iPhone Passcode & Your Apple ID

Protecting your ID from theft and misuse

STEPHEN HUSTON

iPhones Embody Our Digital Lives

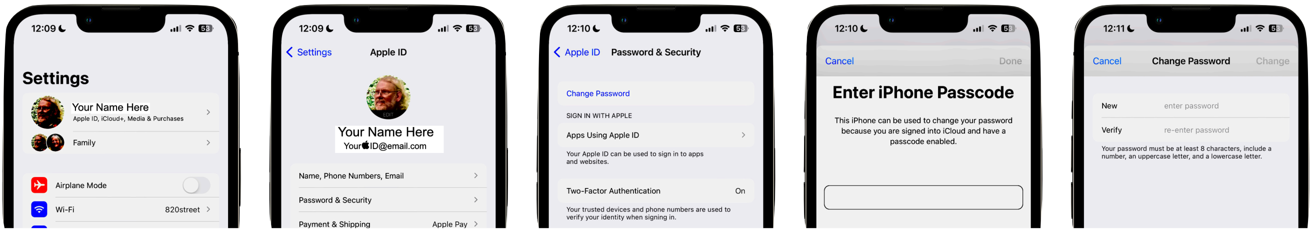
If someone gets your iPhone *and its Passcode*, they can take over your Apple ID (ID) so quickly that you may be unable to stop them. In less than 60 seconds, you could be locked out of your ID so you cannot lock, erase, or remove the stolen iPhone.

Then the thief can take their time — days or weeks — draining your funds from banks, Apple Pay, etc. — *freely using everything you ever accessed on your iPhone*.

How Passcode Thefts Happen

1. Someone watches you enter your iPhone Passcode to unlock your device in a public place; maybe they take video of you unlocking it. They've got your passcode. Later, they grab your iPhone from your hand or wherever you put it down.

2. In just seconds, they can: Unlock your iPhone using your Passcode, open Settings to Apple ID, change your Apple Password, then move on to your other accounts.



Your Apple ID can be used to sign in to apps and websites.

Your trusted devices and phone numbers are used to verify your identity when signing in.

This iPhone can be used to change your password because you are signed into iCloud and have a passcode enabled.

Your password must be at least 8 characters, include a number, an uppercase letter, and a lowercase letter.

Figure 1: Changing the Apple ID Password: **Settings > Apple ID > Password & Security > Change Password > Enter iPhone Passcode > Change Password**. It takes a few seconds, not minutes.

Because the iPhone is your primary Trusted Device for your ID, only your iPhone's Passcode is required to change your ID Password in Settings.

Once a thief changes that password, they also can remove your other devices from your account so you cannot use them to report the theft or even log back into your own ID.

The thieves now have your iPhone — your primary 2-Factor-Authentication (2FA) device — its Passcode, your Apple ID, and access to your texts, emails, and iCloud Keychain passwords. This is enough for them to be able to use apps or reset passwords for your financial apps, bookmarked Safari logins, and even change your email logins.

The thieves can now do everything you could previously do on your iPhone — and you can't! You could be locked out of all digital accounts, even on your other devices.

Even iPhone owners who remembered their ID passwords have found that the thieves changed that password so fast that they were unable to use another device to login and erase, lock, or remove their iPhone. In fact, they were no longer able to use their ID anymore on any device, losing access to everything in iCloud. *It all happened too fast!*

An Ounce of Prevention

If you take the necessary actions *before such a theft takes place*, you can give yourself enough time to erase your stolen iPhone and remove it from your ID before the thieves can get to your ID password. (Keep in mind that *if you delay*, they can still go to iCloud.com and request a Password Reset via email. That's slower than using the Settings described above, but it will happen if you allow them the time to do it.)

Having an extra few minutes to erase your iPhone and remove it from your ID can avoid a massive loss. The goal is to be fast enough to stop thieves from accessing your ID and controlling your iPhone and all of your digital accounts as if they were you.

Giving You Time to Act

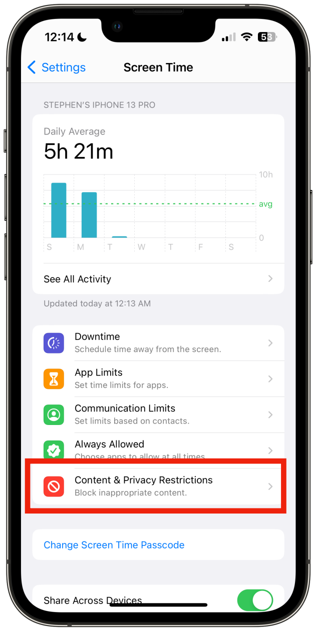
iPhone Settings for Screen Time can stop thieves from seeing your ID settings. With Screen Time restrictions enabled, the user must know a separate passcode to gain access to the ID Password Reset area in Settings.

That separate Screen Time passcode is not something you ever need to enter in public; it's only used when changing the controls to your access to the Apple ID Settings.

Screen Time is a part of Settings which I had ignored until recently, because I don't want to track how much time I use my phone. However, Screen Time's other use — *Parental Controls* — was something I thought I didn't need. *I was wrong*.

Screen Time's controls can limit the user's access within Settings, requiring extra time and effort for a thief to reset your ID by other and slower means (such as a browser request for a password reset).

Screen Time Settings to Hide Apple ID Access



12:14

Settings Screen Time

STEPHEN'S IPHONE 13 PRO

Daily Average
5h 21m

See All Activity

Updated today at 12:13 AM

Downtime
Schedule time away from the screen.

App Limits
Set time limits for apps.

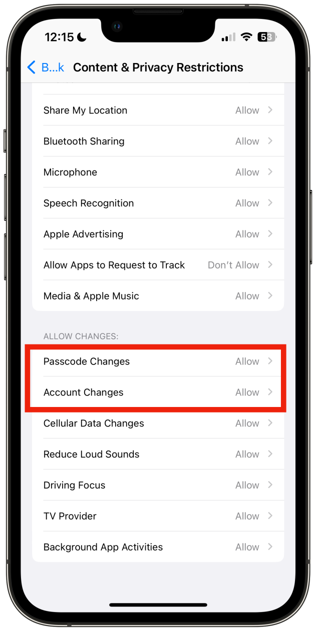
Communication Limits
Set limits based on contacts.

Always Allowed
Choose apps to allow at all times.

Content & Privacy Restrictions
Block inappropriate content.

Change Screen Time Passcode

Share Across Devices



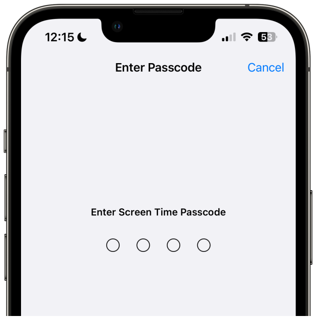
12:15

B...k Content & Privacy Restrictions

Share My Location	Allow
Bluetooth Sharing	Allow
Microphone	Allow
Speech Recognition	Allow
Apple Advertising	Allow
Allow Apps to Request to Track	Don't Allow
Media & Apple Music	Allow

ALLOW CHANGES:

Passcode Changes	Allow
Account Changes	Allow
Cellular Data Changes	Allow
Reduce Loud Sounds	Allow
Driving Focus	Allow
TV Provider	Allow
Background App Activities	Allow

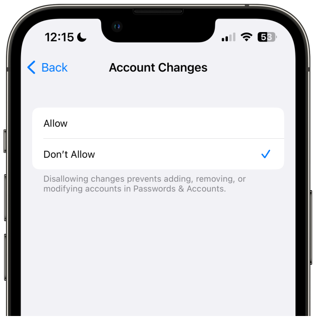


12:15

Enter Passcode Cancel

Enter Screen Time Passcode

○ ○ ○ ○



12:15

Back Account Changes

Allow

Don't Allow ✓

Disallowing changes prevents adding, removing, or modifying accounts in Passwords & Accounts.

Figure 2. Where to set a Screen Time Passcode:
Settings > Screen Time >
Content & Privacy Restrictions > (toggle ON the topmost button to enable restrictions)
Passcode Changes / Account Changes >
Enter Passcode > Don't Allow
(set toggles to Don't Allow on both Passcode Changes and Account Changes)

Choosing **Don't Allow** access for both Passcode Changes and Account Changes blocks user access to the Apple ID areas of Settings where the password can be reset quickly, making those areas of Settings inaccessible without the Screen Time 4-digit PIN.

This Gains You Some Time

- Disables the Apple ID section at the top of the main Settings screen;
- Stops user access to ID Password changes in Settings;
- **Gains some time** for you to access your ID via another device to erase your iPhone and remove it from your Apple ID.

What This Won't Do for You

- This *won't stop a thief* from using a browser at iCloud.com to click "Forgot Apple ID or password?" for an email or text to help them reset your password while they still have access to your emails, iCloud Keychain, and 2FA codes on your stolen iPhone.
- It will *not be as convenient for you* to view or make changes to Apple ID Settings. You must first go to Screen Time, turn off the toggle at the top of **Content & Privacy Restrictions** before making any changes to your Apple ID settings. When done, turn the Restrictions toggle back on. You do not need to change the *Don't Allow* settings; just toggle the Restrictions screen's top switch Off and On as needed.
  Your 4-digit passcode or PIN should be required each time you toggle the setting.

You Must Remember This

Avoid entering your iPhone Passcode in public. Entering it where it might be seen creates a higher risk of a thief getting both your iPhone and its Passcode to misuse it. If you must unlock your iPhone via passcode while in public, be aware of who could be watching, even at some distance. Thieves have been known to video passcode entries from behind the user and across the room while appearing to just read their own phone.

What To do If Your iPhone Is Stolen

The Screen Time “Don’t Allow” settings gain you some extra minutes to slow down the thief from resetting your ID Password, but you still must still act quickly, before they can use a browser and your email to reset it.

If your iPhone is stolen or lost in circumstances where there is a risk that the thief also got its passcode, you need to take action before the thief changes your ID Password:

- Remotely **Erase** your stolen iPhone.
- **Remove** your stolen iPhone from your Apple ID.

After those steps are completed, it is recommended that you also:

- Report the theft to the police.
- Report the theft to your cellular carrier, along with the iPhone’s serial numbers.

Erase & Remove the Stolen iPhone from Your ID

Three methods, from fastest (1) to slowest (3) — all are effective if done right away, not after finishing your evening out. Remember you’re in a race with the thief!

1. Use another Apple device with the same Apple ID:

> Open the *Find My* app. In the app’s *Devices* tab, scroll to the entry for your stolen iPhone and select it. On its details screen, scroll down to *Erase This Device*, and start the erase process. Once that is begun, also use the *Remove This Device* option to remove the stolen iPhone from your ID.
>
> (If either the Erase of Remove This Device options doesn’t appear, you may need to unlock any Screen Time restrictions which may be in effect on that device.)

2. Use another Apple device which is *not* logged in your Apple ID:

   Open the Find My app. In the app's *Me* tab, scroll down to the small blue text that says "Help a Friend." Use that to login to the Apple ID of the stolen iPhone. Once a list of devices appears, find the stolen iPhone and use the *Erase This Device* to start the erase process. After that is begun, use the *Remove This Device* option to remove the stolen iPhone from its Apple account.

3. Use any computer with a browser. At iCloud.com login with the stolen iPhone's ID.

   Locate the account information showing a list of devices on this ID, and find the stolen iPhone in that list. Use the *Erase This Device* option and the *Remove This Device* option to remove the stolen iPhone from your Apple account.

Successfully erasing *and* removing the iPhone from its ID by any of these methods will stop the thief from using the stolen iPhone further with the owner's data or account.

Next, it's time to report the theft to the police and your cellphone carrier.

Your cellphone carrier may require information about your iPhone that you cannot supply unless you saved it before it was stolen! *Save this information now*.

- Go to **Settings > General > About**. Start at the top of the screen and take a screenshot. Scroll downward to the next part of the screen not captured in the first screenshot and repeat as necessary until you have saved the entire *About* screen.
- In the middle of the *About* screen is a hidden tab named SEID. Tap on it to reveal the "Secure Element Identifier" and take another screenshot to capture that long unreadable ID code. Your carrier may require the SEID and other info from the *About* screen to identify the stolen phone and restrict its access to your cellular account.

SAVE IT NOW! Do not store the screenshots in iCloud or on your iPhone. You may need it at a time when those files are not available to you.

Now you're all set to venture back out into the world with your iPhone and be cautious enough not to lose both your iPhone and its passcode. If such a theft ever happens, you are instantly in a very short race with a thief for control of your Apple ID and digital accounts. With Screen Time settings in place, at least you'll have a fighting chance.

NOTES ON PICKING A 4-DIGIT PASSCODE FOR SCREEN TIME RESTRICTIONS

All 4-digit numbers are all woefully insecure. Using a short number to restrict Screen Time changes is acceptable only because time is critical, even though a PIN wouldn't withstand major hacking.

After all, you're only expecting to slow down a thief who *has other faster ways* to change your ID than repeatedly guessing for the right 4-digit number.

However, you don't want to be make it so easy they actually do guess it right away!

4-DIGIT PASSCODE TIPS

1. Don't use your own or a family member's birthdate or birth year.
2. Don't use 4 digits from your phone number, street address, zip code, or iPhone Passcode (which we must assume the thief knows if they got this far).
3. Don't use a number that repeats, such as 0000, 1111, 2222, etc.
4. Don't use sequential numbers, such as 1234 or 0987.
5. Don't use a number because it makes an easy pattern on the 10-key number pad, such as 7913 or 9510.
6. Avoid these PINs which are most commonly used: *

   1234 1111 0000 1212

   7777 1004 2000 4444

   2222 6969 9999 3333

   5555 6666 1122 1313

   8888 4321 2001 1010

7. Pick a number you will **remember**. The process to reset your Screen Time passcode can take longer than resetting your ID password!

* There are 10,000 possible 4-digit numbers from 0000 to 9999. Yet, over 1/4 of phone users pick one of the 20 shown above because they are easy to enter, easy to remember, or both.

Do Better. Don't Get Caught.