

1. How can browser extensions pose security risks?

Browser extensions can access sensitive data such as browsing history, login details, and personal information. Malicious ones can inject ads, track users, or even steal credentials, making them a potential security threat.

2. What permissions should raise suspicion?

Permissions like 'Read and change all your data on the websites you visit' or access to cookies, clipboard, and file system should raise suspicion. These permissions often indicate that an extension might misuse user data.

3. How to safely install browser extensions?

Always install extensions from official stores like Chrome Web Store or Firefox Add-ons. Check reviews, download count, developer reputation, and requested permissions before installing.

4. What is extension sandboxing?

Extension sandboxing isolates the extension's code from the main browser environment. This limits what the extension can access, reducing the risk of malicious code affecting other tabs or the system.

5. Can extensions steal passwords?

Yes, poorly designed or malicious extensions can capture login forms and saved passwords. That's why granting access only to trusted extensions and monitoring their permissions is crucial.

6. How to update extensions securely?

Enable automatic updates through your browser settings or manually check for updates from the official extension page. Avoid downloading updates from third-party sites or suspicious links.

7. Difference between extensions and plugins?

Extensions modify or enhance browser functionality using web technologies like HTML, CSS, and JavaScript. Plugins, on the other hand, handle specific content types (like Flash or Java) and operate outside the browser's core sandbox.

8. How to report malicious extensions?

You can report suspicious extensions directly through the browser's extension store page. Most browsers offer a 'Report Abuse' or 'Flag as Malicious' option to alert security teams for review.