

Identify and Remove Suspicious Browser Extensions

By- Dhruv Bhatia

Objective:




To learn how to identify, review, and remove potentially harmful browser extensions, improving awareness of browser security risks and best practices.

Introduction:

Web browsers are essential tools that allow users to access and interact with content on the internet. To enhance functionality, most browsers support **extensions** or **add-ons**—small software modules that can add features like ad blocking, password management, or productivity tools. However, not all extensions are safe. Some may request excessive permissions or behave maliciously, posing serious security and privacy risks.

This task focuses on identifying and removing such suspicious browser extensions. By learning how to manage browser add-ons effectively, users can significantly reduce their exposure to malware, phishing, and data theft.

Tools Used to execute the task:

Browser:  Google Chrome (also applicable for  Firefox,  Edge, etc.)

Steps Performed:

1. Accessed the Extensions Page

- Navigated to: chrome://extensions/
- Opened the browser’s extension manager to review all installed extensions.

2. Reviewed Each Extension

- Checked each extension’s name, description, publisher, and permissions.
- Verified user reviews and the number of downloads via the Chrome Web Store.
- Noted any unfamiliar or suspicious extensions.

3. Identified Suspicious/Unused Extensions

Extension Name	Reason for Concern	Action Taken
PDF Converter Pro	Unknown source, high permissions	Removed
Weather Extension	Requested access to all website data	Removed
Grammarly	Verified, from trusted publisher	Retained

4. Removed Unwanted Extensions

- Uninstalled unnecessary and suspicious extensions using the “Remove” button.
- Restarted the browser to ensure changes were applied.

5. Post-Removal Verification

- Rechecked performance and verified no suspicious background activity.
- Noted slight improvement in browser speed and responsiveness.

How To Identify Malicious Browser Extensions ?

1. Check the Source and Publisher

- Only install extensions from official web stores (e.g., Chrome Web Store or Firefox Add-ons).
- Verify the developer's identity and check if they are well-known or trusted.

2. Analyze Permissions

- Be cautious of extensions that request broad or unnecessary permissions like:
 - "Read and change all your data on the websites you visit"
 - "Manage your downloads"
 - "Access your clipboard"
- If the permissions do not match the extension's function, it's a red flag.

3. Review Ratings and User Feedback

- Look for:
 - Low ratings or excessive negative reviews
 - Reports of suspicious behavior or hijacking search engines
 - Sudden drop in user trust

4. Monitor Extension Behavior

- Watch out for:
 - Unexpected ads or pop-ups
 - Redirection to unwanted sites
 - Slower browser performance
 - Changes in search engine or homepage

5. Check for Frequent Name Changes

- Some malicious extensions change names frequently to evade detection.

6. Search for Threat Reports

- Google the extension name with keywords like "malware," "spyware," or "data leak" to check for any known threats or articles.

7. Use Browser Security Tools

- Use built-in browser tools or third-party extension checkers to scan for risky behavior.