

Task 7: Identify and Remove Suspicious Browser Extensions

Objective

Learn to detect and remove potentially harmful browser extensions that may compromise user security, privacy, or browser performance.

Tools Used

- Google Chrome (or any Chromium-based browser)
 - Mozilla Firefox
 - Web research tools (for verifying extensions)
-

Step-by-Step Guide

Step 1: Open the Browser Extension/Add-on Manager

Chrome:

- Navigate to `chrome://extensions` in the address bar.
- Alternatively: Click the 3-dot menu (top-right) → More Tools → Extensions.

Firefox:

- Navigate to `about:addons` in the address bar.
- Or use the menu (☰) → Add-ons and Themes → Extensions.

This view shows all extensions currently installed in the browser.

Step 2: Review All Installed Extensions

Carefully examine each extension. Note:

- Extension name
- Developer or publisher name
- Last updated date
- Total number of users and ratings
- Permissions granted (access to browser data, history, etc.)

Check for red flags:

- Unfamiliar or strange names
 - Recently added without user awareness
 - Outdated extensions (not updated in over a year)
 - Poor or no user ratings
-

Step 3: Check Permissions and Research Each Extension

Click on “Details” or “More” to view:

- Permissions requested
- Homepage and support links
- Privacy policy availability

If permissions include:

- Access to all site data
- Reading clipboard
- Controlling downloads
- Running in incognito

...then further investigation is needed.

Search online:

- Google extension name + “malware” or “spyware”
 - Check Reddit or security forums
 - Use antivirus browser scanners
-

Step 4: Identify Suspicious or Unnecessary Extensions

Flag extensions that:

- Are unfamiliar or not installed intentionally
- Provide vague descriptions
- Have no visible reviews or are rated poorly
- Request permissions beyond their purpose

Extensions offering utility (e.g., "free VPN", "coupon finder") are often bundled with tracking scripts or adware.

Step 5: Remove Suspicious or Unused Extensions

Click **Remove** on each:

- Red-flagged extension
- Any unused plugin that hasn't been active recently

Disabling is temporary. For security, it's recommended to **fully remove**.

Step 6: Restart the Browser

- Close all browser windows and reopen.
 - This ensures removed extensions are completely deactivated.
 - Observe if:
 - The browser starts faster
 - Tabs load more quickly
 - CPU or memory usage decreases
-

Step 7: Research the Impact of Malicious Extensions

Learn how harmful extensions can affect users:

- **Keylogging** – capturing typed data including passwords
- **Session hijacking** – stealing cookies and login tokens
- **Redirects** – altering search results or loading unwanted ads
- **Data harvesting** – sending browsing history to unknown servers

Use resources like:

- [Google Safe Browsing](#)
 - [Mozilla Extension Warnings](#)
 - Security blogs (Malwarebytes, BleepingComputer)
-

Step 8: Document the Process

Suspicious Extensions Found & Removed

Extension Name	Status	Reason for Removal
Dark Mode Pro	Removed	Unknown developer, excess permissions
Quick Shopping Now	Removed	Redirects search queries, poor reviews
Grammarly	Kept	Verified, widely trusted and used

Summary of Actions Taken


1. Opened Chrome extensions manager.
2. Identified 6 installed extensions.
3. Found 2 suspicious based on permissions and lack of trust.
4. Verified with online reviews and removed both.
5. Restarted browser and confirmed quicker tab loading.
6. Studied threats from malicious extensions.

Conclusion

This task emphasizes the importance of digital hygiene. Regularly auditing browser extensions helps minimize attack vectors. Many users unknowingly run vulnerable extensions, but with basic awareness, they can take control of their privacy and performance.

By performing this task, you now understand:

- How to inspect, evaluate, and remove browser add-ons
- Which red flags to look for
- How malicious extensions operate in the background

 A secure browser begins with only trusted, necessary extensions.