iPhone Passcode vs Apple ID

Protecting your ID from your own iPhone

STEPHEN HUSTON

Losing Your iPhone & Your Digital ID

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. Within seconds, you can be locked out so you cannot report your own iPhone as lost or erase it.

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

How It's Done

1. Someone watches you enter your iPhone Passcode to unlock your device in a public place; maybe they take video of you entering it. They've got your passcode. Then they grab your iPhone from your hands or pick it up from wherever you set it down.
2. In just a few seconds, they can: Unlock your iPhone using your Passcode, open Settings to Apple ID (ID), and change your Apple Password.

Figure 1: Changing the Apple ID Password: **Settings > Apple ID > Password & Security > Change Password > Enter iPhone Passcode > Change Password**.

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 the thieves change that password, they also can remove your other devices from your ID so you cannot use them to report the theft or to 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 and email on that phone. This is enough for them to be able to use apps or reset passwords for all financial apps, bookmarked Safari logins, and even change your email logins.

Everything you could do on your iPhone, the thieves can now do — and you can't!

Even iPhone owners who remembered their ID password found that the thieves changed the password so fast that they are unable to use another device to login and report their iPhone as lost, lock it, or erase it. It was so fast — it was already too late.

An Ounce of Prevention

If you take action *before such a theft ever takes place*, you can give yourself enough time to lock or erase your stolen iPhone before the thieves have time to change your ID password. (Keep in mind that *if you wait*, they can still go to iCloud.com in Safari and request a Password Reset via email. It's slower than the Settings option above, but it will work if they have the time.)

Having an extra few minutes to report your iPhone lost or to erase it using your ID can avoid a huge financial loss. It might even allow you to keep tracking your stolen iPhone. The main thing is to stop thieves from getting into your Apple ID or using your iPhone as if they were its owner.

Screen Time gives you time to take action

iPhone Settings for Screen Time can stop thieves from using the fast method in Figure 1 (above) by requiring knowledge of a separate passcode to get access to that Password Reset option.

The Screen Time passcode is not something you ever need to enter while in public; it's only to change Screen Time settings affecting user access to the Apple ID Settings.

Screen Time is a part of iPhone Settings which I mainly ignored until now, because I don't need or want Apple to track how much time I spend on it. Screen Time's other primary use is for *Parental Controls*, which I thought I didn't need.

I was wrong.

Screen Time's toggles can limit any user's access within Settings, giving a few extra minutes before a thief can reset your ID by other means.

How to Add a Screen Time Passcode to Hide the Apple ID Settings

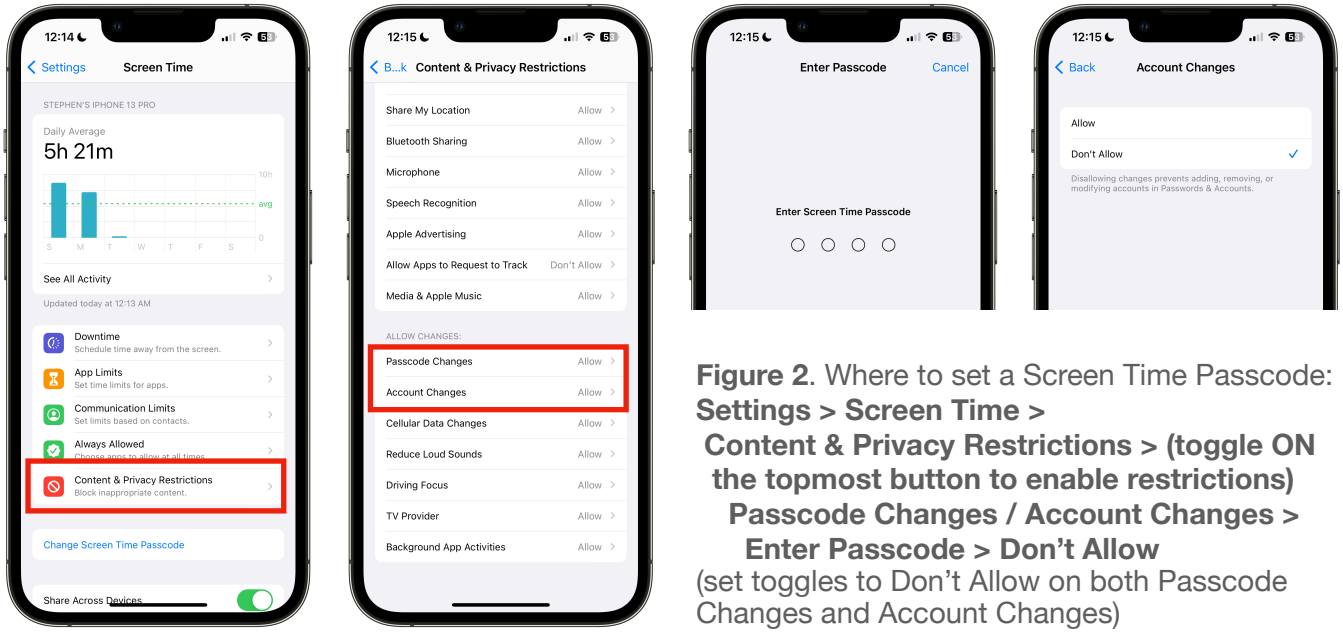

Figure 2. Where to set a Screen Time Passcode: **Settings > Screen Time > Content & Privacy Restrictions > (toggle ON the topmost button to enable restrictions) Passcode Changes / Account Changes > Enter Passcode > Don't Allow** (set toggles to Don't Allow on both Passcode Changes and Account Changes)

Turning Off access to both Passcode Changes and Account Changes via this area of Screen Time turns off user access to the entire Apple ID area of Settings, and disables access to Apple ID account settings in Settings > Mail > Accounts, making it impossible for anyone to use those areas of Settings where the ID can be reset most quickly.

What This Does for You

1. Disables the Apple ID section at the top of the first Settings screen.
2. Hides the listing of Devices where a user can remove other devices from the ID.
3. Stops the user from reaching screens to change the ID Password with just a passcode.
4. Gains more time for you to access your ID via another device and report your iPhone stolen or lost and erase it.

What This Won't Do for You

1. This won't stop a thief from using a browser and entering your email address at iCloud.com, then clicking on "Forgot Apple ID or password?" for an email or text to help them reset your account — they can get your emails and 2FA codes on your iPhone.
2. It will not be as easy for you to make changes in the Apple ID area of Settings. You must go into Screen Time, change the settings (Figure 2, above) back to *Allow*, then make your changes to Apple ID settings, and then reset the Screen Time toggles to *Don't Allow.*

You Must Remember This

Avoid entering your iPhone Passcode in public. If you must, be extremely aware of who's watching. The Screen Time "Don't Allow" settings gain time, but you still must act promptly.

Notes on Picking a 4-Digit Passcode for Screen Time Changes

Any 4-digit number is simply not secure. Using a short number to restrict Screen Time changes is acceptable where time is critical, not something which might face a major hacking attack.

After all, you're only expecting to slow down a hacker, because they have other ways of changing your Apple ID which are still faster than guessing a 4-digit number.

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

4-Digit Passcode Tips

1. Don't use your own or a family birthdate or birth year.
2. Don't use the first 4 digits of your phone number, street address or zip code.
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 known to be 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**.

* There are 10,000 possible 4-digit numbers from 0000 to 9999. Yet, over 1/4 of phone users picked one of the 20 shown above.

Do Better. Think Different.