[To view the original source article, please click here.]

Forbes Apple Update Warning For All iPhone 17, 16 And 15 Users—Act Now

Zak Doffman Nov 28, 2025 at 05:11am EST

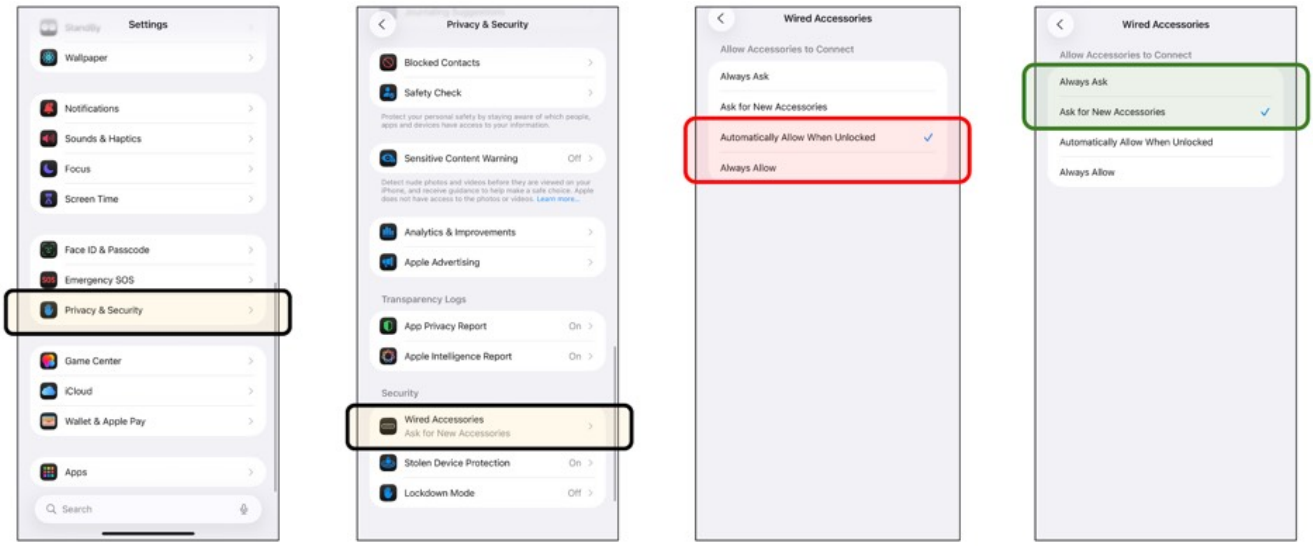
Your phone is at risk — make this change now.
SOPA Images/LightRocket via Getty Images

Apple does not make mistakes often — but it has done so now. If you have an iPhone 17, 16 or 15, then there's a hidden setting you must change. It has been set to a dangerous default, and leaves your phone open to attack. It takes seconds to fix — do that now.

The warning stems from the iOS 26 update in September. This introduced much needed protection against the risk of data being secretly extracted from an iPhone through a malicious charging cable or accessory. But it has been set up badly.

…

After you first unlock your iPhone after it's reset or switched on, it can be connected to a USB accessory or computer. Before it's unlocked that first time it won't connect. That's why Apple added a controversial 72 hour time-out, returning untouched phones to their before first unlock (BFU) state to prevent forensic software extractions.



Wired accessory protection
iOS 26 / @UKZak

With iOS 26, Apple went further. Adding additional defenses for iPhones with USB-C ports, enabling users to prevent a rogue cable connection stealing data or worse. This affects iPhone 15s and newer, after the company moved away from Lightning ports.

Apple offers options to “always ask” whether you want a connection to be to ask for “new accessories.” That should be the default, “ask for new accessories.” But it’s not. Apple has set the default to “automatically allow when unlocked.” That means that once a phone is unlocked it will connect to any USB-C accessory that’s plugged in.

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

Changing the setting is easy. Go to **Settings** > **Privacy & Security** > **Wired Accessories**, and then select either “**Always Ask**” or “**Ask for New Accessories.**”

A critical reminder as to why this is critical has just been posted on X. “WhatsApp end-to-end encryption Vs forensic extraction” points out the exposure of data on your phone once the phone is unlocked, the data decrypted, and then the contect exfiltrated.

“Although WhatsApp uses end-to-end encryption to protect messages, calls, and shared media during transmission, this protection only applies while the data is moving between devices. Once the content reaches the device, it is stored unencrypted within WhatsApp’s local databases and media folders.”

…

As I’ve warned many times before, end-to-end encryption only protects against man-in-the middle attacks intercepting content on a network (as in Salt Typhoon) or server-side, which is why Telegram is less secure than WhatsApp, iMessage or Signal. It does not protect against an endpoint (your phone) being compromised.

Apple’s new protection is excellent — its default setting is not.

Make the change today.