# Why iPhone users should turn on the new Stolen Device Protection

January 25, 2024

**Online Desk:** You're in a crowded bar when a thief watches you unlock your iPhone with your passcode, then swipes it. That sinking feeling hits when you realize it's gone, along with priceless photos, important files, passwords on banking apps and other vital parts of your digital life.

Apple rolled out an update to its iOS operating system this week with a feature called Stolen Device Protection that makes it a lot harder for phone thieves to access key functions and settings. Users are being urged to turn it on immediately.

Here's how to activate the new security option and why it's so important:

The software update for iPhones and iPads includes the essential new feature designed to foil thieves from wiping phones for resale or accessing Apple ID or other important accounts. Stolen Device Protection is a new setting that's included with the latest iOS release, version 17.3.

Apple says the feature, buried in your iPhone's settings, adds an extra layer of security for users. It addresses a vulnerability that thieves have discovered and exploited: allowing them to lock victims out of their Apple accounts, delete their photos and other files from their iCloud accounts and empty their bank accounts by accessing passwords kept in the Keychain password manager.

Apple is introducing the feature as anecdotal evidence suggests phone thefts are surging. Stories of stolen phones abound on Reddit groups and in news articles in places from Los Angeles to London, where police say pickpocketing, "table surfing" and moped snatching are common tactics.

The Wall Street Journal reported last year how criminals watched people use their passcodes to gain access to their personal information after stealing their phones.

**HOW DOES STOLEN DEVICE PROTECTION WORK?**

Stolen Device Protection keeps track of a user's "familiar locations," such as their home or workplace, and adds extra biometric security hoops to jump through if someone tries to use the device to do certain things when it's away from those places.

It also reduces the importance of passcodes, which thieves can steal by peering over someone's shoulder or threatening and forcing victims to hand them over, in favor of "biometric" features such as faces or fingerprints that are a lot harder to duplicate.

Let's say the bar thief that snatched your iPhone tries to erase its contents and settings to sell it. With Stolen Device Protection turned on, the phone will now require a Face ID or Touch ID scan to verify that person is the rightful owner.

And that's the only way — the new feature doesn't let someone use the passcode or any other backup method.

Other actions that will trigger this feature if it's not at a familiar place include using passwords saved in Keychain or payment methods saved in Safari, turning off Lost Mode, applying for a new Apple Card or using the iPhone to set up a new device.

There’s also a second layer designed to slow down thieves trying to access critical security settings. If someone tries to, say, sign out of an Apple ID account, change the passcode or reset the phone while it’s in an unfamiliar location, they’ll have to authenticate using Face ID or Touch ID, wait an hour, then do a second facial or fingerprint scan.

Changing an Apple ID password, updating Apple ID security settings, adding or removing Face or Touch ID, and turning off the Find My device feature or Stolen Device Protection also will trigger this feature.

“The security delay is designed to prevent a thief from performing critical operations so that you can mark your device as lost and make sure your Apple account is secure,” the company said. “When your iPhone is in a familiar location, these additional steps will not be required and you can use your device passcode like normal.”