

Internship Report - Task 7

Identification and Removal of Suspicious Browser Extensions

1. Objective

The objective of this assessment was to examine installed browser extensions, identify unnecessary or suspicious items, and remove them to mitigate potential security and performance risks.

2. Scope

- Browser extensions installed on the system under review.
- Evaluation of extension permissions, usage, and legitimacy.
- Research into potential threats posed by malicious or unverified extensions.

3. Methodology

- Accessed the browser's Extension/Add-on Manager.
- Conducted a review of all installed extensions.
- Verified permissions requested by each extension.
- Cross-checked necessity, origin, and credibility of extensions.
- Removed extensions deemed suspicious or obsolete.
- Restarted browser and observed performance changes.

4. Findings

Extension Name	Status	Observations	Action Taken
Free Coupons Finder	Suspicious	Requested access to browsing history and site data on all websites.	Removed
Old Screenshot Tool	Obsolete	Functionality now included in browser; extension no longer in use.	Removed
Ad Blocker	Trusted	Legitimate, widely used, requires minimal permissions.	Retained
Password Manager	Trusted	Verified developer, essential security tool, permissions justified.	Retained

5. Risks of Malicious Extensions

Research confirmed that malicious browser extensions may:

- Steal sensitive credentials and financial information.
- Collect and sell browsing history without consent.
- Inject advertisements or redirect users to unsafe websites.
- Degrade browser speed and system performance.

6. Recommendations

- Perform regular audits of installed browser extensions.
- Only install extensions from official web stores after reviewing developer credibility and permissions.
- Avoid granting unnecessary permissions (e.g., full access to all websites).
- Keep extensions updated through official channels.
- Report suspicious or malicious extensions to the browser vendor.

7. Interview Preparation (Reference Q&A)

Q1. How can browser extensions pose security risks?

They can access sensitive data, execute malicious scripts, or compromise privacy.

Q2. What permissions should raise suspicion?

Permissions such as “Read and change data on all websites” or “Access browsing history” without clear justification.

Q3. How to safely install browser extensions?

Use official extension stores, verify developer reputation, read user reviews, and review requested permissions.

Q4. What is extension sandboxing?

A containment method that restricts an extension’s ability to interfere with the system or other applications.

Q5. Can extensions steal passwords?

Yes, if granted access to site content, they may capture login details.

Q6. How to update extensions securely?

Enable automatic updates or update manually from the official store. Avoid third-party sources.

Q7. Difference between extensions and plugins?

Extensions enhance browser functionality; plugins are external software modules used to handle specific content types.

Q8. How to report malicious extensions?

Report through the official extension store (e.g., Chrome Web Store “Report Abuse” option).

8. Conclusion

The audit resulted in the removal of two unnecessary extensions, reducing potential security vulnerabilities and improving browser performance. Remaining extensions were deemed safe and essential. Regular monitoring and responsible installation practices are strongly recommended for continued security.