Turn On This New iPhone Setting to Protect Your Money and Photos

Nicole Nguyen and Joanna Stern

How do you protect your life savings, decades of photos and the rest of your digital life? By flipping a new switch buried in your iPhone's settings menu.

On Monday, as a part of the now-available iOS 17.3 update, released Stolen Device Protection. The setting adds a layer of security that could foil a thief who has stolen both your iPhone and the passcode you use to unlock it.

The release follows The Wall Street Journal's yearlong investigation on iPhone thefts happening across the country. Thieves with an iPhone and its passcode quickly lock their victims out of their Apple accounts by changing the password and other settings. Then they go for the money, draining bank accounts, opening credit cards and more. One thief, who is now in prison in Minnesota, told us how he stole hundreds of iPhones and hundreds of thousands of dollars by taking advantage of this vulnerability.

Stolen Device Protection makes a lot of that harder for a criminal—if you turn it on. How does it work? Is there a downside? Are there loopholes criminals can exploit? We have been testing it for the past few weeks to get the answers.

What can a thief do with a passcode exactly?

Your passcode—typically a short string of numbers that grants access to an iPhone—is powerful. When Face ID or Touch ID fails, the passcode serves as a fallback. With this code, thieves can:

• Change the password to your Apple ID so you can't get back in

• Disable Find My iPhone

• Access stored passwords in Apple's iCloud Keychain, including those to bank and money apps

• Enable a recovery key, an Apple security setting that could lock you out of your Apple account—possibly forever

• Erase everything on the device to sell it

What does this new setting do?

If you enable Stolen Device Protection, your iPhone will restrict the passcode's *power* over certain settings when you are away from a location familiar to the iPhone, such as your home or work.

So say you are at a bar, and a thief steals your phone and passcode. The thief would now need more than just that passcode to change settings and access secure information. Depending on the action, there are two levels of protection:

• **Level one: Biometrics.** To access saved passwords or saved payment methods in Safari, the iPhone would require your biometrics—Face ID or Touch ID. The passcode would no longer be available as an alternative.

• **Level two: Biometrics and a delay**. To modify more sensitive settings, such as changing an Apple ID password, enabling the recovery key or disabling Find My, two additional steps would be required. The iPhone would ask for Face ID or Touch ID, then start a one-hour countdown. After the delay, it would ask for *another* Face ID or Touch ID scan. The thief would need to go through these steps to turn off Stolen Device Protection as well.

How does it know my frequented locations?

In a familiar location, like your home, you can use your passcode if a face or fingerprint scan fails. To teach the phone what locations are familiar, you need to turn on a setting called Significant Locations. (It may already be on.) In Settings, go to Privacy & Security, then Location Services. Scroll down to System Services, then Significant Locations.

You can't tell your iPhone outright which locations you consider to be familiar, and your iPhone doesn't provide a list of what it recognizes as your most frequented locales. It isn't ideal—but it means a thief won't be able to drop by your address to use your passcode.

In our testing, the most frustrating part of the setting was that it took a couple of weeks for the iPhone to learn where we spend most of our time. And then, after two weeks away from the office, it no longer recognized that building as familiar.

You can test what your iPhone considers a familiar location. Once Stolen Device Protection is enabled, try to turn the Stolen Device Protection setting off. If you can use just Face ID or Touch ID without a time delay, then you're in a familiar location.

Should I really turn this on?

Yes. Just read our previous stories and you'll see why. We have heard from hundreds of victims of these crimes. In most cases, thousands of dollars were looted from their iPhones. And if the thieves enabled Apple's recovery key, victims have been locked out of their Apple accounts for good. They lost access to decades of family photos, videos, notes and other precious files.

In its default state, Apple's iOS gives victims few ways of preventing harm if their passcodes fall into the wrong hands.

OK, how do I turn it on?

Even when you upgrade to iOS 17.3, Stolen Device Protection is turned off. Go to Settings, Face ID & Passcode and type in your passcode. Then scroll down to Stolen Device Protection and turn it on. Apple says it will prompt users to turn this setting on in a future iOS update.

You must have two-factor authentication and Find My enabled for your Apple ID account to use Stolen Device Protection.

Is there any reason to leave this off?

If your front-camera face scanner or home-button fingerprint reader break, then you won't be able to access any of the protected features until you're back in a familiar location or fix the device.

This could be a problem if you're away from home, break your phone and need to access saved iCloud Keychain passwords, for example. (You could mitigate this by setting up a third-party password manager.)

When you're traveling, you should also know that some actions will take an hour-long wait, such as changing your Apple ID password on your phone.

What isn't protected?

If a thief has your passcode, Stolen Device Protection won't stop them from gaining access to email and other unprotected apps. Third-party accounts can be reset by text or email. Apple Pay still works with just a passcode.

That's why you should consider these additional security measures:

Create a hard-to-guess passcode. Make sure it's long and complex—at least six or more digits. A string of

letters and numbers is harder to snoop, even if the thieves film you from a distance: Go to Settings > Face ID & Passcode > Change Passcode > Passcode Options > Custom Alphanumeric Code.

Add PINs to sensitive apps. Protect finance apps, such as Venmo and Cash App, by enabling an additional PIN or biometrics. If you use an authenticator app, such as Google Authenticator or Authy, you can turn on Face ID or Touch ID protection. You can also set up a separate passcode for Coinbase and Robinhood in security settings.

If your device is stolen, act quickly. Memorize this simple web address: icloud.com/find. You can use it on any device. Plus, you won't need a two-factor code from your phone to locate the device and remotely erase its data.

—For more WSJ Technology analysis, reviews, advice and headlines, sign up for our weekly newsletter.

Write to Joanna Stern at joanna.stern@wsj.com and Nicole Nguyen at nicole.nguyen@wsj.com

Appeared in the January 24, 2024, print edition as 'Don't Ignore This New iPhone Setting'.