Understanding Your iCloud Data

Compiled by the Clinic to End Tech Abuse

Last Updated: December 9th 2022

Who is this guide for?
The information in this guide is intended for those who:

- Have an Apple device connected to an iCloud account (iPad, iPhone, iMac, Macbook)
- **AND** suspect an abusive person may have access to their iCloud account
- **AND** do not feel safe or comfortable removing the abusive person's access due to the threat of violence or some other reason
- Would like fine-grained control over what information is shared with iCloud

If you **do** feel safe in securing your iCloud and are looking for general safety information, then this is **not** the correct guide. **This guide will not provide information about removing an abusive person's access or securing your account. You should read our General iCloud Safety Guide instead as not all information in that guide is included here.**

What does this guide cover?

- **Reviewing who might have access to your iCloud or other sensitive information**
- **Reviewing applications that share information to your iCloud**
- **Turning off and on sensitive location settings**
- **Information about stalkerware**
- **Tips for device safety**

Aspects to take into account

- If you are concerned about the threat of violence, you can search for a local agency, call the hotline, or chat with someone at https://thehotline.org to help make a plan for your safety. Please keep in mind that if you are concerned about someone monitoring your Internet or phone usage that visits to the Hotline and other organizations may be visible.

- Some steps in these guides may, directly or indirectly, notify an abuser of your actions. For example, they may receive an alert that you have changed a password or notice that they can no longer read your messages.
  We have marked steps that may be visible to an abuser with this sign:

Be careful!

This action could be visible to the abuser

- This guide links to official Apple guides for up-to-date, step-by-step instructions. CETA guides provide supplemental information for the unique concerns related to IPV. Where we have provided both external links and our own instructions, reading through both sets of instructions may help you make the best decision for your situation.

- All images included in this guide are for educational purposes only.

Table of Contents

Introduction

iOS refers to an operating system developed by Apple for mobile devices. An operating system is the non-physical software that runs on the physical device and makes it work. iOS can only run on physical devices made by Apple, such as iPhones and iPads.

This guide is based on how your iCloud settings should look if you're using version 16.05 of iOS on an iPhone 14. If you are using an iPad, or a different version of iOS, the screenshots may not reflect exactly what you see on your device. Nonetheless, we have made an effort to develop a guide that is as general as possible. The guide also includes a section for checking iCloud settings using a web browser.

Shared Phone Plans

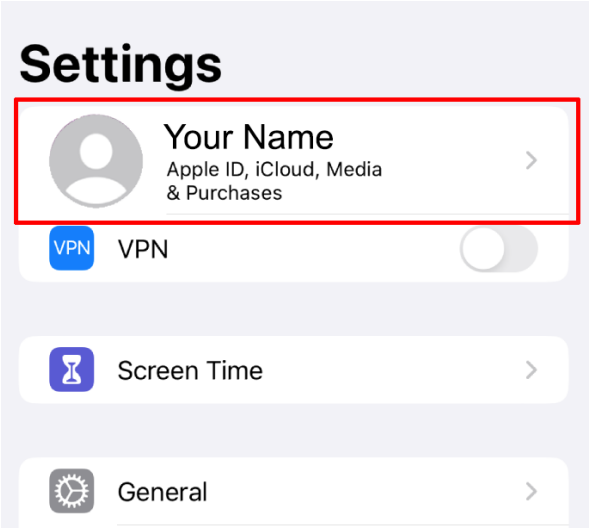
If you are concerned that someone seems to be able to access information in your phone without your permission, you should be aware that if you share a phone plan with that person, they will be able to have access to information about what your phone is doing, especially if they are the account holder. Anyone who has either access to your phone plan information or is the owner of the account can view information such as call logs, phone numbers of people who have been texted from that phone, and potentially other information.

The information in this guide can increase the security of your device, but it cannot prevent information from being accessed via a shared phone plan. The only solution is to leave the shared phone plan. The Safe Connections Act is a federal law requiring phone companies to allow survivors of domestic violence and their dependents to leave a phone contract. It requires documentation such as an attestation from a social worker or an order of protection. If you are interested in this option, please discuss it with a local domestic violence response professional.

Learn Who Has Access to Your iCloud

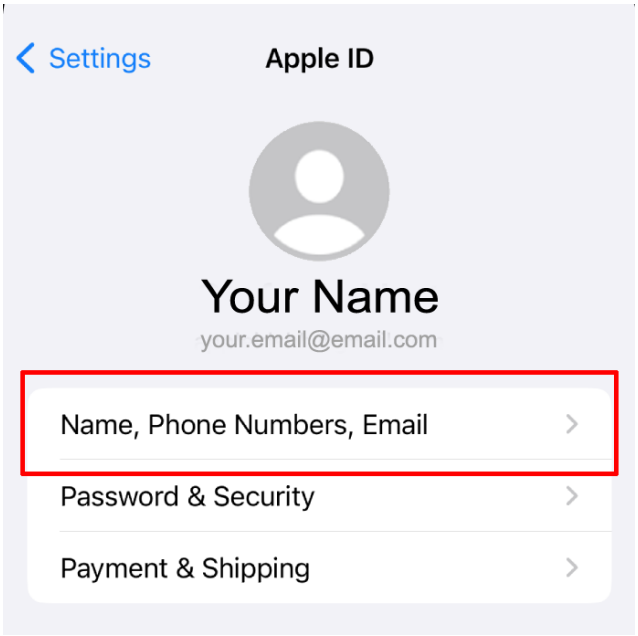
Confirm iCloud contact information

From the home screen on your phone, open Settings. Check that you recognize the name and image of the iCloud user in the Apple ID section at the top.



⚠️**Warning!** If you do not recognize the Apple ID, it means that someone else is signed in to your device from their iCloud account.

Next, tap on the name to open the Apple ID Menu, and tap >**Name, Phone Numbers, Email.**



Check that any email addresses and phone numbers in the **“Reachable At”** section are yours. Apple can send account-related information to these email addresses and numbers. Whoever controls these numbers or has access to these emails may have access to your account

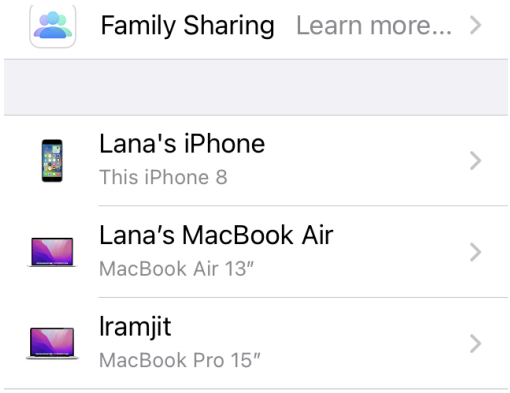
You may remove unwanted contact information from this menu, but it is **highly** visible to an abusive person. If you would like further instructions on removing devices and securing your account, we suggest you read our general iCloud Safety Guide.

Check which devices are connected to iCloud

For the purpose of this guide, devices are smartphones, tablets, laptops, or other electronics that can connect to the internet. If another device was previously used to log in to your iCloud account, then Apple trusts that device to gain entry to your iCloud account and manage it.

Navigate to the Apple ID menu (by going to Settings and then tapping on the icon with your name and photo).

Scroll down until you see a list of devices. These are the devices where your Apple ID is being used to sign into iCloud. Click on each listed device to see more information about it.



⚠️ You may remove unwanted devices from this menu, but it is **highly** visible to an abusive person. **If you would like further instructions on removing devices and securing your account, this is not the correct guide. We suggest you visit our General iCloud Safety Guide.**

Checking if text messages are being forwarded

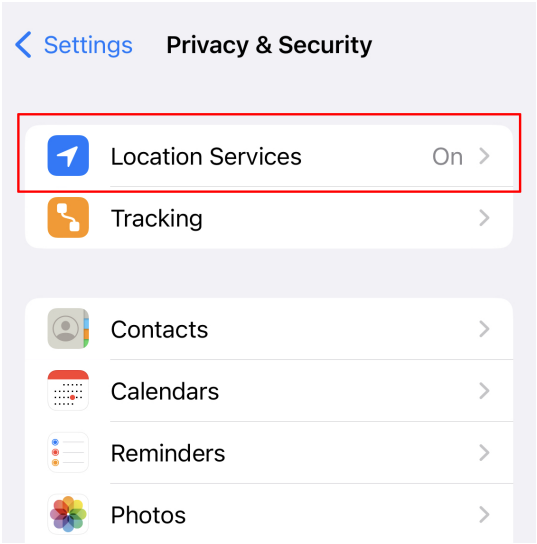
If someone has had physical access to your device, they can set up text forwarding that will persist even after you have secured your AppleID. This will affect SMS text messages (which usually show up in green, unlike iMessages which are blue and not affected by this setting.)

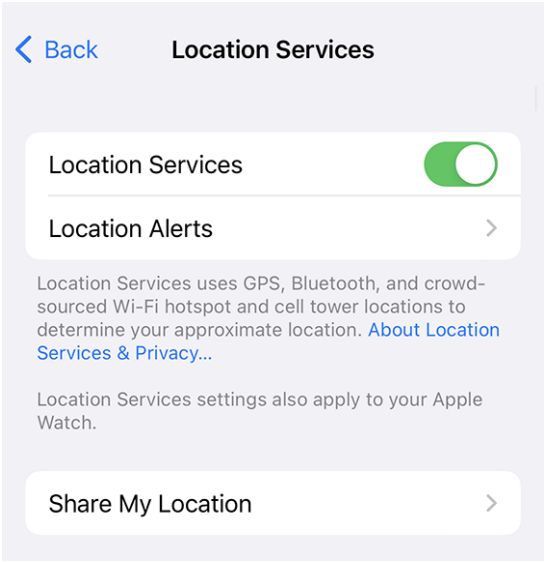
To check your iMessage forwarding settings, go to **Settings > Messages**. Then examine the information under **Send & Receive** and the devices under **Text Message Forwarding.**

Location Sharing Settings

Review "Location Services" settings

Location Services use a combination of GPS, Bluetooth, Wi-Fi, and cell-tower signals to determine the location of your devices and share them with apps. If an abuser has access to your iCloud account, and you cannot secure your account using the steps in the previous section, they may be able to see your location or location history.





To manage Location Services, go to **Settings > Privacy & Security.** Next, tap **Location Services** to check if they are turned on or off for the device.

⚠️**Important! While disabling location services temporarily will not immediately notify an abusive person, they may notice that they can no longer see your location if they are actively monitoring it.** If Location Services are **OFF**, the following will also be true:

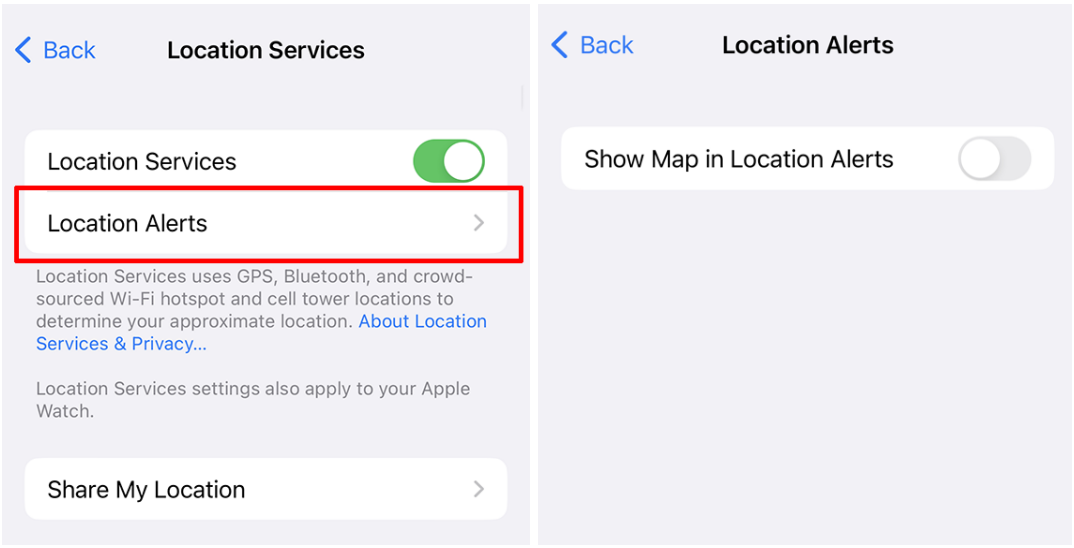
- If someone has access to your iCloud, they are still able to find your device's location.
- Without Location Services, your device will not alert you if AirTags are nearby. See the section about checking for nearby AirTags.
- Common services such as navigation or rideshare apps may not function normally.

Manage location settings for individual apps

To turn Location Services off for specific apps only, click “Back” to go to the “Privacy & Security” screen. From here, you can tap on each app to manage its location settings individually.

In addition, there is a setting that controls if your iCloud-connected devices can receive alerts about your location. **These alerts might also include a map of your location.**

To check this, go to Location Services > Location Alerts from the Privacy & Security screen. From here, you can switch “Show Map in Location Alerts” to the off position.



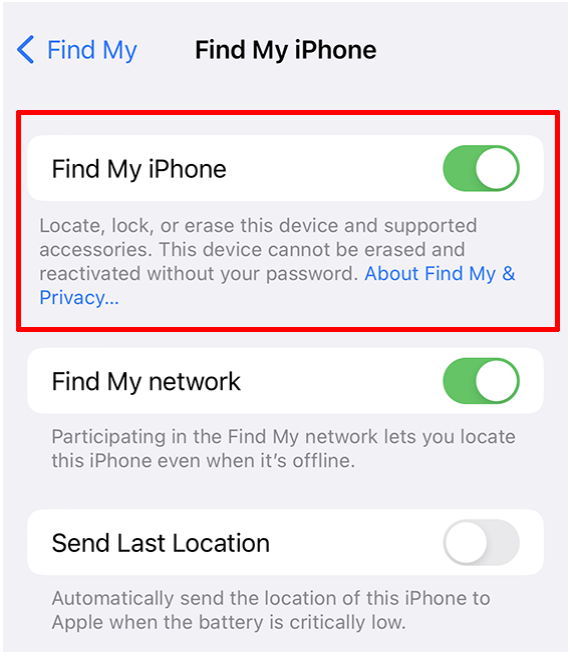
For more information about the Share My Location setting, see the section on “Find My” below.

Review “Find My” settings

Find My is an Apple feature that lets you track the location of your device, as well as lock and erase it remotely if you lose access to it. In addition, Find My can share your location with other people via Messages and the Find My app.

From **Settings > Apple ID**, tap **Find My**.

At the top of the screen, it will say whether Find My iPhone is “On” or “Off.”



To change your Find My settings for your current device, click on “Find My iPhone” to toggle the switch on (green) or off (gray).
⚠️**Warning! Turning Find My OFF will prevent you from finding your device if it is lost or stolen**. It will also be visible to anyone actively tracking your location, although you may turn it back on later. You will also not receive potentially important notifications about unwanted AirTag tracking. See the section about checking for nearby AirTags.

Manage who you share your location with

Return to the Find My screen and find the switch for “Share My Location.” This setting lets you share your device’s location *with other people,* via iMessage or the Find My app. It does not impact whether you are sharing location with apps.

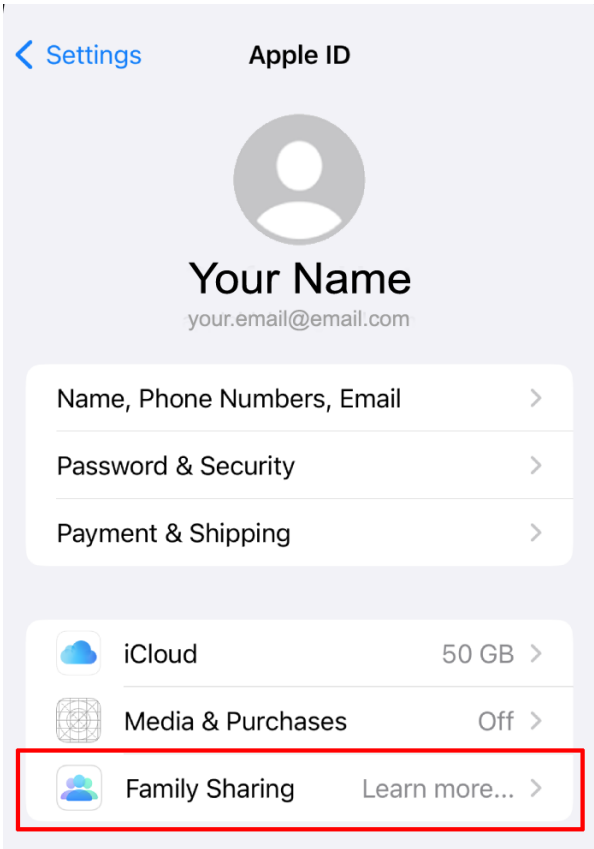
If Share My Location is **ON**, a list of the people you are sharing your location with will be visible at the bottom of the screen. If you don’t want to share location data with other people this way, turn Share My Location **OFF**. You may also remove people from this section individually.

For more information about Find My, see Apple’s guide: [Use the Find My app to locate a missing device or item - Apple Support]

Check “Family Sharing” settings

Family sharing allows you to share Apple purchases, photos, iCloud storage, and your location with up to five other people.

To check if Family Sharing is turned on, go to Settings > Apple ID



If Family Sharing is turned off, it will say “Learn more…” as pictured above.

If Family Sharing is turned “On”, click into it, and then click “Shared Features” to check what information is being shared.

From here, you can turn specific Family Sharing features on or off and manage who has access to them by following the steps below.

To remove yourself or another person from Family Share Settings, follow the instructions on Apple’s guide: Leave Family Sharing - Apple Support. Anyone who is removed will lose access to shared purchases and media.

To learn more about all of the features of Family Sharing, see Apple’s guide on What is Family Sharing? - Apple Support

Check for nearby AirTags

iCloud can alert people of unwanted Apple AirTags that are moving with them. If you are concerned about being tracked by an AirTag, consider enabling the settings on Apple's support guide to be notified if an AirTag is nearby.

Check if Apps are Sending Information to iCloud

If you have reviewed who has access to your iCloud and you are comfortable with who has access to your iCloud account, then there is no danger in having applications send information to your iCloud.

However, **if you believe an unauthorized or abusive person may have access to your iCloud** and are unable to secure the account using the above steps, then it is important to know which applications have been sending information to your iCloud.

Check iCloud app settings

The apps on your device can send information to iCloud, which means that other devices sharing the same Apple ID can access the apps and information. Connected devices can share information to iCloud even if the device is turned off.

Go to **Settings > Apple ID > iCloud** and click **Show All.**

Review the list of apps under Apps Using iCloud and make sure you recognize all of them.

If an app is “On” then this means that it is backing up copies of its information to your iCloud. For example, if the Notes app is “On” that means anyone with access to your iCloud account can see copies of your Notes.

⚠️**Warning!** If you write down sensitive information in your apps (such as storing passwords in Notes) and they are synced to iCloud, anyone with access to your iCloud can view this information.

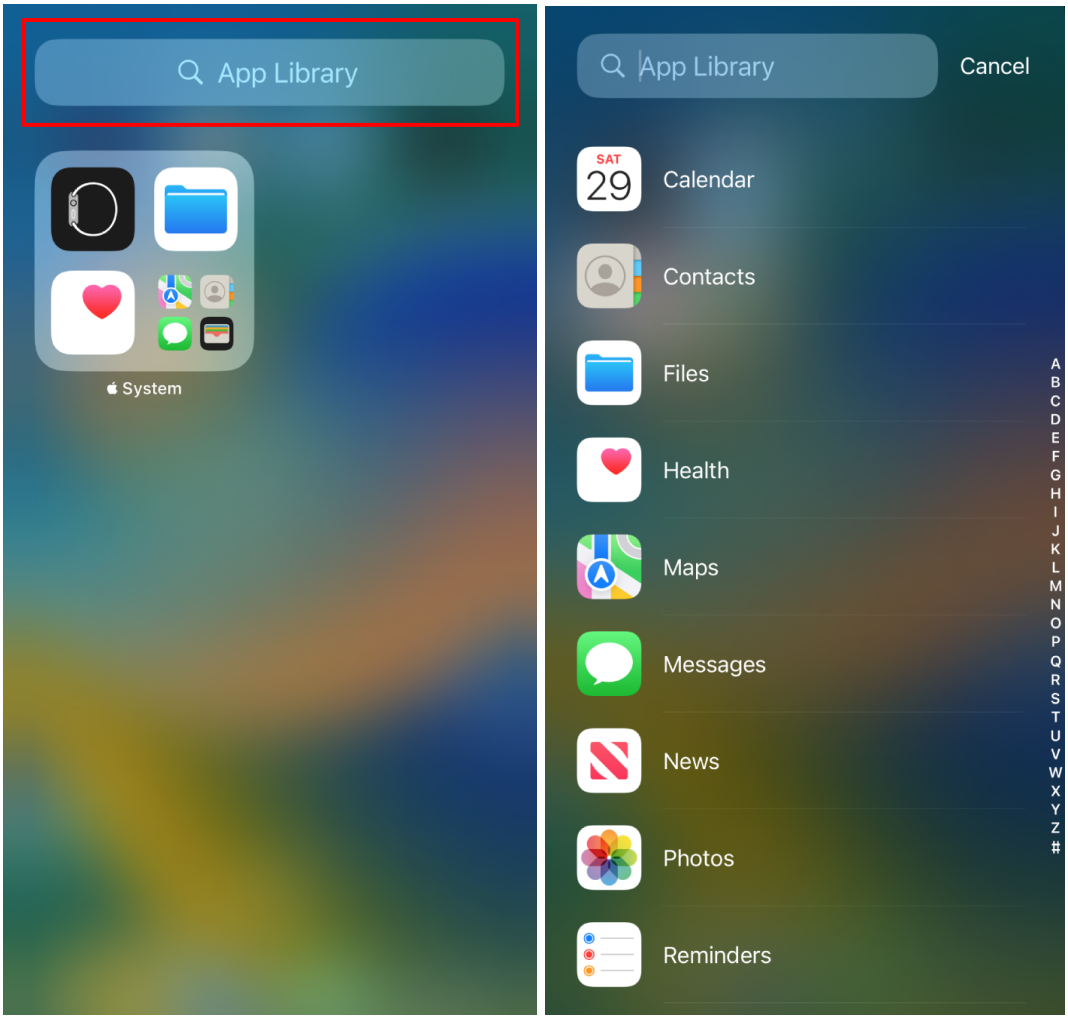
You can turn off the connection between an app and iCloud by clicking into it and changing “Sync this iPhone” to the “Off” position.

If you stop syncing an app with iCloud, you will lose access to information on that app from other devices. For example, if you have Notes on other devices that are synced to iCloud, they will be removed from your current device. However, they will remain on the device they were created on, and other devices that are synced.

Check App Library for unrecognized apps

Some apps might not be visible from the Home screen of your device. This could be the case if they were deliberately hidden by someone with physical access to your device, or if they are being used as stalkerware. For information about stalkerware, see the Information about stalkerware section at the end of this guide.

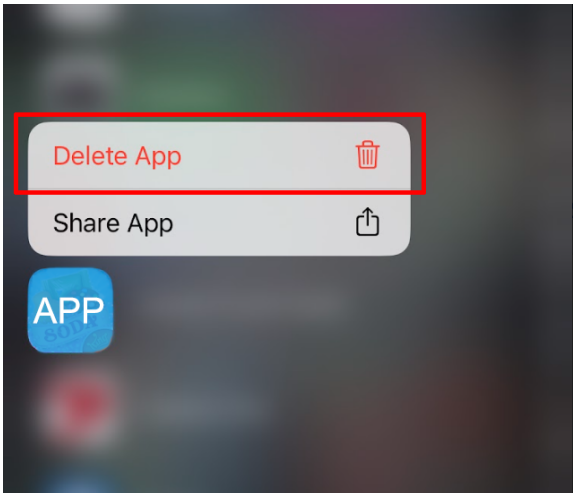
To view all of your apps, you can use the App Library by going to your Home screen and swiping left until you see the App Library screen. Click into the Search bar (where it says “App Library”) to view all your downloaded apps.



Be careful!

This action could be visible to the abuser

To delete an app, tap and hold the icon until a menu appears, then select “Delete App.”



You can not delete the Apple apps that come with your device. For example, if you try to delete the “Contacts” app it will only remove the app from your Home screen, and the app will remain in the App Library.

Deleting app data from iCloud

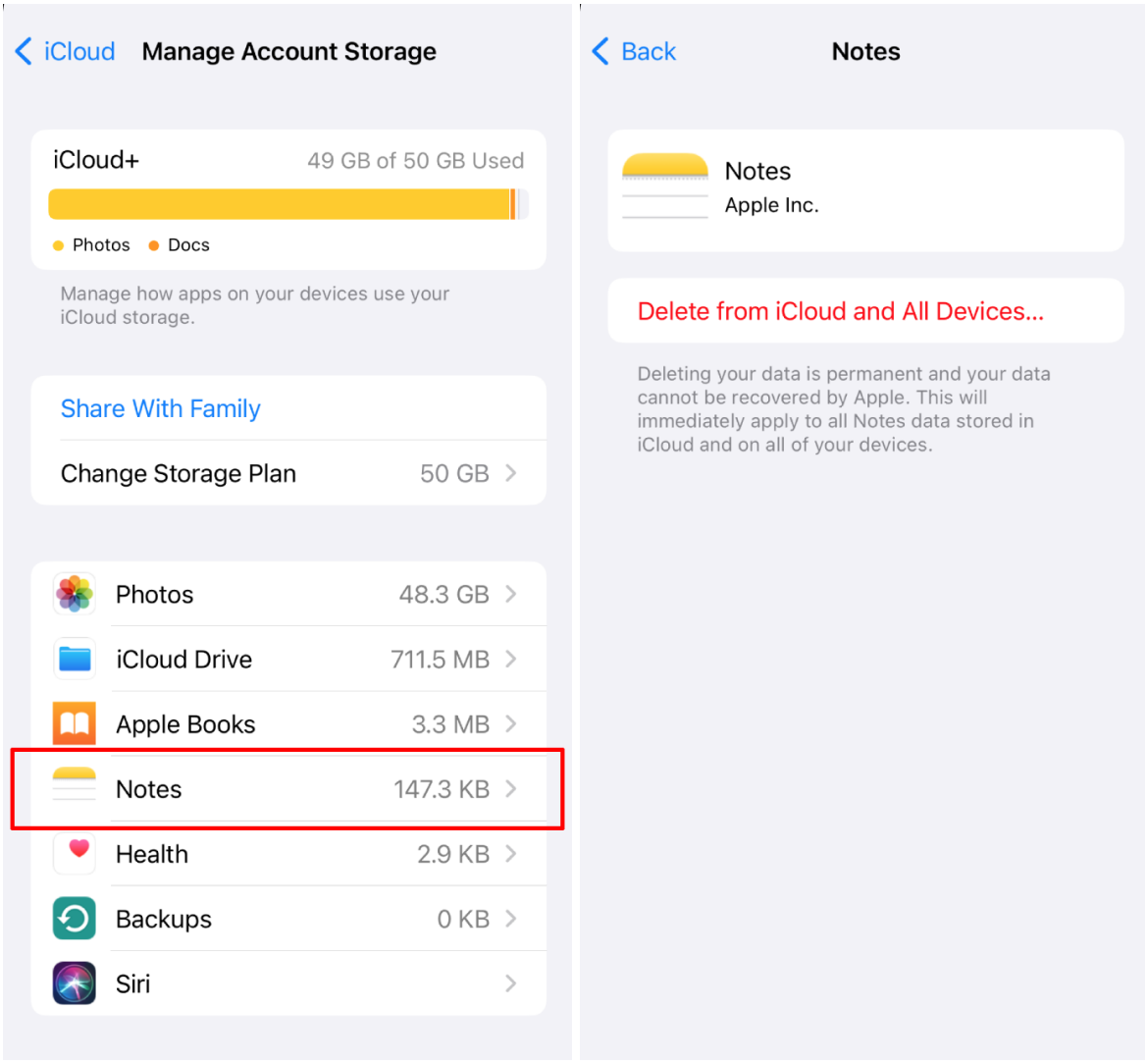
When you delete an app from your device, its data will still remain in iCloud if it had previously been sent there.

To check this, go to Settings > Apple ID > iCloud > Manage Account Storage

Be careful!

This action could be visible to the abuser

To delete data that is stored in iCloud, click into each app (for example, Notes) and look for the Delete option in red text.



⚠️**Warning!** Read the descriptions for each app carefully, since they could delete iCloud data in different ways. For example, deleting your iCloud Photos could also delete the Photos from your device.

Check “Photos” settings

The Photos app is a tool to organize, edit and share your pictures and videos. This content can be stored on your device, in iCloud, or both. If it is being sent to iCloud, then it is visible to anyone who has access to your iCloud account.

To check Photos iCloud settings, go to Settings > Apple ID > iCloud > Photos

If “Sync this iPhone” is switched on (green), then all the photos and videos in the Photos app on your device are being added to iCloud.

⚠️**Warning!** If Sync is turned on, then screenshots that you take on your device (such as for evidence gathering of a compromise) will also be sent to iCloud.

To stop syncing your Photos with iCloud, switch “Sync this iPhone” to the off position (gray).

For more information about Photos settings such as My Photo Stream and Shared Albums, see Apple’s guide: [Set up iCloud Photos on all your devices - Apple Support]

Check “Apple Home” settings

The Home app is designed to control a wide variety of smart home accessories, such as an Apple TV, home security cameras and more.

These settings can vary in complexity, depending on the number and type of devices that you have linked to Apple Home. If you are concerned about devices in your home, see the guide on Apple’s website to learn how to manage their settings: [Share control of your home - Apple Support]

What is Stalkerware?

Information about stalkerware

Stalkerware, also known as spyware, is software that is added to a device without the device owner’s knowledge. Once installed, a stalkerware app can extract information from the device and send it to an abuser. The biggest risk for stalkerware is if someone has physical access to your device and downloads the apps onto the device.

For iOS devices, stalkerware is usually downloaded directly from the app store and could be disguised as something innocent, such as an unrecognized sports app or baby monitor. It is important to check for apps that you do not recognize and delete them from your device.

To check for apps that could be stalkerware, see the section of this guide for how to check the App Library for unrecognized apps.

Actual spyware that is not in the form of an app is extremely rare. Apple devices have a "Lockdown Mode" for extreme use cases, such as for journalists or politicians who are targeted by highly sophisticated cyber attacks. To learn more, see Apple's guide About Lockdown Mode - Apple Support. Enabling this feature will greatly limit the functionality of your device.

Information about jailbreaking

Some stalkerware apps require the iOS device to be "jailbroken" in order to be downloaded. Jailbreaking requires physical access to the device, since it involves making changes to the iOS operating system (the software that runs the device). Normally, Apple phones can only download apps from the app store, so jailbreaking is usually done so that custom software can be downloaded to the phone.

If the apps "Cydia" or "Sileo" are installed on your device, that could be an indicator that it is jailbroken. These apps function similarly to the App Store, but can install unofficial software on your device, including stalkerware.

At the time of this writing, there is no reliable jailbreak option past iOS 14. The best defense against jailbreaking is to make sure that iOS is up to date (see next section).

⚠️**Warning!** If your device is jailbroken, updating the iOS version might cause the device to stop working.

Check if iOS is up to date

To learn what version if iOS your device is running on, and how to update it, see Apple's guide: Find the software version on your iPhone, iPad, or iPod - Apple Support

Other Tips for Device Safety

There are various apps that can help you identify security misconfigurations on your device. iVerify is one example (it can also check if your device is jailbroken). For more information, see iVerify | Frequently Asked Questions and iVerify. - Secure your Phone! on the App Store.

In some cases where an abuser has physical access to your iPhone, accessibility features can be exploited. For example, a feature to automatically answer calls might be enabled: Route and automatically answer calls on iPhone - Apple Support

In addition, you can check the settings for your device's Microphone, Camera, Bluetooth, and other connectivity features by going to Settings > Privacy & Security and clicking into each one to see how they are used by other apps.