

Task 7: Identifying and Removing Suspicious Browser Extensions

Objective

To review, identify, and remove potentially harmful browser extensions, and to understand the risks associated with malicious extensions.

1. Accessing Extension Manager

- **Google Chrome:**
Navigated to `chrome://extensions/` via the menu (**More Tools > Extensions**).
- **Mozilla Firefox:**
Navigated to **Menu > Add-ons and themes > Extensions**.

2. Review of Installed Extensions

- Examined all installed extensions for:
 - Unfamiliar or unused extensions.
 - Extensions with vague or generic names.
 - Extensions requesting excessive permissions (e.g., access to all browsing data, ability to modify website content).
 - Poor user reviews or low ratings.
 - Sudden changes in browser behavior (pop-ups, redirects, slowdowns).

3. Permission and Review Check

- For each extension, reviewed:
 - The permissions requested (e.g., access to all websites, reading clipboard data).
 - The developer's reputation and extension reviews in the Chrome Web Store or Firefox Add-ons site.

4. Identification and Removal

- Identified the following suspicious or unnecessary extensions:
 - Example 1:** “PDF Converter Pro” – Unfamiliar, excessive permissions, poor reviews.
 - Example 2:** “Super Shopping Deals” – High access permissions, caused pop-up ads.
- Removed these extensions using the browser’s extension manager^{[6][7][1]}.
- Restarted the browser to ensure changes took effect.

5. Post-Removal Checks

- Monitored browser performance and verified that pop-ups and redirects ceased.
- Noted a noticeable improvement in browser speed and fewer unwanted ads.

List of Suspicious Extensions Removed

Extension Name	Reason for Removal	Permissions Requested
PDF Converter Pro	Unfamiliar, poor reviews, excessive access	Read/modify all data on websites
Super Shopping Deals	Caused pop-ups, intrusive ads	Access to browsing history, all URLs

Risks of Malicious Browser Extensions

- Data Theft:** Can steal passwords, financial info, and personal data.
- Credential Harvesting:** Some extensions log keystrokes or capture login credentials.
- Browser Hijacking:** May redirect searches, change homepages, or inject ads.
- Malware Spread:** Can download and install additional malware or spyware.
- Performance Issues:** Poorly designed or malicious extensions can slow down the browser and system.
- Excessive Permissions:** Extensions requesting more access than necessary can be abused for malicious purposes

Best Practices Learned

- **Install only essential, reputable extensions.**
- **Review permissions before installing; avoid extensions that request unnecessary access.**
- **Regularly audit and remove unused or suspicious extensions.**
- **Check developer reputation and user reviews.**
- **Keep browser and extensions up to date.**
- **Be wary of sudden changes in browser behavior, which may indicate a malicious extension.**