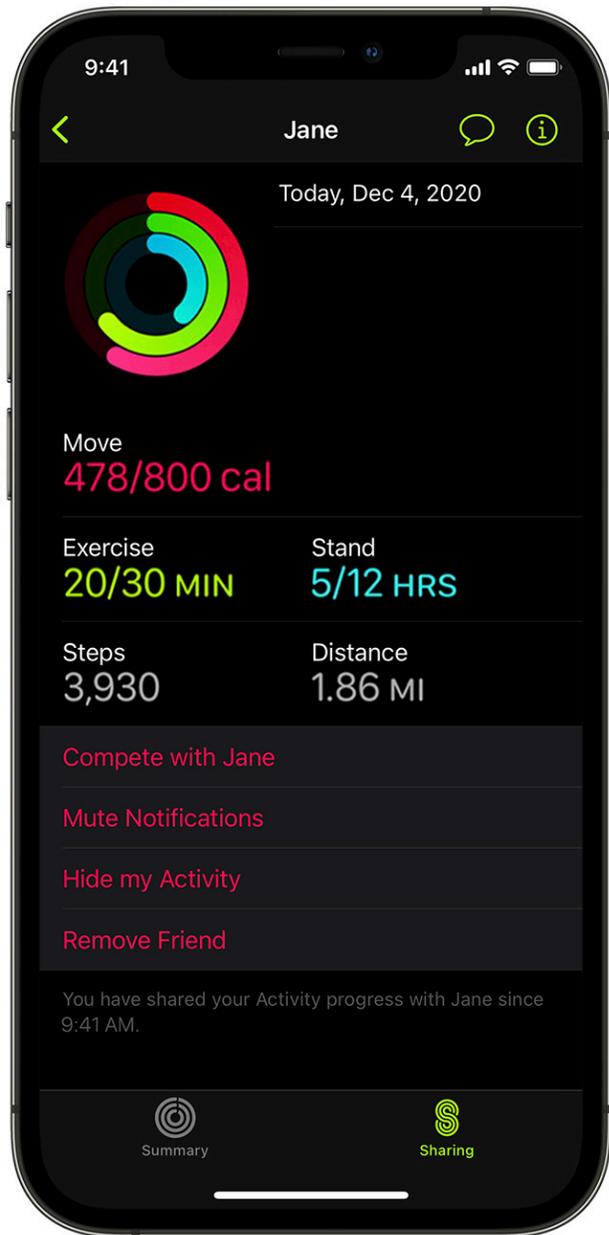


Sharing your Activity with Apple Watch

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. There are no notifications if you stop sharing your activity.

[Share your Activity and compete with friends with your Apple Watch](#)



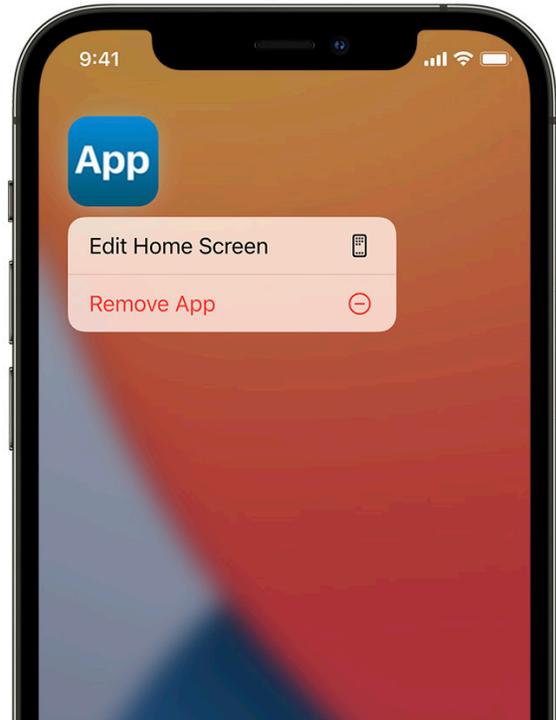
Delete unknown third-party apps

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.

To delete an app on your iPhone, iPad, or iPod touch, touch and hold the app. Tap Remove App. Tap Delete App, then tap Delete to confirm.

[How to delete apps on your iPhone, iPad, and iPod touch](#)

[How to delete apps on your Mac](#)



Delete unknown configuration profiles

Device profiles, Mobile Device Management (MDM) tools, and custom apps may be used by companies or educational institutions to manage devices, and these tools may allow access to data or location information on the device.

If you see a profile installed on your device, and don't know of any reason for it, you can remove it and delete any associated apps. If your device belongs to your school or organization, check with your system administrator before deleting a necessary app or profile.

To remove a profile or MDM configuration from your iPhone, iPad, or iPod touch, go to Settings > General > Profiles & Device Management.* Select the profile, tap Delete Profile, and follow the onscreen instructions. Restart your device.

On your Mac, go to System Preferences, then click Profiles. Click the suspicious profile to select it, then click the Remove button (-) below the list of profiles. Click Remove to confirm. Restart your Mac.

*If you don't see this option in Settings, then no device management profiles are installed on your device.

[How to delete an app that has a configuration profile on your iPhone, iPad, or iPod touch](#)

[Use configuration profiles to standardize settings on Mac computers](#)



If you use Family Sharing

If you want to share purchases, photos, a calendar, and more with someone else, you can use Family Sharing, Shared Albums in Photos, or other easy-to-use sharing features.

Family Sharing makes it easy to share—App Store, music, movie, TV, and book purchases, subscriptions to [Apple Music](#), [Apple Arcade](#), [Apple News+](#), or [Apple TV+](#), [iCloud storage](#), and much more—without sharing each other's Apple accounts.

One adult in your household, the organizer, chooses the features the family will share and can invite up to five additional members to join. After the family members join, Family Sharing is set up on everyone's devices automatically—including a shared calendar and shared photo album. The family organizer can add anyone who has an Apple ID to their family and remove anyone over the age of 13 from the family group.

You can check if you're already part of a family in Settings > [your name]:

- If you see Set Up Family Sharing, you are not 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.

If the family organizer turns off Family Sharing, it removes all family members from the family group at once. If there are children under 13 (age varies by country/region) in the family group, you must transfer them to another family before you can disband yours.

Also, any family member over the age of 13 can remove themselves from a family group at any time. Just tap your name and then tap Leave Family. You can also sign in to appleid.apple.com and choose Remove Account in the Family Sharing section.

For security reasons, a child (under 13) account cannot remove themselves from a family and cannot stop sharing details such as Screen Time without the Screen Time passcode. If you use a child account, the family organizer has access to shared family content on your device, such as shared photo albums and shared calendars, and can view Screen Time activity.

[Family Sharing](#)

[Leave Family Sharing](#)

Phishing and fraudulent requests to share info

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

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.

You can use the tips at the page below to avoid being tricked into compromising your accounts or personal information.

[Recognize and avoid phishing messages, phony support calls, and other scams](#)

Checklist: If you want to see if anyone else has access to your device or accounts

- 1** Check which devices are signed in with your Apple ID by going to Settings > [your name]. If you see a device you don't recognize, tap the device name and select Remove from Account.
- 2** Check to see if there is an unexpected alternate appearance or additional fingerprint set up on your device by following the instructions to [use Face ID on your iPhone or iPad Pro](#) or [use Touch ID on iPhone and iPad](#).
- 3** Sign in to appleid.apple.com with your Apple ID and review all the personal and security information in your account to see if there is any information that someone else has added. Make sure all your information is up to date. If you have two-factor authentication turned on, review trusted devices for any devices that you do not recognize. If your account doesn't use two-factor authentication, [turn it on](#) now.
- 4** 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.
- 5** Mobile Device Management (MDM) profiles are typically installed by employers, schools, or other official organizations, and allow additional privilege and access to a device. Look for an unknown MDM profile on your iPhone, iPad, or iPod touch in Settings > General > Profiles & Device Management. If you don't see this option in Settings, your device doesn't have any profiles installed.

Checklist: If you want to stop sharing with someone whom you previously shared with

- 1** Check Family Sharing settings by going to Settings > [your name]. If you're in a family, the names of the family members are visible. If you're part of a family, you can remove yourself from the family group as long as the account lists your age as over 13. If you're the family organizer, you can remove anyone over the age of 13 from the family.
- 2** In the Find My app, select the People tab to see with whom you share your location. Tap a person and tap Stop Sharing My Location, or to stop sharing with everyone, turn off Share My Location in the Me tab.
- 3** In the Photos app, go to Albums and then go to Shared Albums. Select a shared album and tap People to see the owner of the shared album and with whom the album is shared. If you're the album owner, tap the name of a subscriber for the option to remove them. If you're a subscriber, select Unsubscribe from the bottom of the screen. You can also delete any photos that you shared.
- 4** In the Calendar app, select Calendars. Select a shared calendar and tap Info to see with whom the album is shared. If you're the calendar owner, tap the name of the subscriber for the option to remove them. If you're a subscriber, you can tap Delete Calendar from the bottom of the screen.
- 5** If you have an Apple Watch and shared your Activity rings with someone, you can choose to stop sharing. In the Fitness app on your iPhone, tap the Sharing tab. Tap the person icon to see who you share with, click on the person's name and select either Remove Friend or Hide my Activity.
- 6** You can choose to share information with others through third-party apps as well. Review the apps that you installed on your device to see if any of them are sharing information, and follow their instructions to stop sharing. You can also delete the app.
- 7** If you're not running the latest version of iOS and have concerns that someone else may have had physical access to your device, or if someone else set your device up for you, you can backup the information from your device and restore it to factory settings. Learn [how to back up your iPhone, iPad, and iPod touch](#) and [how to erase your iPhone, iPad, or iPod touch](#).

Checklist: If you want to make sure no one else can see your location

- 1** To stop sharing your location with apps and services, for even a short period of time, go to Settings > Privacy > Location Services and turn off Location Services. This stops apps on your device, such as Maps, from using your location. No one is notified when you turn off location services, but some features may not work as expected without access to your location.
- 2** If you need to use certain apps that require location permissions, such as Maps or ride sharing apps, you can give app permission individually by going to Settings > Privacy > Location Services and allowing only certain apps to use location services.
- 3** To Stop sharing location in the Find My app, go to Settings > Privacy > Share My Location and turn off Share My Location. If you're concerned someone may have access to your Apple ID, you can also temporarily turn off Find My iPhone in this tab.
- 4** You can stop sharing your location with a particular person by going to the Find My app, going to the People tab, select the individual and tap Stop Sharing My Location. If you stop sharing your location in Find My, the person will not receive a notification, but they will not be able to see you on their list of friends. If you re-enable sharing, they get a notification that you have started sharing your location with them.
- 5** You can also choose to share your location with others using third-party apps. If you haven't turned off Location Services in Privacy Settings, conduct a review of apps you have installed on your device to see if any of them are sharing your location, and follow the relevant instructions to stop sharing.