iOS 26—3 iPhone Settings To Change Now, Security Experts Say

Summary

Three iPhone settings to change for enhanced security and privacy: enable Advanced Tracking and Fingerprinting Protection for all browsing in Safari, set Wired Accessories to “Ask for New Accessories” or “Always Ask” to prevent data exfiltration, and enable “Automatically Install” for Background Security Improvements to ensure critical security fixes are downloaded and installed.

Zak Doffman Nov 12, 2025 at 07:50am EST

Check your settings now.
NurPhoto via Getty Images

Despite what you might have read, iPhone remains ahead of Android when it comes to your security and privacy. And while much of this is obvious — locked down app installs and tracking transparency, Safari versus other browsers and permission warnings, to name just a few, here are three other settings hidden away and less well understood.

Let’s start with Apple’s defence against the “pervasive and hidden tracking" that was has returned with the unleashing of digital fingerprinting this year. Unlike cookies which can be easily disabled, this works by collecting lots of unrelated data points about your device, and assembling them into a unique fingerprint to identify you.

Forbes Google Chrome Secretly Tracks Your Phone — How To Stop It By Zak Doffman

Fortunately, Apple users are protected in Safari by a novel technique that throws a mass of misleading data at your browser, making it near impossible for trackers to collate real data and build a unique, trackable profile. Before iOS 26, this was applied just to private browsing. But now it *should be* the default for all browsing. Check your setting now.

Go to **Settings** > **Apps** > **Safari** > **Advanced** > **Advanced Tracking and Fingerprinting Protection**, and make sure it’s selected for “**All Browsing**.”

Next we come to Apple's new protection against the use of physical cable connections to exfiltrate your data, even if you think you're just charging your iPhone. This defends against so-called juice jacking, highlighted again this year with a new TSA warning.

As long as you have an iPhone with a USB-C port, rather than an older lightning port, you can stop your iPhone making any unexpected, data connections. Go to **Settings** > **Privacy & Security** > **Wired Accessories**. Make sure this is set to "**Ask for New Accessories**" or "**Always Ask**." The default is "Automatically Allow When Unlocked," which is dangerous. So this is a setting you need to change.

Finally for now, we have Apple's newest security improvement. This one needs iOS 26.1, installed. and it enables your iPhone to download and install critical security fixes without you having to do anything. Change the setting now, if it's not enabled.

The Prompt: Get the week's biggest AI news on the buzziest companies and boldest breakthroughs, in your inbox.

Forbes Yes, Google Warns All Gmail Users To Stop Using Passwords — Act Now By Zak Doffman

Go to **Settings** > **Privacy & Security** again, but this time select "**Background Security Improvements.**" All you need to do is make sure the toggle is set on for "**Automatically Install**" and Apple will do the rest. The newly updated feature hasn't been used yet, but will make a huge difference with urgent fixes that must be deployed quickly.

Next time we'll look at other iPhone settings that will help you stay safe from scams, rogue calls, malware-laced texts and phishing emails.