

Security: Basic iPhone Settings

Prepared for the *Alameda MUG & iPhone Without Tears* classes

Essential iPhone Security

Without a passcode, there is no security at all on an iPhone.

Security Settings control who has access to your iPhone and its most sensitive contents. This paper covers Passcodes, log-in ID, and related settings for a secure iPhone.

When an iPhone is unlocked, anyone who handles it has full access to everything on it and everything to which it can connect.

For example, if you use a Mail app on your phone, your unlocked iPhone lets anyone who picks it up use your email. Your email can be used to reset passwords to online accounts, including bank accounts, sometimes even if you don't usually bank online yourself.

However, with properly enabled Passcode settings, your iPhone can be extremely secure.

Passcodes & Touch ID/Face ID

Login Settings for unlocking your iPhone are in the *Touch ID & Passcode* section for devices with a Home button, or in *Face ID & Passcode* for devices supporting Face ID.

In Settings, scroll down the main Settings screen to the section which begins with *General*. Find the section name which includes *Passcode*.

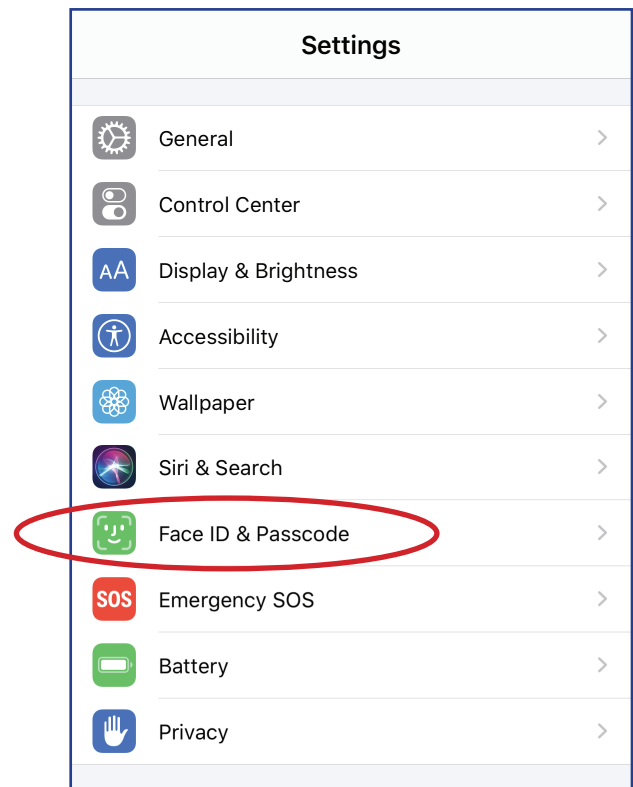
When you select that section, you must enter the current Passcode to proceed. This requirement protects you from having your

Prepared February 19, 2020

by Stephen Huston

AlamedaMUG@gmail.com

All screenshots captured
on an iPhone XS
running iOS 13.3.1



passcode changed by anyone who doesn't know your current iPhone passcode.

Basic Passcode Setup

Passcode settings let you setup Touch ID or Face ID, depending on your device. (Follow the simple onscreen instructions to quickly set it up.)

Both forms of login ID are secure, and you should set up the appropriate option to avoid having to hand-enter your passcode each time you use your phone. Using Touch ID or Face ID, unlocking your iPhone takes under a second.

Next, scroll down to the area which says:

Turn Passcode On/Off

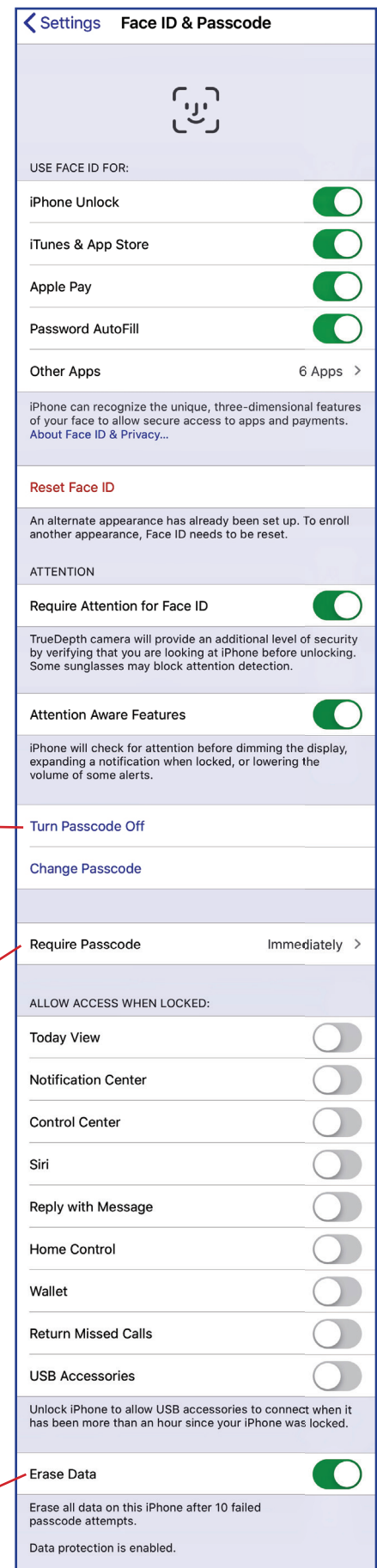
If it says *Turn Passcode On*, then your passcode is currently Off and you need to fix that right away. If you don't use a passcode, anyone who picks up your iPhone could set up a passcode and lock you out of your own phone!

(If it says *Turn Passcode Off*, leave it alone because a passcode is already On.)

Once your Passcode is On, and you've enabled Face ID or Touch ID, make sure the *Require Passcode* timing is set to *Immediately*.

Next is the list of what people can see on your lock screen while the iPhone is still locked. You can safely set all of these to Off and still be able to see everything yourself with a click or a glance. If you leave these items visible to others while your iPhone is locked, they may be able to interact with your calls, messages, calendar events, etc.

The *Erase Data* option should be enabled if you have any type of iPhone backup. (You really should.)



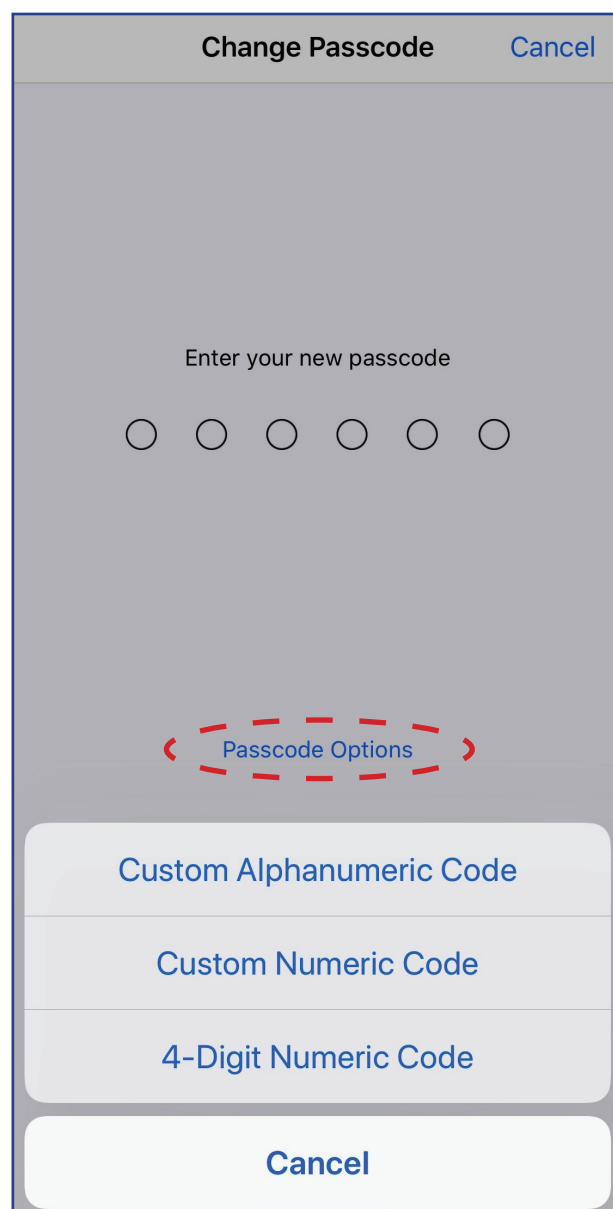
Creating a Strong Passcode

Now that you have a Passcode working, consider using the *Change Passcode* option (below *Turn Passcode On/Off*) to choose a more secure passcode. Apple offers three styles of passcodes:

- 6-digit PIN — (a Personal Identity Number, Apple's default option)
- Custom PINs of 4 or more digits
- Custom Alphanumeric passcodes

All of the numeric PIN options are very weak because they use only numbers. A 4-digit PIN has only 10,000 possible variations, while a 6-digit PIN still offers only a million possible entries. While that may sound like a lot, it's actually extremely weak. Modern hacking tools try passwords at the rate of billions and even trillions of attempts per seconds. A PIN that's 18-digits long can be cracked in just a few minutes because all of the characters are numbers. Numbers alone make extremely weak passcodes.

For the best security, create a Custom Alphanumeric Code of 12 *or more* characters containing both upper-case and lower-case letters, plus one or more numbers, and a symbol or punctuation character. This provides 95 possible characters to choose from for each of your 12 or more characters (instead of 10 each for numbers-only). Even at trillions of tries per second, you're now into the range of weeks, months, and — with any luck — years to break your passcode.



To create a strong passcode, when told to enter your new passcode, click instead on **Passcode Options** lettering above the numeric keypad.

You will get three option buttons. The top choice, Custom Alphanumeric Code, will reveal the full iPhone keyboard so you can enter your numbers, upper-case, lower-case, and symbol/punctuation choices to create a much more secure passcode. Remember, you won't use it often with Touch ID or Face ID enabled.

Securing the Lock Screen

Now that you've made sure your iPhone is protected by a strong Passcode, double check that you've also turned off access to potentially personal stuff on your Lock Screen (noted on page 2). Everything visible on the lock screen can be read by anyone who handles your iPhone even if they can't unlock it.

If you leave items exposed on the Lock Screen, they can be used to interact with your phone while it's still locked. That means someone else could use them.

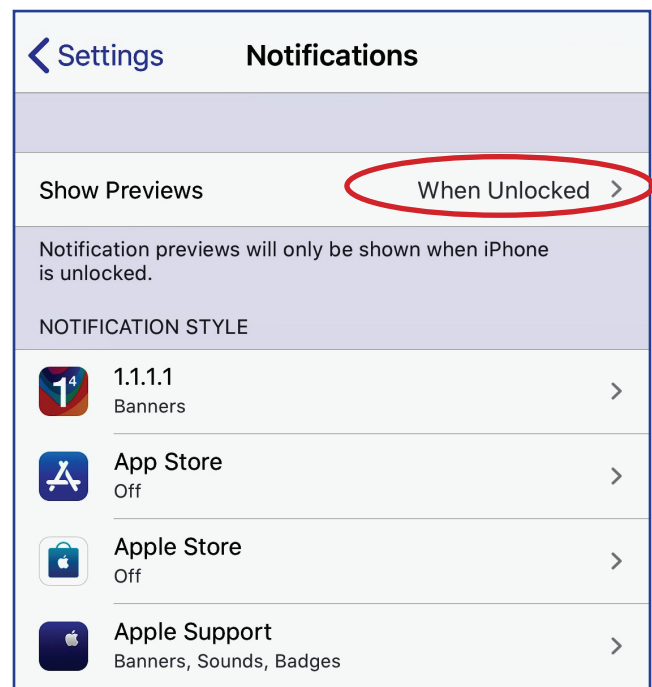
When your iPhone dings or rings, will someone other than you be able to pick it up to read or even respond to messages? How about seeing your Calendar events, or responding to phone calls with a text?

Notifications Settings

From the first Settings screen, you can click on *Notifications* and change its top setting to *Show Previews* of Notifications only *When Unlocked*. (The default setting is *Always*, which some find convenient but is far less secure.)

With that change, when your iPhone is locked, only an indicator of a notification will appear when something arrives, but its contents won't be viewable until the iPhone is unlocked.

Remember, you can unlock your own Lock Screen and have the details fully appear with a simple glance when using Face ID, or with one click for Touch ID. You're making it tougher on those who can't unlock your phone, not on yourself.



Protecting Codes for Two-Factor-Authentication

If you use Two-Factor-Authentication (2FA) for an iCloud Account or a bank, turning Notification previews off when locked will stop others from reading those 2FA codes that get sent to your iPhone. That will be extremely important if your iPhone is ever lost or stolen.

Do It Now

You can't fix these settings *after* you lose control of your iPhone.

