Apple Device Security Best Practices

Cove Apple Club — April 26, 2023

Most iPhones in use today have **Face ID**, which was introduced in November, 2017. It provides the best, quickest and most secure **first-level** of device and account security for iPhone and iPad Pro users.

Face ID has been shown to be secure against attacks such as photographs, realistic masks and even animatronic mannequins. Using Face ID on every device that features it is the best first line of defense to keep your devices secure.

In addition to Face ID, the iPhone's device setup flow requires the user to create a device passcode. When Face ID fails, or after an iPhone restart or software update, the passcode will unlock the iPhone and re-enable Face ID.

For this reason, Apple recommends and the default setting is a 6-digit passcode. Optionally, for even stronger passcode security, you can enable a **custom alphanumeric passcode**.

To set up a custom alphanumeric passcode:

- On your iPhone, go to Settings ➔ Face ID/Touch ID & Passcode ➔ Change Passcode ➔ Passcode Options ➔ Custom Alphanumeric Code.
- *Be sure to record your passcode in 1Password, as well as offline on paper in a document safe, and where your partner / spouse / spice has access to it and is aware of it in case of your incapacitation.*

For more information on iPhone passcodes, **click here** or visit:

- https://support.apple.com/guide/iphone/set-a-passcode-iph14a867ae/ios

As a further protection against bad actors taking over your Apple ID account if your iPhone is lost, stolen or your account password is compromised, you can set an account ***Recovery Key***. A Recovery Key is a randomly generated 28-character code that you can use to help reset your password or regain access to your Apple ID.

While it's not required, using a Recovery Key improves the security of your account by putting you in control of resetting your password.

Creating a Recovery Key turns off account recovery. Account recovery is a process that would otherwise help you get back into your Apple ID account when you don't have enough information to reset your password.

Using a Recovery Key is more secure, ***but it means that you're responsible for maintaining access to your trusted devices and your Recovery Key.***

If you lose **both** of these items, you could be locked out of your account **permanently**. With that in mind, it's important to keep your Recovery Key in a safe place. ***You will want to give a copy of your Recovery Key to a family member, and keep copies in more than one place, like in a document safe and in 1Password.*** That way you always have your Recovery Key when you need it.

To set up a Recovery Key:

- Go to Settings ➔ [your name] ➔ Password & Security. You might need to enter your Apple ID password to continue.
- Tap Recovery Key.

- Slide to turn on Recovery Key.
- Tap Use Recovery Key and enter your device passcode.
- ***Write down your Recovery Key and keep it in a safe place. Keep additional copies of your Recovery Key offline in a document safe, online in 1Password, and where your partner, spouse or trusted friend can access it and is aware of it.***
- Confirm your Recovery Key by entering it on the next screen.

Protect your Recovery Key from being hijacked using Screen Time Account Controls

In the nightmare scenario that your iPhone is stolen ***while it is unlocked***, or your Apple ID account is compromised, bad actors can do the following to lock you out of your Apple account ***permanently***:

- Change your Apple ID password to one they control
- Change your Recovery Key to one they control

Right now, Apple does not have an elegant way to protect against this, but clever security researchers have devised a good workaround that solves the problem.

It uses the Screen Time feature in iOS to prevent the bad actors from changing your account password, and thereby, prevent them from changing or turning off your Recovery Key.

To enable this protection for your Apple ID account and Recovery Key:

On your iPhone or iPad:

- Tap Settings ➔ Screen Time ➔ Use Screen Time Passcode
- Choose a Screen Time Passcode, then confirm it when prompted. You will be asked for your Apple ID and Apple ID password.
- Once the Screen Time Passcode has been set, tap Content & Privacy Restrictions, and toggle it On. Enter your Screen Time Passcode when prompted.
- Scroll down to Allow Changes ➔ Account Changes, and tap Don't Allow.
- Finish by tapping the back arrow at the top of each screen until returning to the main Settings menu.

For more information on Recovery Key, **click here** or visit:

- https://support.apple.com/en-us/HT208072

For more information on Apple's best practices for keeping your iPhone secure, **click here** or visit:

- https://support.apple.com/guide/iphone/keep-your-apple-id-secure-iph904b71f28/16.0/ios/16.0