Why isn't incognito mode as private as you think?

Is incognito mode on web browsers really safe?

Incognito mode (or private mode) is one of many security features available on modern web browsers. With incognito mode, you are implicitly invulnerable while browsing. You can do whatever you want in incognito mode, and when you close that tab, everything disappears.

Because no browsing history is saved when browsing in incognito mode, you might think you're invulnerable. Many people thought so too, until they actually took the time to understand how incognito mode works and its limitations. It turns out that incognito mode doesn't guarantee private browsing.

How does incognito mode actually work?

Although I no longer use incognito mode, that doesn't mean the feature is useless. Incognito mode, or private browsing mode, is designed to keep your local browsing session secure – but only on your own device. When you open an incognito window, the browser starts a separate browsing session, disconnected from your regular browsing session. This mode temporarily saves everything you do in that session, including browsing history, cookies , and more.

After you close that private session, all that temporary information will be automatically deleted. This information won't show up in your browser history, and anyone who picks up your device afterward won't know what you did. The downside to this mode is that session data and cookies aren't saved to your browser profile. That means if you log into your email, you'll still need to log in the next time because the browser will delete everything in that session after you exit.

Things that anonymity can't do.

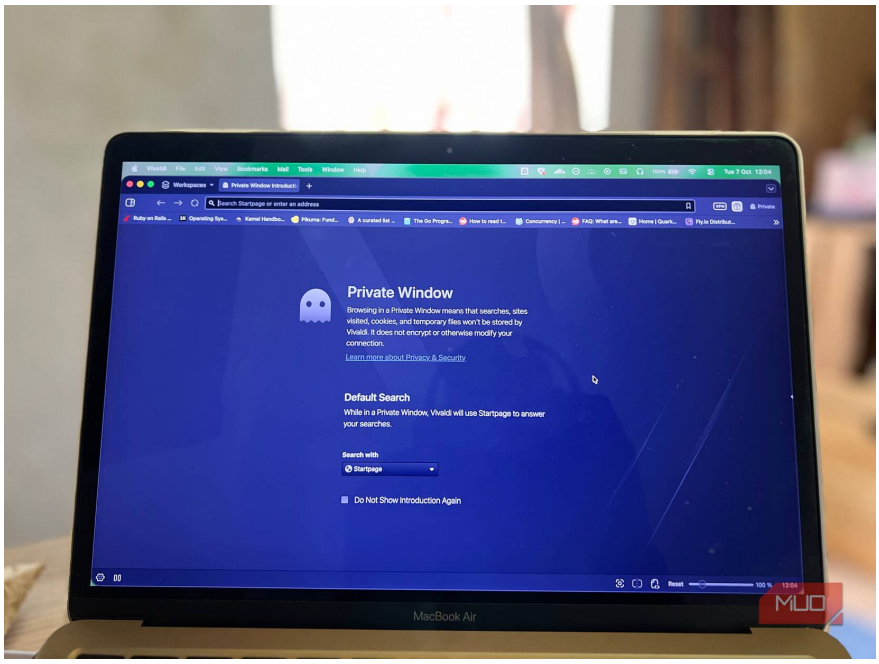
Common misconceptions about anonymity

While incognito mode is useful for keeping your browsing private from other users on the same device, it doesn't make you completely invisible on the internet. Many people assume this mode hides all their online activity, but that's completely untrue.

First, incognito mode doesn't hide your activity from your Internet service provider (ISP). This is because, even with incognito mode, every request you send still goes through your ISP's network (unless you're using an encrypted DNS provider). Suppose your ISP tracks user activity on their network. In that case, they can still

track your activity and know all the domains you visit, and in some cases, even your unencrypted traffic. And if you're using a company Wi-Fi network, the network administrator can also see the websites you visit.

Incognito mode doesn't prevent websites from tracking you. Of course, while cookies are deleted after you exit incognito mode, that's not the only way websites track your online activity. Websites also use device and browser fingerprints, including creating profiles of each user based on unique device characteristics, including screen size and resolution, installed extensions, etc.



Browser fingerprinting can allow websites to track your online activity regardless of whether you're browsing in incognito mode. There are ways to prevent browser fingerprinting, but incognito mode is ineffective. Similarly, using incognito mode won't prevent advertisers from creating profiles of your interests. For example, according to NPR, a class-action lawsuit alleging Google tracked user data in Chrome's incognito mode was settled in late 2023 with the company agreeing to pay $5 billion and promising to delete the data.

Another common misconception is that using incognito mode will hide your IP address. The short answer is no. Your IP address is like your passport to travel in the digital world – incognito mode doesn't change it. So, if you're already blocked by a particular website, using incognito mode to try to access it won't help.

Why should you stop using incognito mode?

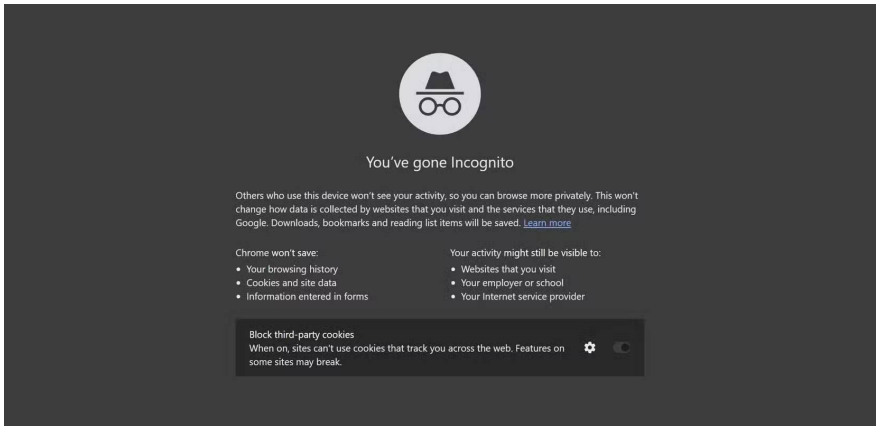
It doesn't meet the needs of many people.

Although browsing in incognito mode often has benefits, many people stop using it after learning the truth. Firstly, it gives you a false sense of privacy. You think your browsing activity is hidden from everyone, but as discussed earlier, that's not true. It turns out your ISP can still track you, and even if you're connected to a public Wi-Fi network, a network administrator or some malicious actor monitoring connected devices can still see the websites you visit.

Incognito mode is really convenient for shared devices – you log into your account, do whatever you want, then when you're finished, close the browsing session and you can continue. The next person won't see your activity. But many people don't see the need to use incognito mode because they don't share their device. Besides, if you want to keep your browsing history and activity private, you can easily do so using other methods.

What alternatives are there to truly protect privacy?

The best ways to hide your online footprint.



If incognito mode doesn't meet your expectations, what should you use? There are a few options to consider that will help protect your privacy better than incognito mode.

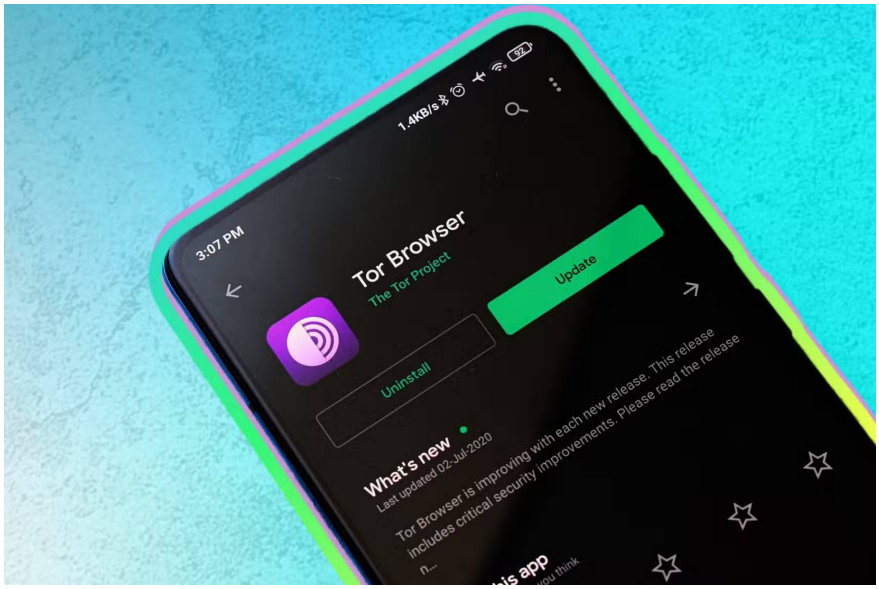
1. Use a VPN

A Virtual Private Network (VPN) is a security tool that serves two main purposes. First, it hides your IP address. Therefore, when you connect to a VPN, a website cannot know your real location. Instead, it only sees the location of the VPN server you are connected to. This is something that incognito mode cannot do.

Secondly, a VPN routes your traffic through an encrypted tunnel, thus concealing your browsing activity and any unencrypted data you exchange online. So, even if you're using your company's Wi-Fi at work, your administrator can't see the websites you visit. But that's just the tip of the iceberg; using a VPN has many more benefits.

2. Use a privacy-focused browser.

Privacy-focused browsers are designed to block trackers, ads, and browser fingerprinting by default, thus offering stronger protection than incognito mode. The Tor browser is a prime example of a browser built with privacy in mind. Tor works by routing your traffic through the Tor network, hiding your IP address and location from websites.



It also automatically deletes your entire browsing history when you exit and blocks trackers by default, offering better privacy than standard web browsers. It also blocks browser fingerprinting by default. Sounds like a scary browser, but it's actually not.

3. Use a private search engine.

Unlike mainstream search engines like Google and Bing, private search engines are far better in terms of privacy because they don't track your searches or store your data. Some good options include DuckDuckGo and Startpage. For example, DuckDuckGo claims that it doesn't store your IP address or track online activity, and that your searches are anonymous.

Additionally, it integrates protection against third-party trackers, thus blocking many trackers on the websites you visit, providing an extra layer of security. On the other hand, Startpage uses proxies to anonymize Google search results, thus also blocking trackers.

Don't rely on incognito mode for security!

Despite its drawbacks and misleading name, incognito mode still has its place. If you share a device, it helps keep your browsing history out of reach of others. It also allows you to log into your services without worrying about others accessing your accounts. But if you want privacy, look for other options.

You can use a VPN to hide your browsing activity from your ISP and conceal your real IP address. Using private search engines like DuckDuckGo and private browsers is also a better alternative to incognito mode.

You finished reading the article "**Why isn't incognito mode as private as you think?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.