

iCloud - Compromise Cleanup

Improving Your Security If You Think Someone Else Has Gotten In

Compiled by the Clinic to End Tech Abuse

Last Updated: August 18, 2020

Who is this guide for?

If you suspect or know that someone else has gotten access to your iCloud account.

What does it cover?

- Checking for unrecognized activity
 - [Confirming linked devices](#)
 - [Confirming linked accounts](#)
 - [Confirming linked apps](#)
- Securing the account so that it is safe
 - [Changing your password](#)
 - [Turning off iCloud Location Services](#)
 - [Resetting or Unlocking Your Account](#)
 - [Check Family Sharing Settings](#)

Before we start:

- We created this guide based on how your iCloud account should look if you're using version 13.5 of iOS (the basic software that makes iPhones and iPads function). If iCloud or your Settings menu look different to you, we recommend checking to see if your software is up to date.
- **Is it safe for you to make changes to your account?** If anyone else has access to your account, they may learn quickly about any changes you make, such as if you change your password. Some abusers may become more violent if they get locked out of your account. If this is a concern for you, we strongly recommend that you talk to a domestic violence or other support professional about your safety before you make any changes to your account.
- We have marked changes that could be visible to an abuser with the following sign:



You can look at Apple's own guide to iCloud security here:

<https://support.apple.com/en-us/HT204145>.

Step 1: Checking for Activity You Don't Recognize



1.1 Confirming that You Recognize Any Devices Linked to Your iCloud



From the home screen on your phone, go to Settings (1).

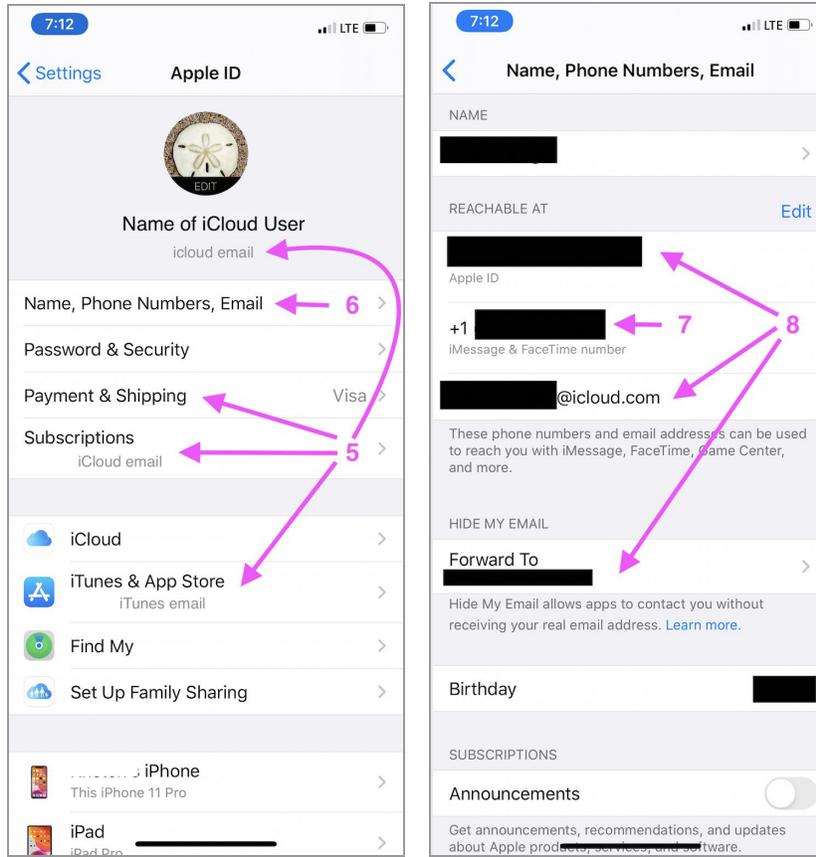
Make sure you recognize the name of the iCloud user (2) and icon under **Settings**. Is this you?

Then, click through to the Apple ID menu. Make sure you recognize all of the devices (3) listed at the bottom of the screen. A “device” is a smartphone, tablet, laptop, or other electronic gadget that can connect to the internet.

You can click on a listed device to see more information about it. If you do not recognize the device, you can click ‘Remove from Account’ (4) to disconnect the device from your iCloud account.

Then, you can [change your password](#) to keep someone else from logging into your account on that device again.

1.2 Confirming that Information in the iCloud Account Is Yours

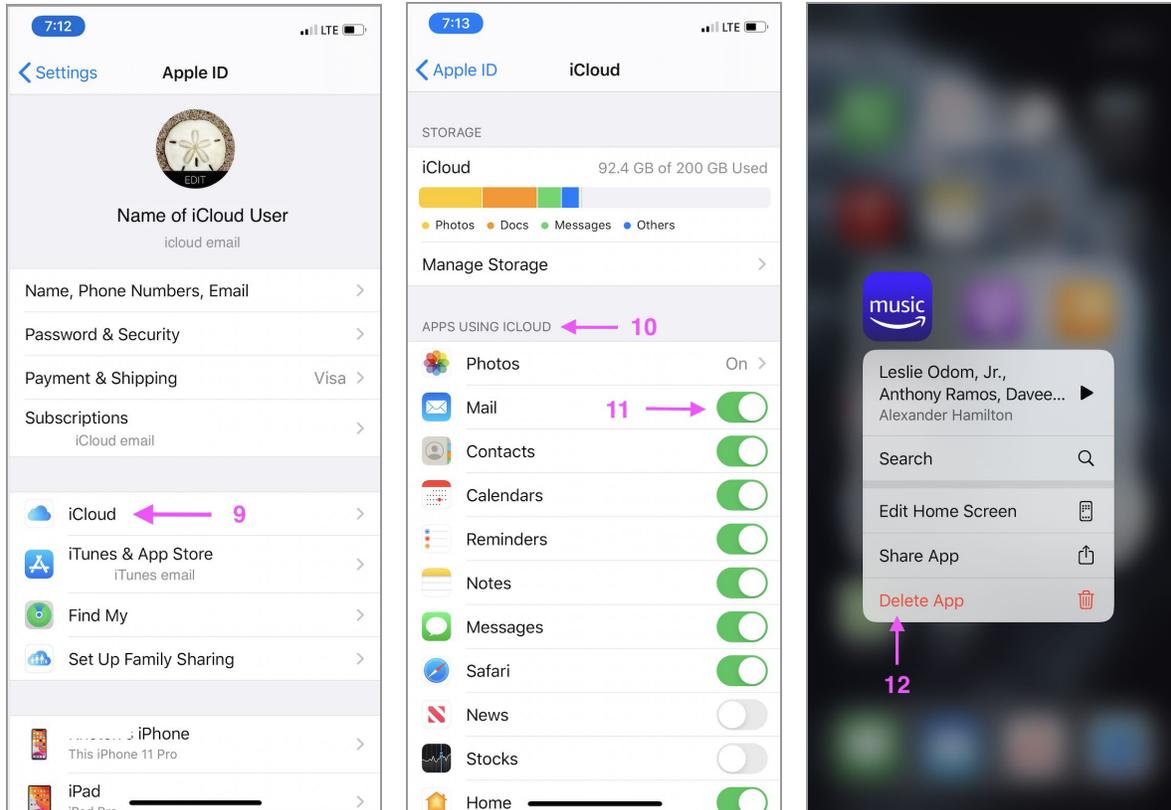


If your iCloud account has information linked to it that isn't yours, this could allow an abuser to learn things about you or get access to the account.

On the Apple ID menu (in Settings), make sure that any emails and credit cards linked to the account belong to you (5).

Then, click 'Name, Phone Numbers, Email' (6). Make sure the connected phone number (7) and email addresses (8) are yours. You can click Edit to add or delete a phone number. You will need to have that phone on hand to confirm the number via an automatic text message or a phone call that Apple will send.

1.3 Checking Apps that Send Information to Your iCloud Account



Your iPhone apps could be storing information about you in your iCloud account. If an abusive person gets access to your account, they may be able to see this information from the apps.

For this reason, it's important to **check and see which apps on your phone are backing up information to your iCloud.**

On the Apple ID menu (in Settings), click iCloud (9). Look at the list of apps under **APPS USING ICLOUD (10)** and make sure you recognize all of them.

If the app button on the right is toggled (set) to "on" and looks green, that means the app is backing up copies of your information in your iCloud account.

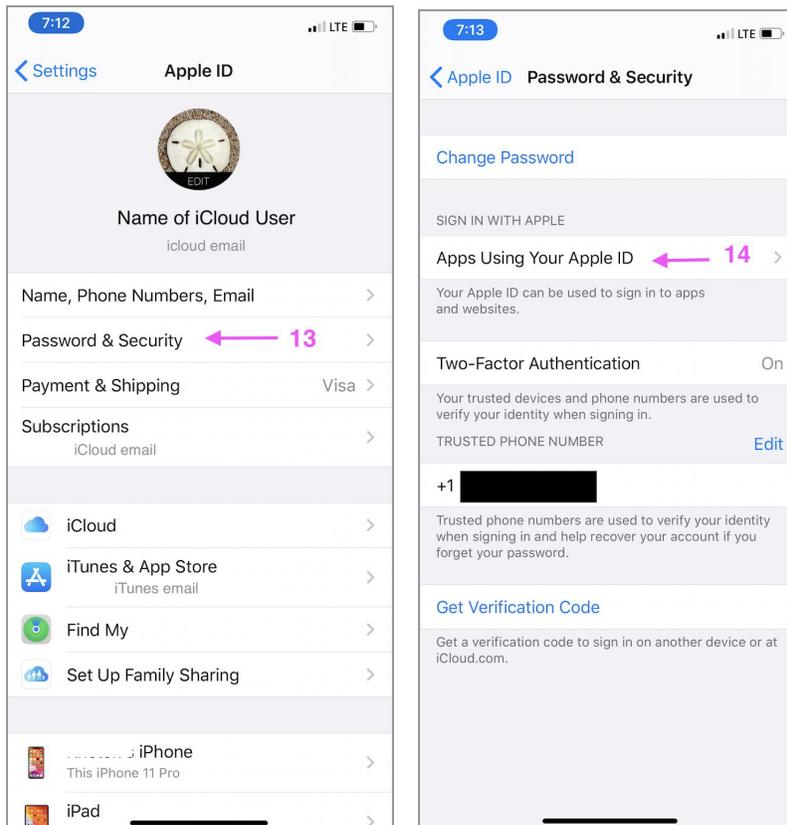
For example, if the Notes app is set to "on," that means anyone who gets access to your iCloud account could see copies of your Notes.

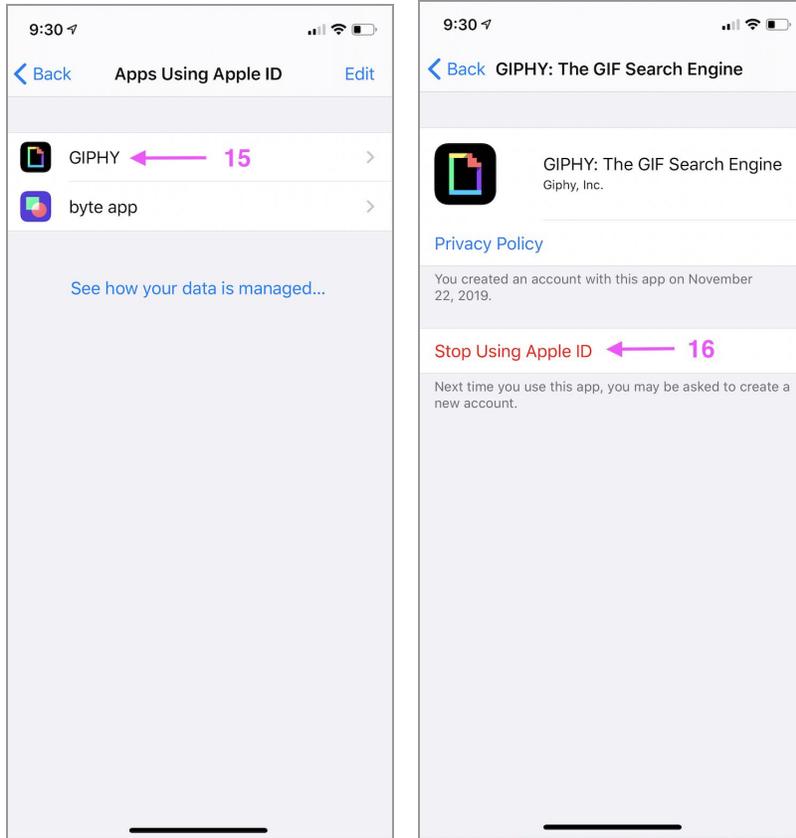
→ **This is very important.** For example, if you write down a password in Notes, and Notes is backing up to your iCloud account, an abuser could see your password if they get access to your iCloud.

You can turn off the connection between an app and iCloud by toggling (switching) the app's button to "off," which will look gray (11).

If you do not recognize an app and it isn't one that came pre-installed by Apple, you should be able to remove it from your device.

To delete an app from your device, find the app on your home screen. Touch and hold the app icon, then click 'Delete App' (12).





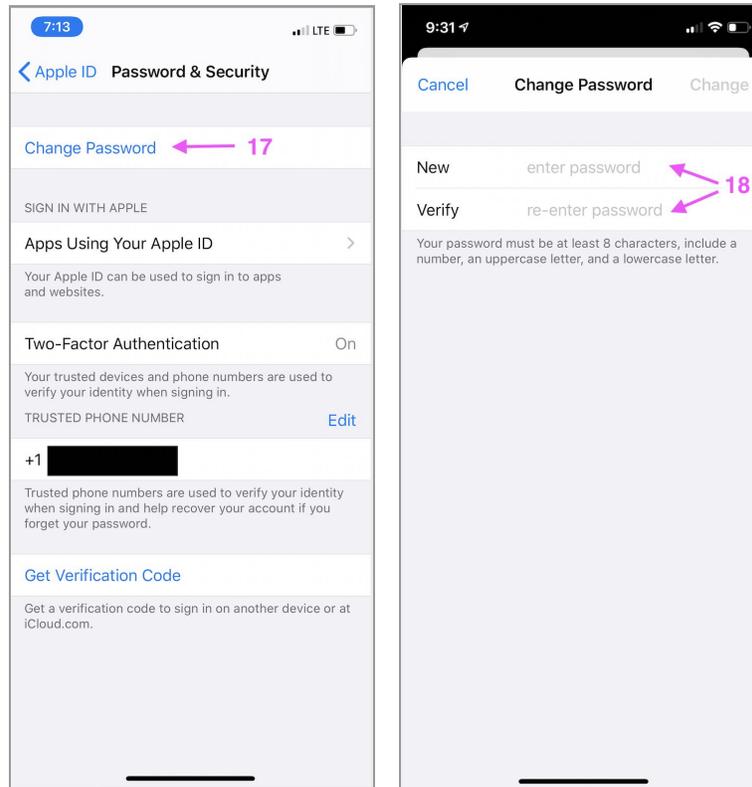
You can also remove apps using your Apple ID by returning to the Settings menu (1 -- see above) and selecting 'Password and Security' (13).

Under **SIGN IN WITH APPLE**, select 'Apps Using Your Apple ID' (14). Select the app you want to disconnect from your Apple ID (15) and then select 'Stop Using Apple ID' (16).

Step 3: Securing the Account



3.1 Changing Your Password



You can change your Apple ID password by returning to the 'Password and Security' menu (13 -- see above). This is also your iCloud password.

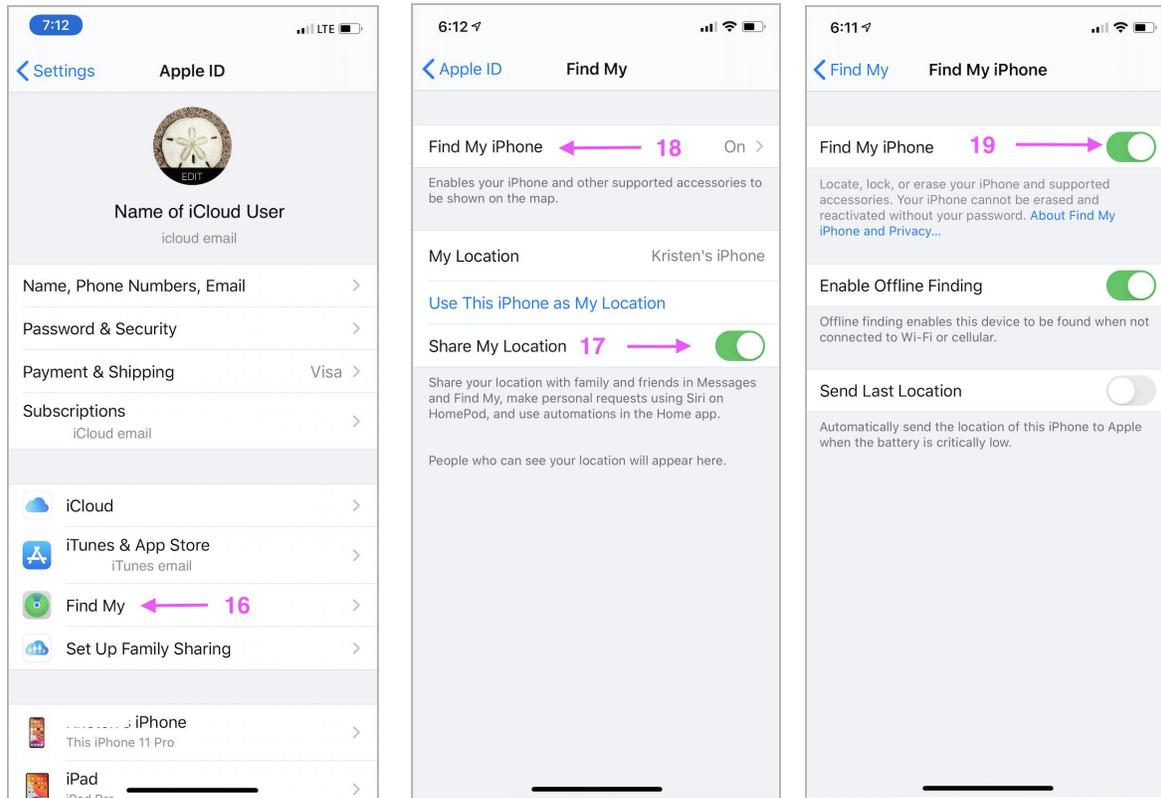
Click 'Change Password' (17). Apple may prompt you to enter your iPhone passcode. Then enter your new Apple ID password twice (18).

We recommend using strong passwords that are at least 8-12 characters long and include:

- A mix of capital and lowercase letters
- Some numbers that would be difficult for an abusive person to guess
- Some symbols such as !, ?, @, and \$

We suggest **not** using words that could be easy for someone else to guess, such as a child's or pet's name.

3.2 Turning off iCloud Location Services



iCloud location services let apps such as Find My iPhone use the phone's location. If an abusive person gets access to your iCloud account, they may be able to see this location data.

You can turn off iCloud location services by returning to the Settings menu (1 -- see above), selecting 'Find My' (16), looking for 'Share My Location' (17), and turning the toggle switch to "off" (so it looks gray). This will disable location sharing for the 'Find My' service..

Find My iPhone lets you see the location of your iPhone and lock and erase it remotely -- for example, if you lose it.

But if someone else gets access to your iCloud account, they could be able to see your phone's location.

You can turn off Find My iPhone by going to the 'Find My' menu (16 -- see above), selecting 'Find My iPhone' (18), and then toggling off 'Find My iPhone' (19) so that the switch turns from green to grey.

Just know that if you turn off Find My iPhone, you won't be able to use this app to find your phone remotely or lock and erase it if it gets lost.

3.3 Resetting or Unlocking Your Account

If you are unable to [reset your password from](#) one of your devices, you can use a web browser. A web browser is a program you use to visit websites, and some examples include Safari, Firefox, Google Chrome, and Edge. The Safari icon looks like this:



And the Google Chrome icon looks like this:



But you can use any browser you like.

In your web browser, go to <https://appleid.apple.com/> and then select 'Forgot Apple ID or password'. Enter your Apple ID and click the blue "Continue" button.

Confirm your account associated with your Apple ID (phone number) and click the blue "Continue" button.

Then pick from among the given options (security questions, recovery email, or recovery key) to decide how you'd like to reset your password. Reset your password and then use this new password to sign into iCloud.

Warning: If someone else has access to your account and you change the password, that other person will get locked out.

3.4 Check Family Sharing Settings

Family sharing allows you to share Apple purchases, photos, iCloud storage, and your location with up to five other people. An abuser could have access to your location or other information through Family sharing.

You can check your Family Share Settings to see if this is turned on, and if so, who has access. Follow the instructions here: <https://support.apple.com/en-us/HT201081>.

If you decide to keep Family Share turned on, then be sure to check what information is being shared by looking under Shared Features. You can choose what information you want to share.

© Cornell Tech 2020. This guide is for nonprofit educational and research purposes only and is not intended for commercial use. iCloud screens, notifications, and text are included selectively pursuant to the “fair use” provisions of United States copyright law, 17 U.S.C. § 107.