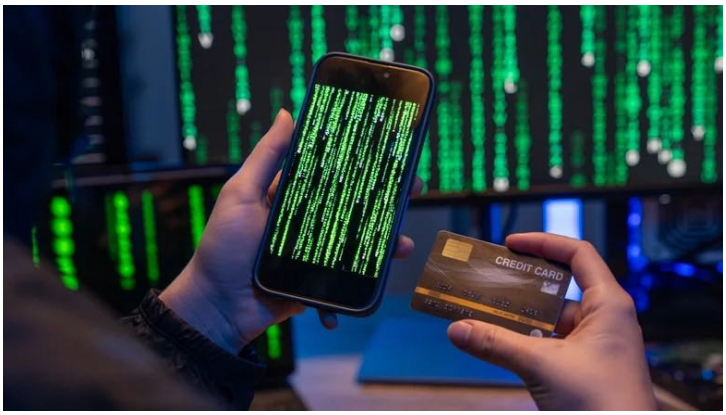
This Hidden iOS Feature Can Save Your Private Data From iPhone Thieves

By Michael Bizzaco Aug. 10, 2025 1:17 pm EST



Boonchai Wedmakawand/Getty Images

Your iPhone is packed to the brim with all things you, and that includes private data you wouldn't want falling into the wrong hands. We also can't pretend we live in a world where phones and other mobile devices aren't stolen on a daily basis. That's why companies like Apple have to be forward-thinking when it comes to defending its users, which leads us to a great peace-of-mind feature introduced with iOS 17.3 called Stolen Device Protection.

When the feature is enabled, Stolen Device Protection requires additional steps and verifications before using certain iPhone features, especially when it comes to financial info stored on your device. These extra failsafes aren't the only new iPhone security features, or even the strongest, but they help to keep your most sensitive data under lock and key, while giving you more time to use tools like the Find My app to disable your lost or stolen Apple tech.

First, let's unpack the Stolen Device Protection function a bit more by exploring the intricacies of this Apple feature. Then, we'll teach you how to enable and disable the iOS function, as well as how to customize it.

How Stolen Device Protection works

Surasak Suwanmake/Getty Images

When enabled, Stolen Device Protection puts up additional security checkpoints across iOS. These deterrents are particularly useful if the individual who grabbed your iPhone knows your passcode, as the extra security could prevent them from wreaking digitized havoc.

One of these security measures is one-time biometric sign-ins for info like stored passwords and credit cards, using either

Face ID or Touch ID (for older iPhone models). Usually, you'll be prompted to enter your passcode when Apple biometrics fail, but in the event that a thief is using passcodes to sign in to your iPhone, Stolen Device Protection ensures Face ID or Touch ID is the only way in.

There's also a security delay that activates when your iPhone detects it's not in a familiar location, like your house, school, or workplace. If a thief attempts to sign in to your Apple account when iOS knows your phone isn't at its usual stomping grounds, a one-hour delay is imposed for actions like changing your account password. Your iPhone will also require a second Face ID or Touch ID sign-in. You can also modify Stolen Device Protection's settings to require these additional sign-in steps all the time, so not even a familiar location will prevent iOS from employing these safeguards.

How to enable Stolen Device Protection

Yalcin Sonat/Shutterstock

In order to use Stolen Device Protection, you'll need to make sure your iPhone is updated to iOS 17.3 or later, as the feature isn't available in older versions of iOS. You'll also need to make sure you've set up two-factor authentication and a passcode for your device. Make sure Face ID (or Touch ID) is enabled, too, and that both "Significant Locations" and "Find My" functions are toggled on.

To access the Stolen Device Protection options, tap "Settings" followed by "Face ID & Passcode." Key in your iPhone's login code, then tap "Stolen Device Protection." On the next screen, you'll be able to toggle the feature on or off and can also adjust the security delay by choosing "Away from Familiar Locations" or "Always" from the "Require Security Delay" options.

We were also pleased to learn that if the person who stole your iPhone knows your Apple account sign-in, with Stolen Device Protection enabled, they won't be able to update any of your security settings from a web browser.