# 6 Threats That Incognito Mode Can't Protect You From

No one wants their personal information to be spread all over the internet, that's true. Whether you're planning to buy a gift or your browsing history, there are always reasons to keep it private.

Incognito mode isn't as private as you might think. While it does prevent your browser from saving history and cookies , that's only a small fraction of the tracking it blocks. You're still vulnerable to a number of privacy and security risks. Here are some common threats to watch out for!

## 6. Your Internet Activity Is Not Completely Private to Your ISP

Private browsing does not hide your activity from your Internet Service Provider (ISP). Your ISP can still track the websites you visit, when you visit, and how long you stay because everything you do online is routed through their servers. So they can track your browsing habits if they want to.

So how do you protect yourself? One simple and effective option is to use a VPN (virtual private network) . It encrypts your internet traffic and routes it through a secure server, making it difficult for your ISP to track your activity. However, VPNs have limitations and risks, so you need to be aware of them.

## 5. Others can see your downloaded data

When you download a file during a private browsing session, it's saved to your device just like any regular download. That means that even after you close your incognito window, the files are still accessible on your computer. Unless you manually delete them, anyone using your device can view, open, or move them, putting your sensitive data at risk.

The good news is that your browser won't record these downloads in your history. However, if you're using a public or shared device, you'll need to manually delete these files when you're done. If you need to keep a large downloaded file on a shared device, consider encrypting or password-protecting it to prevent unauthorized access.

## 4. Network administrators can still monitor your browsing activity

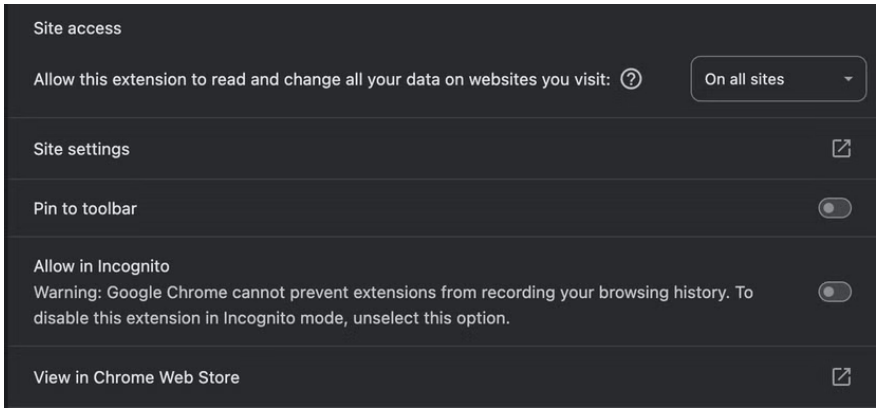
Do you use private browsing mode at work, school, or on public Wi-Fi and think your activity is hidden? Unfortunately, that's not the case. Network administrators, including your IT team, can still track what you do online, even in private mode. So how can you stay off their radar? As mentioned earlier, an easy solution is a VPN (virtual private network).

A VPN creates an encrypted tunnel between your device and the Internet , masking your activity. However, VPNs are often blocked on such networks. In that case, you can try the Tor Browser , which routes your traffic through several encrypted nodes to help maintain privacy. Alternatively, you can use the Brave browser's privacy mode with Tor.

## 3. Browser extensions may collect your data

By default, browser extensions are disabled during private browsing sessions — but you can choose to enable them. If you've allowed certain extensions to run in private mode, they can collect data about the websites you visit and your actions. So even if you think your activity is private, these extensions can still track you in the background.

In Chrome, you can see which extensions are running in private mode by clicking the Extensions icon near the main menu. To stop extensions from running, go to the Extensions page, click Details for the extension you want to restrict, and turn off the setting that allows extensions to run in Incognito mode. You can easily manage this permission in other browsers.



## 2. Incognito mode doesn't protect you from malware

When you first start using Incognito mode, many people believe that they are completely protected from online threats. But if you think that, you are wrong. Incognito mode does not protect you from malicious websites, risky downloads, or harmful scripts. If you interact with dangerous content, your device will be just as vulnerable as it would be in a regular browsing session.

That's why you should follow all standard security precautions when browsing privately. Scan suspicious files and links with tools like VirusTotal, keep malware protection on, and don't disable your browser's built-in security and privacy features. Be as cautious when using private mode as you would when browsing normally!

## 1. Websites Can Still Track and Identify You

When you browse in private mode, websites can still detect your IP address and collect device-specific information to build a unique profile of you. This means you can still be targeted with ads. If you log in to accounts like Google or Facebook while in Incognito mode, your activity can still be associated with your account or profile.

While it's hard to eliminate this type of tracking, you can minimize it by using privacy-focused browsers like Brave . Also, don't log in to your main account when browsing in private mode. For example, if you just want to watch a YouTube video or look at your Facebook or Instagram profile, doing so without logging in won't affect your main account.

There you have it! These are some of the major threats that private browsing mode doesn't protect you from. If you had any misconceptions about being completely protected, now you have a better understanding. Follow the tips we've shared to protect your data, privacy, and security. While these precautions don't eliminate all risks, they do help to greatly reduce them.

similar articles on tips and guides. Thank you for reading and for following us regularly.