PSA: Make sure you have these privacy features enabled on your iPhone

Summary

The article describes three privacy features that iPhone users should enable. These features include preventing cross-site tracking, protecting mail activity, and adjusting lock screen settings. The article also mentions that these features are set to be on by default, but users should double-check their settings to ensure they are enabled.

Table of Contents

Marcus Mendes Aug 2 2025 - 3:34 pm PT

Over the years, Apple has introduced multiple features that help preserve your privacy and curb abusive tracking and data mining from your activity. Here are three settings every privacy-conscious user should have enabled on their iPhone.

Prevent Cross-Site Tracking

When done correctly and responsibly, personalized advertising really can help users find relevant and interesting products online.

However, there is a multibillion-dollar business supported by very invasive tracking methods that really push the limits of what should be acceptable when it comes to collecting data for advertising purposes.

The iPhone's Intelligent Tracking Prevention aims to put a stop to that. It uses machine learning models that Apple developed specifically to nip cross-site tracking at the

bud, and it also hides your IP address, so that, as Apple says, “what you look at on the web remains your business — not an advertiser’s”.

The good news is that this feature is set to be on by default. The bad news is that sometimes, users may accidentally disable it.

To ensure Prevent Cross-Site Tracking is active, go to **Settings > Apps > Safari**, and flip that switch on **Prevent Cross-Site Tracking** in the **Privacy & Security** section.

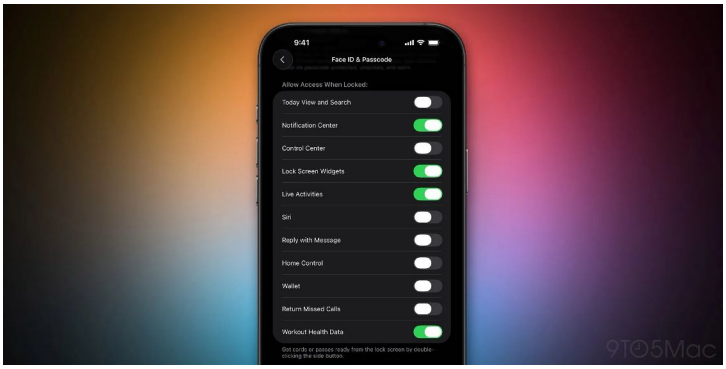
Protect Mail Activity

While it is widely known that advertisers try to track your activity across the web, not everyone knows that sometimes, emails may include trackers as well.

These trackers are used for a variety of reasons, including knowing when you opened an email, how many times you viewed it, whether you forwarded it, and even where you were at the time.

However, if you go to **Settings > Apps > Mail > Privacy Protection**, you can toggle on **Protect Mail Activity**, making it harder for senders to gather information about your behavior, or build a profile about your online habits.

Lock screen settings



Even with Face ID enabled and a strong passcode, bad actors can still exploit what’s available from the lock screen.

For instance, a thief can try to access Control Center from the Lock Screen, and quickly turn off Wi-Fi, Cellular and Bluetooth, before the user has a chance to set the iPhone as lost or look for it via Find My.

Fortunately, Apple lets you fine-tune exactly which features are accessible from the lock screen.

Go to **Settings > Face ID & Passcode**. Once you input your passcode, head down to the **Allow Access When Locked** section to decide what stays available from the lock screen, and what stays off-limits until you unlock your phone.FTC: We use income earning auto affiliate links. More.