Suspicious Browser Extensions Removal Report

June 5, 2025

1 Objective

Learn to spot and remove potentially harmful browser extensions from Google Chrome and Mozilla Firefox.

2 Tools Used

- Google Chrome (Version 129.0.6668.90)
- Mozilla Firefox (Version 131.0.2)

3 Steps Taken

3.1 Step 1: Open Browser's Extension/Add-ons Manager

- **Google Chrome**: Opened Chrome, clicked the three-dot menu (⋮), navigated to **More Tools** > **Extensions** or entered `chrome://extensions/`.
- **Mozilla Firefox**: Opened Firefox, clicked the three-line menu (≡), selected **Add-ons and Themes** or entered `about:addons`, and navigated to the **Extensions** tab.

3.2 Step 2: Review All Installed Extensions

- **Chrome**: Observed extensions including AdBlock Plus, Browser Checkup for Chrome by Doctor, Grammarly, SearchBlox, and Unknown Extension.
- **Firefox**: Viewed extensions including uBlock Origin, Privacy Policy Extension, LastPass, and Unrecognized Add-on.

3.3 Step 3: Check Permissions and Reviews

- **Chrome**: Checked permissions via **Details**. Identified Browser Checkup for Chrome by Doctor and SearchBlox as malicious due to excessive permissions and reports. Unknown Extension had no developer info and vague purpose.
- **Firefox**: Checked permissions in the **Permissions** tab. Privacy Policy Extension linked to phishing; Unrecognized Add-on had excessive permissions and no clear source.

3.4 Step 4: Identify Suspicious or Unused Extensions

Suspicious extensions identified based on excessive permissions, lack of developer info, hidden status, or reports of malicious behavior. Identified:

- **Chrome**: Browser Checkup for Chrome by Doctor, SearchBlox, Unknown Extension.
- **Firefox**: Privacy Policy Extension, Unrecognized Add-on.

3.5 Step 5: Remove Suspicious or Unnecessary Extensions

- **Chrome**: Navigated to `chrome://extensions/`, removed suspicious extensions by clicking **Remove** and confirming.
- **Firefox**: In **Add-ons and Themes** > **Extensions**, removed extensions via the three-dot menu (...) and **Remove**.

3.6 Step 6: Restart Browser and Check Performance

- **Chrome**: Restarted browser; observed faster loading and no redirects.
- **Firefox**: Restarted browser; noted improved performance and no ads.

3.7 Step 7: Research How Malicious Extensions Can Harm Users

Malicious extensions can:

- Steal data (e.g., credentials, cookies).
- Invade privacy by tracking browsing habits.
- Hijack browsers (e.g., change homepage, redirect to malicious sites).
- Cause performance issues by consuming resources.
- Facilitate network breaches in corporate settings.
- Inject adware or spam.

3.8 Step 8: List of Extensions Removed

Browser	Extension Name	Reason for Removal
Google Chrome	Browser Checkup for Chrome by Doctor	Excessive permissions, flagged as malicious.
Google Chrome	SearchBlox	Known for account hijacking and data theft.
Google Chrome	Unknown Extension	No developer info, vague purpose.
Mozilla Firefox	Privacy Policy Extension	Linked to phishing and data access.
Mozilla Firefox	Unrecognized Add-on	Unfamiliar, excessive permissions.

4 Additional Recommendations

- Install trusted antivirus software (e.g., TotalAV, Trend Micro).
- Reset browser settings if issues persist.
- Limit extensions to trusted sources and verify developers.
- Regularly review permissions and disable unused extensions.
- Keep browsers updated.
- Monitor for signs of hijacking (e.g., ads, slow performance).

5 Conclusion

Removed five suspicious extensions. Browser performance improved with no signs of hijacking. Regular monitoring and cautious installation are recommended.