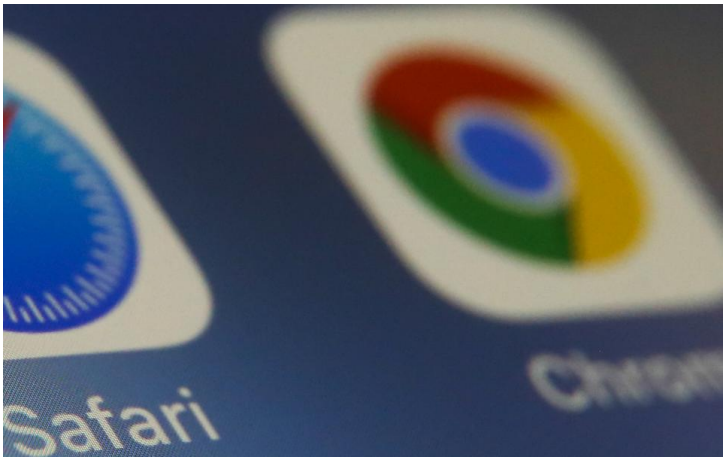
Apple Warns All iPhone Users—Do Not Use Google Chrome

Summary

Apple is urging iPhone users to stop using Google Chrome, highlighting Safari's superior privacy features, including protection against cross-site tracking, IP masking, and malicious extensions. Apple's warnings come as Chrome, despite privacy concerns, continues to gain market share, especially with the introduction of its new AI-powered Gemini upgrade. This upgrade, which will soon be available on iOS, raises further privacy concerns for iPhone users, who may be hesitant to trust Google's AI engagement directly.

Zak Doffman Sep 23, 2025 at 04:30pm EDT



Do you really need to quit Chrome?
NurPhoto via Getty Images

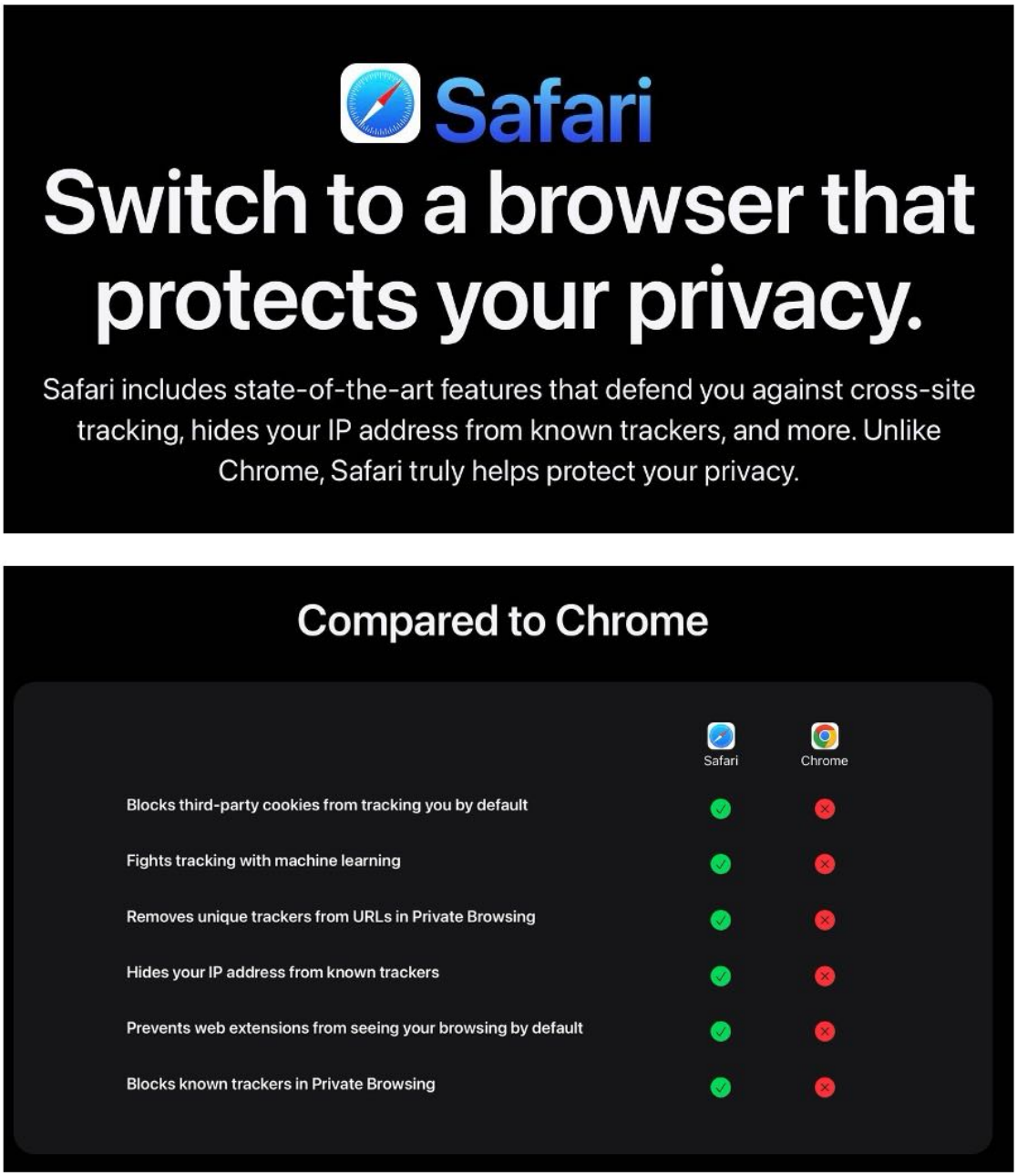
Republished on September 23 with Google's new Chrome AI update and a new privacy warnings for Gemini users carrying across to iPhones.

Apple's warning is clear — stop using Google Chrome. The world's most popular browser is as dominant on mobiles as it is PCs. And right now it's surging, stealing market share from Apple. But Apple is fighting back.

"Switch to a browser that protects your privacy," Apple says. "Safari includes state-of-the-art features that defend you against cross-site tracking, hides your IP address from known trackers, and more. Unlike Chrome, Safari truly helps protect your privacy."

Microsoft is doing the same, warning Windows users to stop using Chrome, interrupting installs with ads for Edge, pushing its "browsing securely" alternative as "the same technology as Chrome, with the added trust of Microsoft." But when it comes to market share, Edge is an also ran. Not so Safari, the default on most — but not all — iPhones.

And Apple goes further. There's a checklist. Safari versus Chrome. This covers tracking cookies, URL trackers, IP masking, malicious extension protection and blocking known trackers. Safari scores all ticks, Chrome scores none. Again, it's the same playbook as Microsoft's, which has its own Edge versus Chrome checklist.



Why you should stop using Google Chrome.
Apple

What isn't covered in Apple's checklist is digital fingerprinting. The secretive device tracking Google brought back from the dead this year, having banned it on privacy grounds. There's no way to switch off this silent tracking, which collates multiple device characteristics into a unique fingerprint to track you across the web.

But Apple *has* found a way to stop it working — at least to an extent. Safari's new "Advanced Tracking and Fingerprinting Protection" has been on by default for private browsing for a while. With iOS 26 it's now on by default for all browsing.

…

This throws junk data at fingerprint trackers when they're detected, making it difficult to identify your own device, to separate the wheat from the chaff. This works in Safari, but if you use Chrome on your iPhone, you're not protected in the same way.

Last year, Apple parodied Google's now failed FLoC (federated learning of cohorts — its first Privacy Sandbox initiative) with "Flock," a play on Hitchcock's "*The Birds*." The video portrayed Safari keeping users safe from other browsers that track their phones.

Apple didn't mention Chrome in its "Flock" video. It didn't need to. Between them, Chrome and Safari control 90% of the mobile browser market. Nothing else matters — yet. But Chrome *is* mentioned on Apple's website, in this clear attack.

Despite Microsoft's warning to Windows users and Apple's warning to iPhone users, Chrome is surging. Users are not deterred. This is an issue for Apple as the browser market becomes the latest to brace for AI disruption. But the iPhone-maker is steadily raising the stakes, doubling down on its warnings, even though it's not yet working.

I have reached out to Google for any comments on Apple's warning.

Forbes FBI Warning — Do Not Use These Websites On Your Phone Or PC By Zak Doffman

Meanwhile, the importance of iPhone to Google when it comes to Chrome is clear for all to see — literally. With the launch of iOS 26 earlier this week," *9to5Google* reports, "Google Chrome 141 rolled out with Liquid Glass tweaks on iPhone and iPad." This means "Chrome is Google's first iPhone app with Liquid Glass."

Chrome on iPhone already has "a pretty different interface and experience from the Android version." And now "the Liquid Glass changes start on the Tab Grid with the Incognito (which is always visible), Tab, and Tab Group switcher, as well as search at the left. Edit and Done also get the same treatment below."

What really matters though is the user capture and stickiness. And with all the excitement around Apple's new iPhone look and feel, Chrome isn't missing out. Google has set out its ambition when it comes to tracking iPhones, with up to 300 million more devices in its sights. As nre AI browsers come to the fore, and Apple eventually sorts out its own AI mess, this will become ever more critical.

But from a privacy standpoint, the difference is as clear as the new display. Per ExpressVPN, "Safari blocks third-party cookies by default and limits how long first-party cookies last. Intelligent Tracking Prevention (ITP) also reduces cross-site tracking and fingerprinting by sharing less information about your device. It even stops social widgets like Facebook Like buttons from tracking you unless you interact with them."

By contrast, “Chrome doesn’t block third-party cookies or fingerprinting by default, so you have to change those settings manually.” And as well we know, almost no users change the default privacy and security settings on any browser. Ever.

The Chrome on iPhone conundrum will now be complicated by Google’s confirmation of the “biggest upgrade to Chrome in its history.” Per *Tech Republic*, this Gemini upgrade will add features “to summarize pages, combat scams, and simplify browsing.”

…

The website reports that “users must opt in the first time they enable Gemini in Chrome, and the feature is not available in Incognito mode. Visual cues such as glowing page edges and a tab icon indicate when content is being shared.”

This comes first to U.S. and desktops, “Support for Android and iOS will arrive soon after,” at which point iPhone users will have a serious decision to make.

Google says “Gemini in Chrome can understand the context of what you’re doing across multiple tabs, answer questions and integrate with other popular Google services, like Google Docs and Calendar. And it’ll be available on both Android and iOS soon, letting you ask questions and summarize pages while you’re on the go.”

And AI also ups security. “None of this matters without safety,” Google says. “We’re continuing to expand the way we use AI to keep you protected: securely filling in login credentials with Chrome autofill, proactively blocking new types of scams, helping you fix security issues like compromised passwords and spammy notifications, and simplifying some privacy decisions like granting sensitive permissions.”

But is it enough for iPhone users when Safari has all those ticks? The issue with Google’s deployment of Google’s AI is the mix-matched privacy policies that apply to different user bases across different apps. It’s like iPhone users will turn to Apple first.

The latest Google AI privacy warning has just been issued. Google’s Nano Banana, it seems, “has quietly turned into 2025’s most dangerous cybersecurity crisis.” At least according to Point Wild’s Lat61 Threat Intelligence Team.

Forbes iOS 26.1 — Apple’s Rapid Security Update For All iPhone Users By Zak Doffman

The team warns “every photo you upload carries what cybersecurity experts call a biometric fingerprint: your unique facial geometry, skin texture, micro-expressions, body proportions, even behavioral patterns like how you hold your phone or typical photo angles. Here’s what you may be handing over:

- Precise GPS coordinates embedded in image metadata
- Device fingerprinting data (phone model, camera specs, OS version)

- Behavioral biometrics and habitual traits
- Social network mapping (who appears in your pictures and relationship dynamics)
- Psychological profiling insights revealed by your creative prompts.”

And that’s the issue for Chrome AI coming to iPhone. Will iPhone users trust the AI engagement from their phones directly into Google’s Gemini offerings rather than via some form of Apple-ised privacy architecture?