iCloud General Safety Guide

Compiled by the Clinic to End Tech Abuse

Last Updated: December 9th, 2022

Who is this guide for?
If you are using an Apple device that has an iCloud account (iPhone, iPad, Macbook, or iMac), this guide will help you review important safety settings if you suspect that your account and/or device has been compromised by an intimate partner or close acquaintance.

What does this guide cover?

- **Shared phone plans**
- **Securing your iCloud**
- **Location sharing 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

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

Table of Contents

.

Shared Phone Plans

If you share a phone plan with another person, they will be able to have access to information about what your phone is doing, especially if they are the account holder. The owner of the account (or anyone authorized to manage 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.

iOS Safety Check Feature

Safety Check is a feature developed by Apple and available to certain iPhones and iPads that walks you through key steps to securing your device. If you are using iOS version 16 or later and have 2FA enabled, then you have the option to use Safety Check by going to Settings → Security → Safety Check.

Using Safety Check may alert an abuser if certain actions suddenly lock them out of your iCloud account or device. Examples include:

- Changing your Apple ID password
- Stopping location sharing from your device or apps
- Changing which devices are connected to your iCloud account
- Changing your device passcode (if someone has physical access to your device)

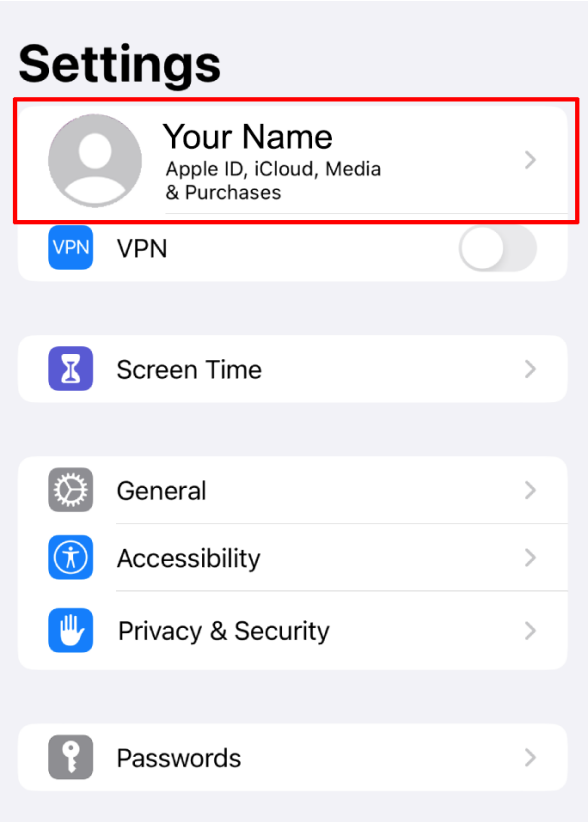
Instructions for using Safety Check can be found in Apple's guide: How Safety Check on iPhone works to keep you safe - Apple Support. If you do not have Safety Check on your device, you can use this guide to manage the same settings on your iOS device directly from settings.

Check iCloud Account Settings

Confirm iCloud contact information

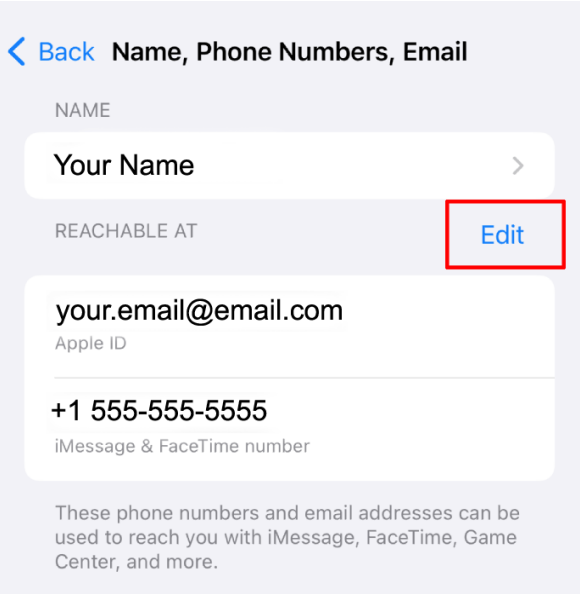
If the contact information on your account isn't yours, this could allow an abuser to see information on your phone or get access to the account, even if you change your password. We recommend checking these settings as a first step to securing your iCloud account.

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. To change the Apple ID email address, you must change it from a web browser.

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.

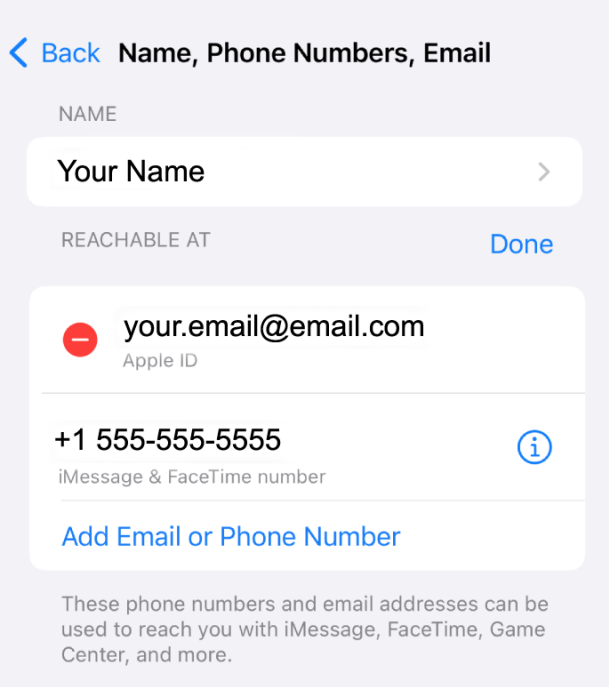
The email address that is listed as your AppleID can be used to recover your account or change your password. Even if the email address that is listed is yours, we recommend that you check the security of that email account as well by making sure you use a strong, secure password to access it. [See our guide on Google + Gmail Safety for more information.]

If you notice an email address or phone number that you do not recognize, you can change or remove it from your account. If someone else has access to your account and you remove their email or phone number, they will be locked out.

To change an email address or phone number, click "Edit" to the right of "Reachable At."
To **remove** an email address or phone number, select the red "minus" icon next to the one you want to remove. **If you are not comfortable removing an unfamiliar device due to the threat of violence, we strongly recommend reading through the information in our Understanding iCloud Safety Guide.**

- You can not remove the email that is associated with your Apple ID.

    - If the email that is associated with your Apple ID is an email that you suspect an abuser may have access to, you should take steps to secure that email address by changing the password or following the steps in our Gmail Safety guide.
- You can also change the email associated with your Apple ID by following the instructions to **Change your Apple ID**: https://support.apple.com/en-us/HT202667



When removing a phone number, you might be asked to sign out of Messages and FaceTime. If this happens, follow the steps below:

- Go to Settings > Messages > Send & Receive
- Select your Apple ID at the bottom of the screen and click Sign Out
- Go to Settings > FaceTime, select your Apple ID and click Sign Out

If the phone number you want to remove belongs to a phone that you can't access, you must change your Apple ID password to delete it. Changing your Apple ID password removes all phone numbers from your devices and will be known to anyone who previously had access.

⚠️**Warning!** When you remove a phone number from your iCloud account, previous calls or messages for the removed number will no longer appear on your devices. Keep this in mind if you want to collect a record of the activity.

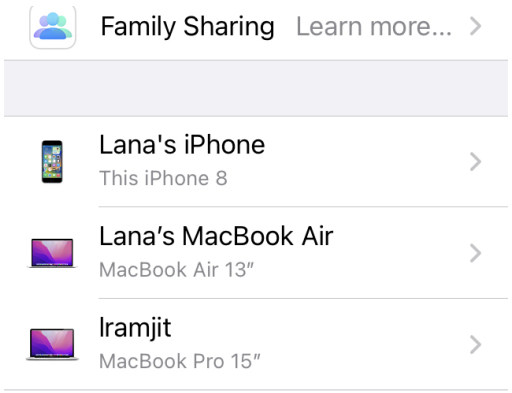
To add a new phone number or email address, click “Add Email or Phone Number.” You will need to have access to the new email address and phone in order to receive a verification code from Apple and confirm the changes.

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. If you do not recognize the device, you can click “Remove from Account” to disconnect it from your iCloud account. **If you are not comfortable removing an unfamiliar device due to the threat of violence, we strongly recommend reading through the information in our Understanding iCloud Safety Guide.**

If you decide to remove a device, you can also change your Apple ID password to keep someone else from logging into your account on that device again.

Secure Access to your iCloud Account

Be careful!

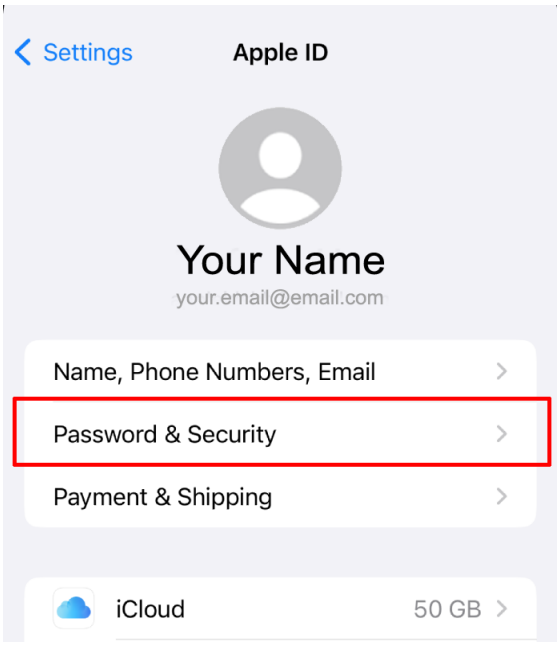
This action could be visible to the abuser

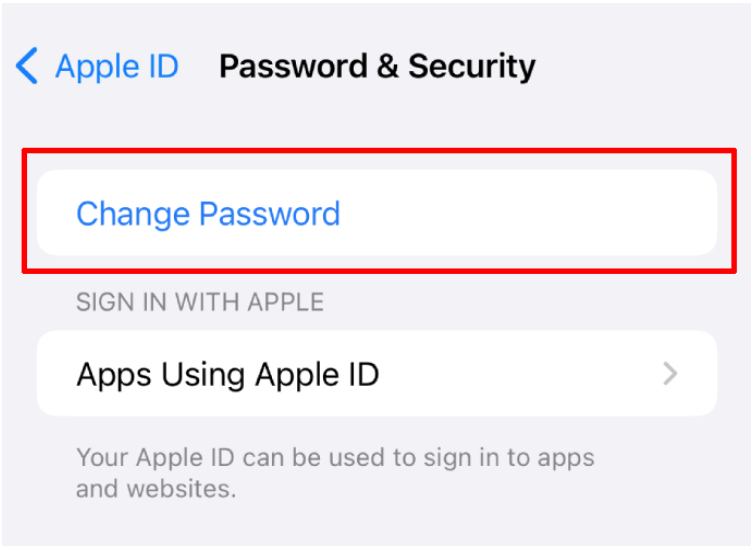
Changing your Apple ID password

Your password is the first line of defense against access to your iCloud account. Your Apple ID password is also your iCloud password.

⚠️**Warning!** If someone else has access to your account and you change the password, they will get locked out.

To change your password, go to Settings > Apple ID and click Password & Security.
Next, click Change Password. Apple may ask you to enter your device passcode to unlock the screen.





Enter your current password in the “Current” field, then enter your new password in the “New” and ”Verify” fields. When finished, click Change at the top right.

Tips for creating a strong password

- At least least 8-12 characters long
- Includes capital and lowercase letters
- Includes random numbers
- Includes some symbols such as !, ?, @, and $
- Do not use words or numbers that could be easy for someone to guess, such as a child's name, pet's name, or birthday

Keep your passwords in a safe, secure location, either written down on paper, or in a password manager if you are the only one with physical access to your device.

If you are unable to change your password from your device's Settings, you can try resetting it from a browser.

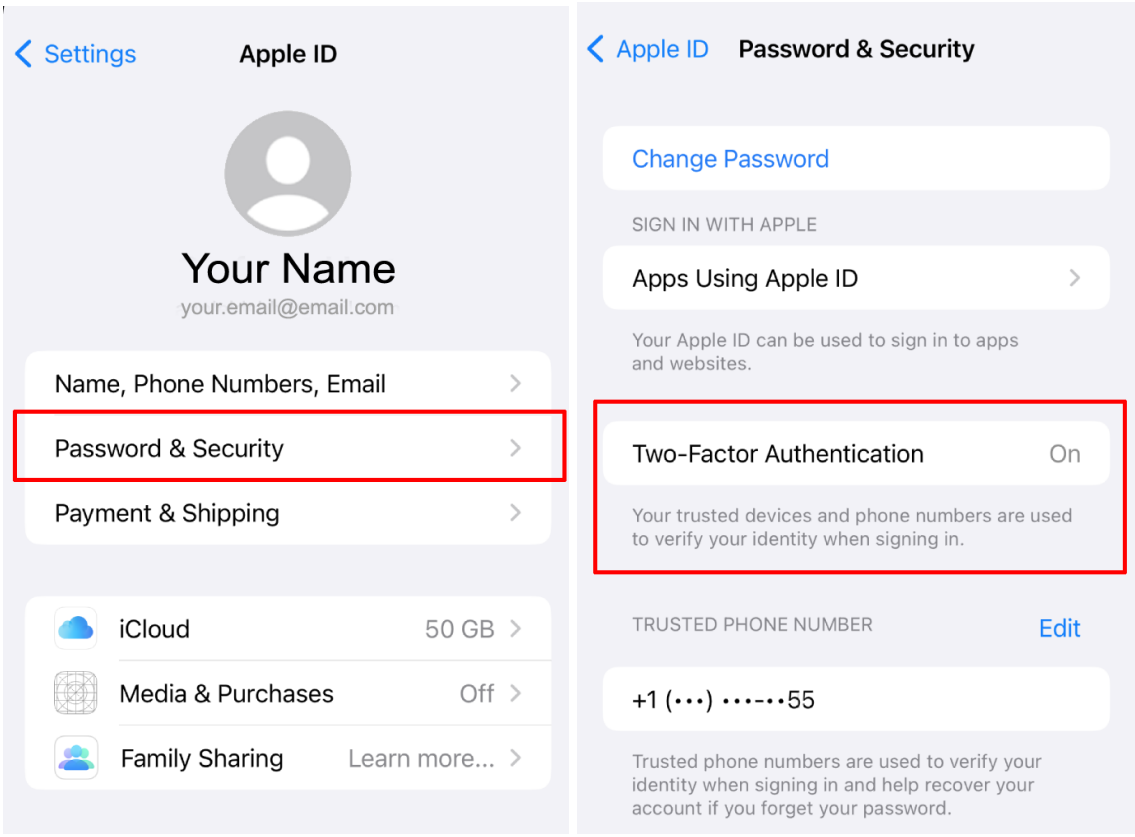
Enabling Two-Factor Authentication (2FA)

2FA adds an extra layer of security to your account. With 2FA, signing into your account will require both your password and a two-factor code, which Apple will send to your phone number or one of your trusted devices.

⚠️**Warning!** Turning on 2FA is an action that will be visible to anyone who has access to your devices.

Apple strongly recommends 2FA so you might not be able to turn 2FA off after it is on, depending on your device. However, you can always change the phone number and devices where 2FA codes are sent to.

To check your 2FA settings, click "Password & Security" from the Apple ID menu.



If 2FA is on, you will see a setting similar to the screenshot above. If 2FA is turned off, you will see an option to “Turn on Two-Factor Authentication.” Click this to turn it on.

Enter the phone number where you want to receive verification codes when you sign in. You can choose to receive the codes by text message or automated phone call.

Click “Next” to continue. You will receive a verification code at the number you chose. Enter the verification code to verify your phone number and turn on two-factor authentication.

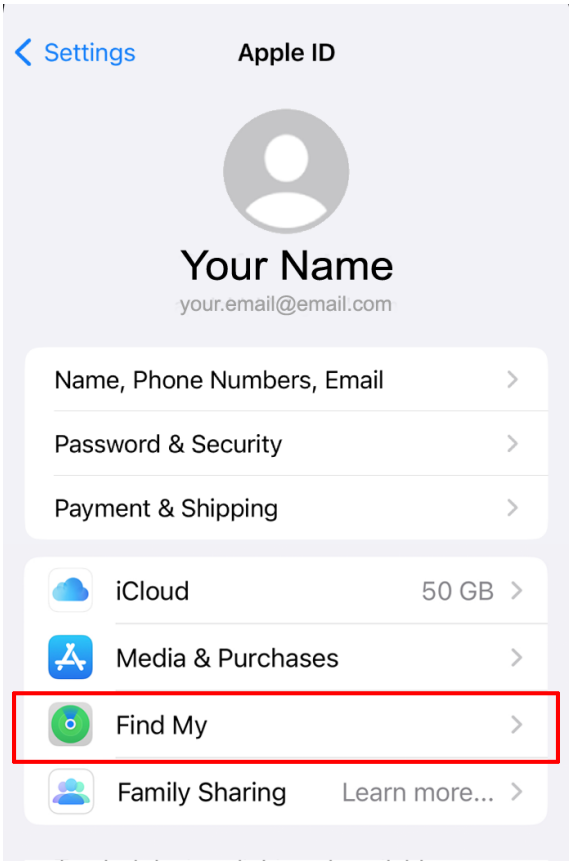
Apple’s 2FA guide can be found here: [Two-factor authentication for Apple ID]

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



Be careful!

This action could be visible to the abuser

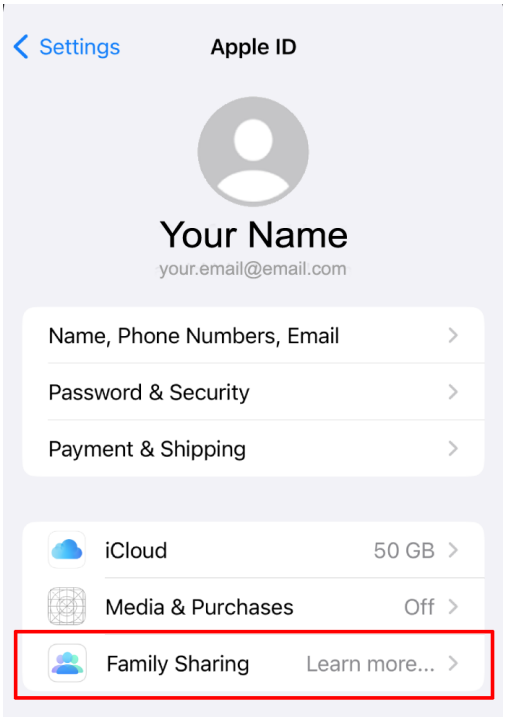
From **Settings > Apple ID**, tap **Find My**. At the top of the screen, it will say whether Find My iPhone is “On” or “Off.” Having Find My “On” is okay and even recommended for your safety as long as your iCloud is secure. If you believe your iCloud is not secure, then you may want to consider turning it off or review the information in our iCloud management guide.

On the Find My screen, make sure to review the information under "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**.

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

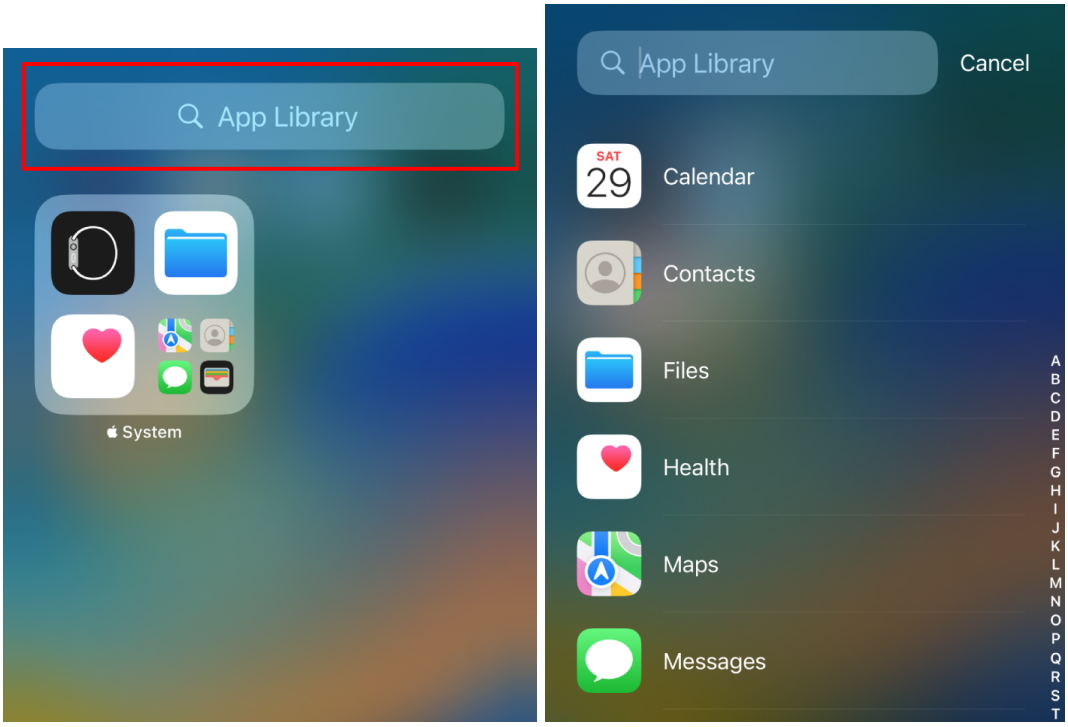
Check for nearby AirTags

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 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.

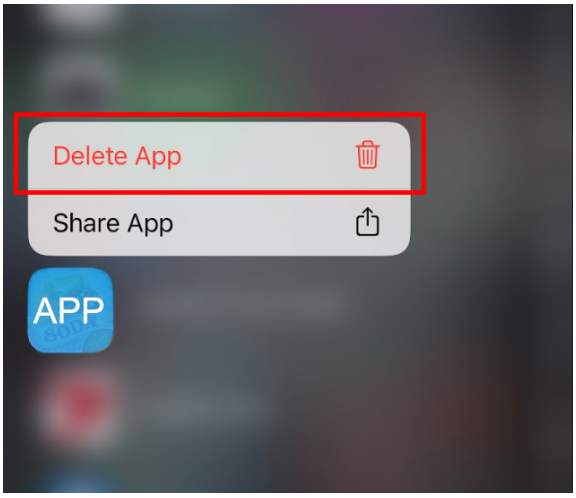
To view all of your apps, you can use the App Library by going to your Home screen and swiping left until you see the App Library screen. Click into the Search bar (where it says “App Library”) to view all your downloaded apps.



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.

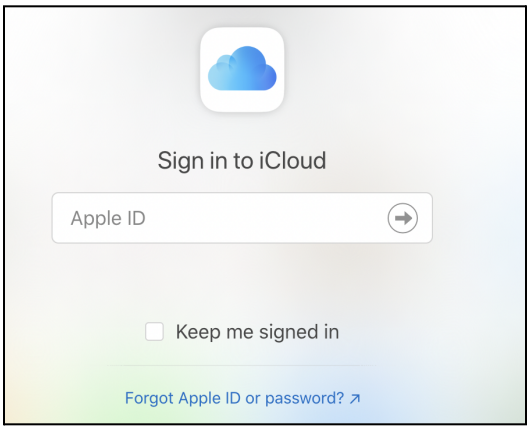
Manage iCloud Settings from a Browser

Apple also has a website that allows you to check various settings associated with your Apple ID account using your web browser. A web browser is an application to connect to the internet, such as Safari, Google Chrome, Firefox, or Edge. These are the same settings as in the previous sections. This section is designed for those who:

- Have an Apple laptop or iMac, but not an iPhone or iPad
- Are more comfortable navigating settings on a laptop or iMac rather than phone
- Want to recover their iCloud account
- Want change the email associated with their AppleID

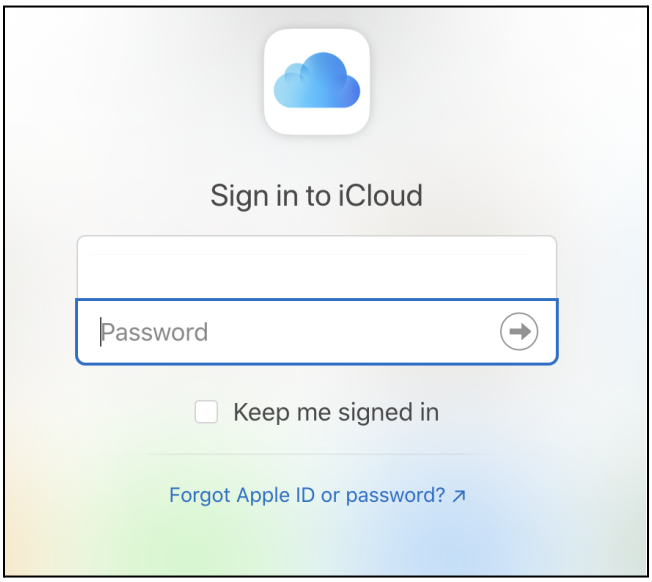
Following the steps in this section may send prompts to the devices that are connected to your iCloud account, as well as to your email address that you use for your Apple ID. The prompts sent to your devices may include information about your location, such as a map of the city or town where you logged in from.

1. Go to https://www.icloud.com/. You will see something like this:

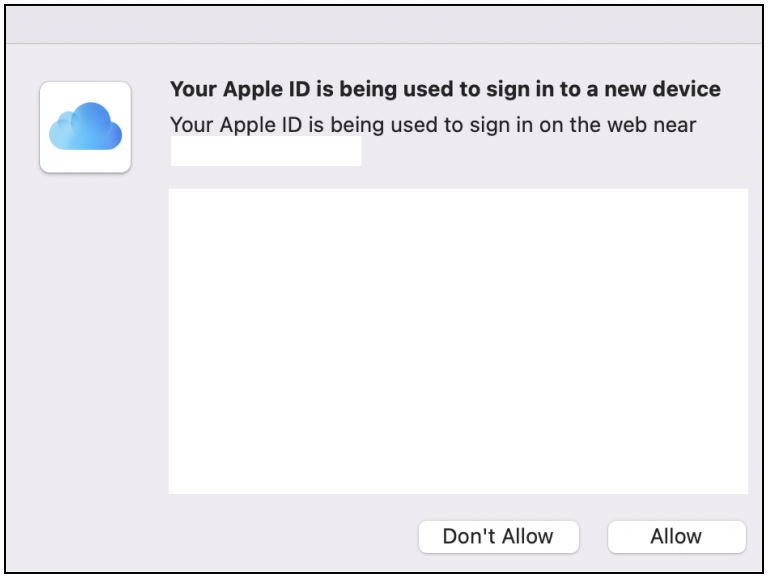


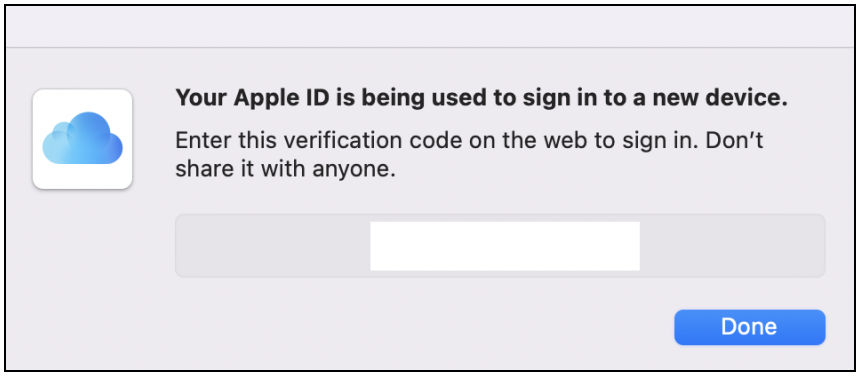
2. Enter your Apple ID (i.e., your iCloud address or the email address that you set up when creating your Apple ID) and hit enter

3. Enter your password

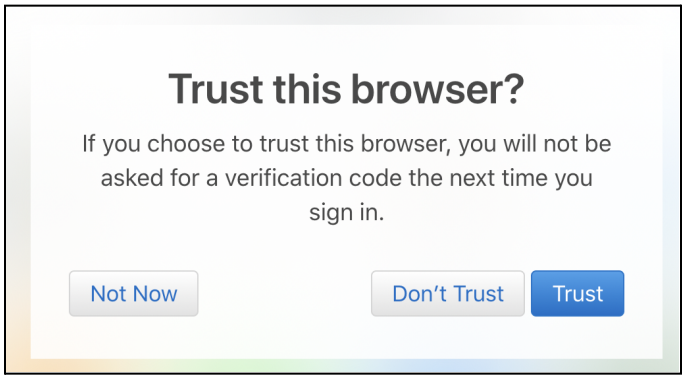


A prompt might be sent to your other Apple devices. Check the prompt and follow the instructions:



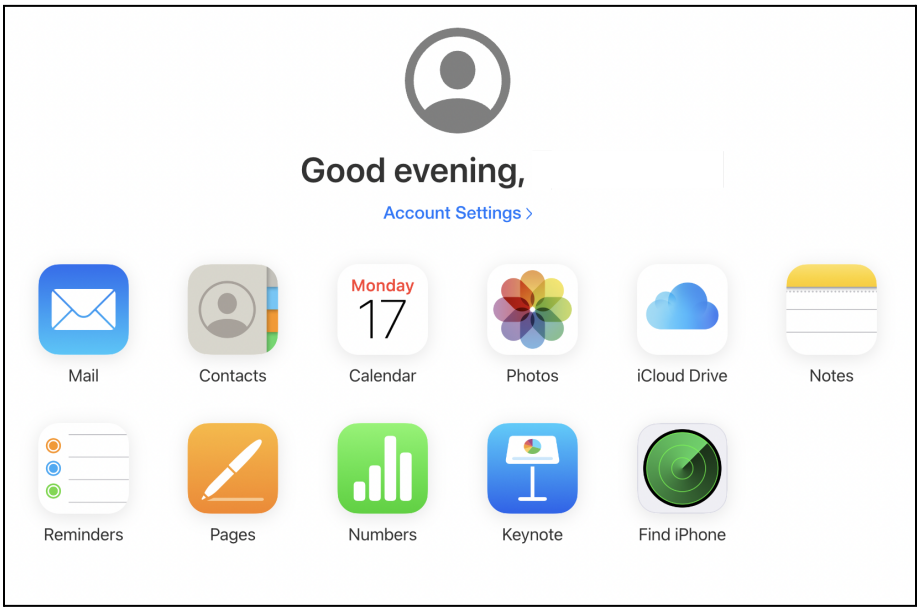


4. After approving the prompt, you might see something like this:



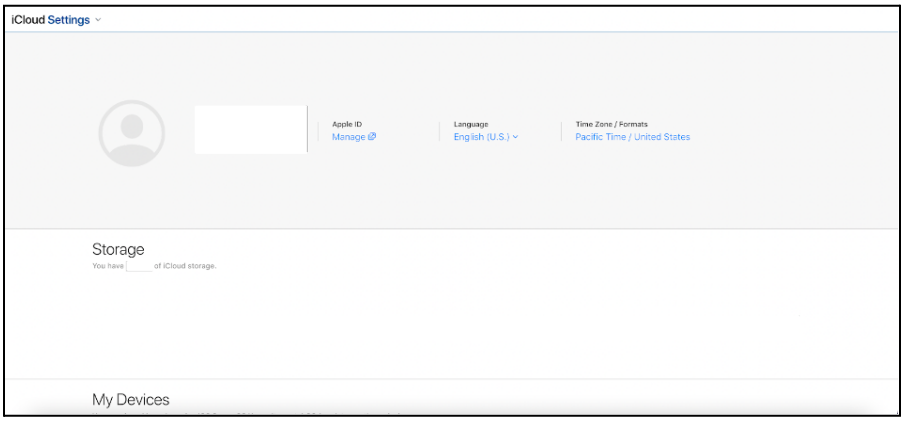
On the previous screen, you can choose the option you feel most comfortable with.

When you are logged in, you will see a screen like this one:



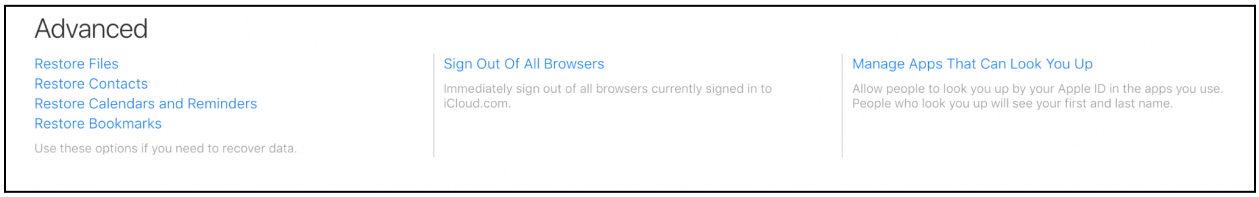
In this moment, Apple will send an email to your iCloud/Apple ID email address informing that there was a sign in into your account.

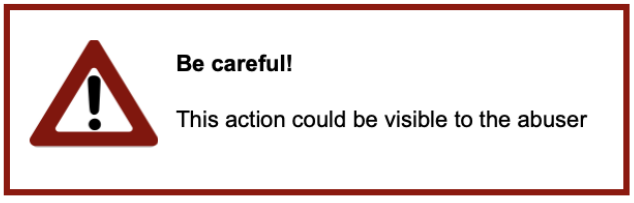
Click on **Account Settings**. You will see something like this:



Scroll down until you see **My Devices**. You will see a list of devices in which your iCloud/Apple ID account is currently being used:

Keep scrolling down until you see the following:

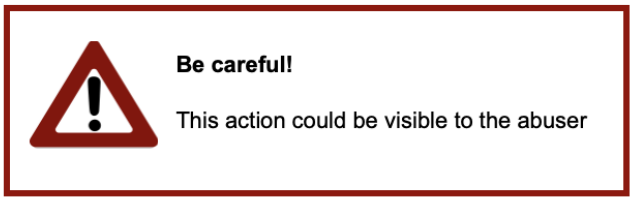




In this part, Apple provides you with various options that can be interesting for you, including restore files, contacts, calendars and reminders, and bookmarks.

There is also an option that allows you to sign out of all browsers where your iCloud/Apple ID account is currently signed in.

Recover your password using a web browser



If you are unable to change your password by following the steps in Change your Apple ID password, you can try using a web browser to recover your account by following the instructions on Apple's guide ("Change your Apple ID password on the web").

See also: Tips for creating a strong password

⚠️**Warning!** Your device may ask to save your new password, either in the browser or in Apple Keychain. If someone has physical access to your device, then they could log into your account this way.

Change the email address of your Apple ID

If someone has access to the email address that you use for your Apple ID, this could allow them to access your iCloud account or change its password.

To change your Apple ID, follow the instructions from Apple's guide here: Change your Apple ID - 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.