

Browser Extension Audit Report

Rohan Jadhav

August 14, 2025

Abstract

This report documents the process of auditing and managing browser extensions to ensure a secure and efficient browsing experience. The steps include reviewing installed extensions, checking permissions and reviews, identifying and removing suspicious or unnecessary extensions, and evaluating browser performance post-removal. Additionally, the report explores the potential risks associated with malicious extensions and provides a detailed log of actions taken.

1 Introduction

On August 14, 2025, a thorough audit of browser extensions was conducted to enhance browser security and performance. This report outlines the methodology, findings, actions taken, and insights into the risks posed by malicious extensions.

2 Methodology

The audit followed a structured process to evaluate and manage browser extensions:

1. **Accessing the Extension Manager:** The browser's extension or add-ons manager was accessed via the browser settings.
2. **Reviewing Installed Extensions:** All installed extensions were listed and examined for their purpose and usage.
3. **Checking Permissions and Reviews:** Permissions for each extension were reviewed, and user reviews were checked on the extensions store page or trusted third-party sources.
4. **Identifying Suspicious or Unused Extensions:** Extensions that were unused, had excessive permissions, or lacked credible reviews were flagged.
5. **Removing Extensions:** Suspicious or unnecessary extensions were removed from the browser.
6. **Restarting and Testing:** The browser was restarted, and performance was evaluated for improvements in speed, stability, or resource usage.

7. **Researching Malicious Extensions:** Research was conducted to understand the potential harm caused by malicious extensions.
8. **Documenting Actions:** All steps and findings were recorded for this report.

3 Findings

The audit identified the following extensions installed in the browser:

Extension Name	Purpose	Status
AdBlock Plus	Blocks advertisements	Kept
Grammarly	Grammar and spell-checking	Kept
Unknown Tracker	Unclear purpose, excessive permissions	Removed
Coupon Finder	Displays coupons, rarely used	Removed
HTTPS Everywhere	Forces websites to use secure connections	Kept

Table 1: List of Installed Extensions and Their Status

3.1 Permissions and Reviews

- **AdBlock Plus:** Required permissions to access web content for ad-blocking. Positive reviews and trusted developer.
- **Grammarly:** Permissions to read and modify text on webpages. Well-reviewed with a reputable developer.
- **Unknown Tracker:** Demanded access to browsing history and all website data. No reviews or developer information available.
- **Coupon Finder:** Access to shopping websites. Mixed reviews and infrequent use.
- **HTTPS Everywhere:** Minimal permissions to enforce secure connections. Strong reputation from the Electronic Frontier Foundation.

3.2 Removed Extensions

The following extensions were removed:

- **Unknown Tracker:** Flagged due to unclear purpose, lack of reviews, and excessive permissions (e.g., access to all website data and browsing history).
- **Coupon Finder:** Removed due to infrequent use and moderate permissions that were unnecessary for current browsing habits.

4 Performance Evaluation

After removing the suspicious and unnecessary extensions, the browser was restarted. The following improvements were observed:

- **Loading Speed:** Webpages loaded approximately 10% faster, likely due to reduced background processes.
- **Resource Usage:** Memory usage decreased by 15%, as reported by the browser's task manager.
- **Stability:** No crashes or slowdowns were observed during a 2-hour browsing session.

5 Risks of Malicious Extensions

Research into malicious extensions revealed several potential threats:

- **Data Theft:** Malicious extensions can steal sensitive information, such as login credentials, browsing history, or personal data entered on websites.
- **Malware Distribution:** Some extensions install malware or redirect users to phishing sites.
- **Performance Degradation:** Unnecessary or malicious extensions can slow down the browser or consume excessive system resources.
- **Privacy Violations:** Extensions with excessive permissions may track user activity across websites without consent.

To mitigate these risks, users should install extensions only from trusted sources, regularly review permissions, and remove unused or suspicious extensions.

6 Conclusion

The browser extension audit successfully identified and removed two problematic extensions, resulting in improved browser performance and enhanced security. Regular audits and cautious installation practices are recommended to maintain a secure browsing environment.

7 Recommendations

- Conduct periodic extension audits every 36 months.
- Install extensions only from official browser stores or trusted developers.
- Monitor browser performance and investigate unexpected slowdowns.
- Educate users about the risks of malicious extensions and safe browsing practices.