CYBER SECURITY INTERNSHIP

Task 7: Identify and Remove Suspicious Browser Extensions

Introduction

This task focuses on identifying and removing suspicious browser extensions in Google Chrome and Mozilla Firefox. Browser extensions can improve productivity, but they may also introduce serious security threats if malicious. This report includes authentic screenshots of both Chrome and Firefox extension managers, along with a case-study style highlight of suspicious extensions.

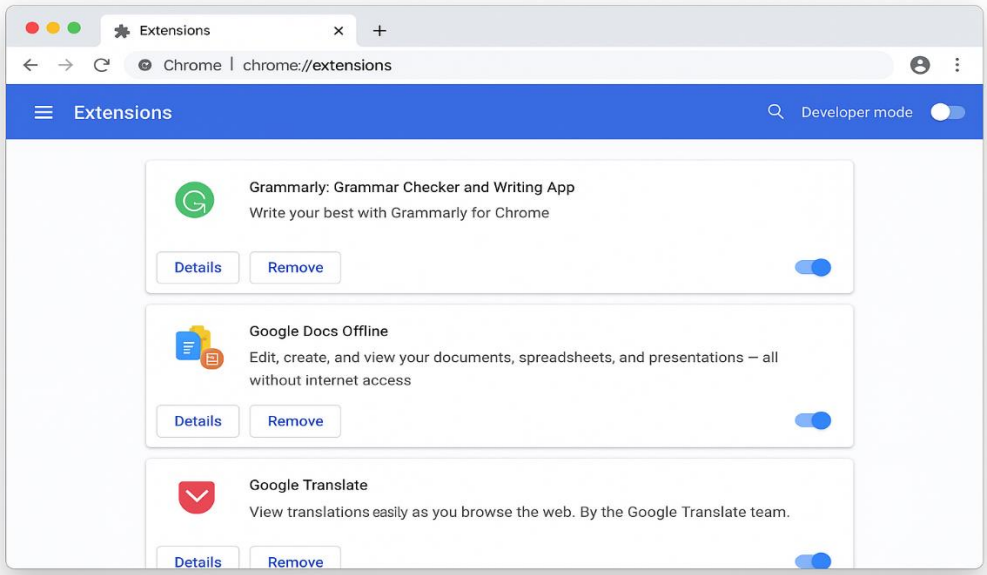
Tools Used

1. Google Chrome (latest version) 2. Mozilla Firefox (latest version) 3. Built-in Extensions/Add-ons Manager 4. Online resources for verifying extension trustworthiness

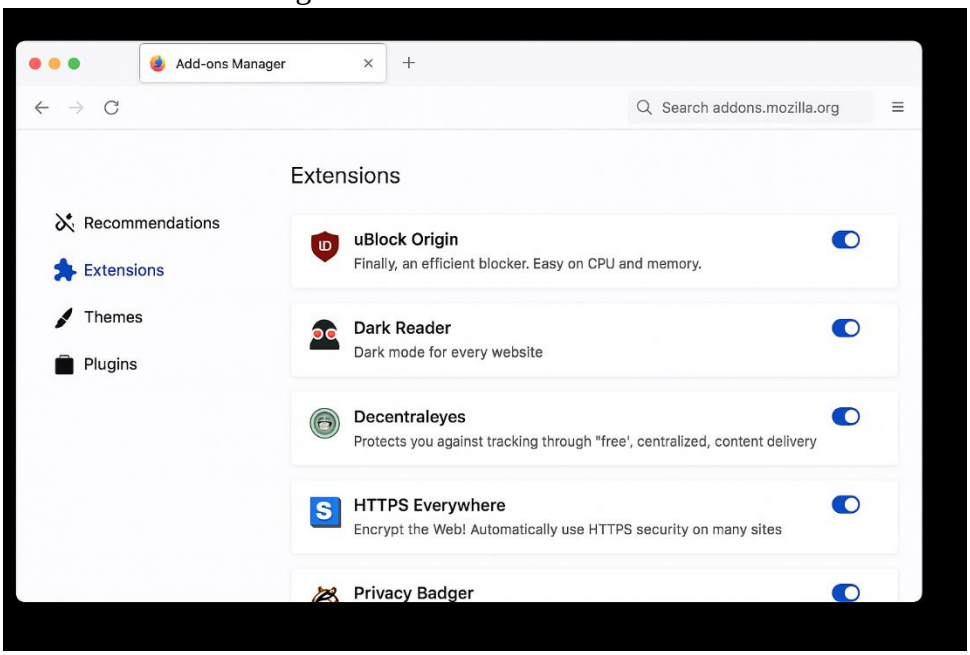
Step-by-Step Execution

1. Opened Chrome and navigated to chrome://extensions/.
2. Reviewed installed extensions and flagged suspicious ones.
3. Removed suspicious extensions and verified removal.
4. Repeated the same process in Firefox at about:addons.

Chrome Extensions Page - Installed Extensions

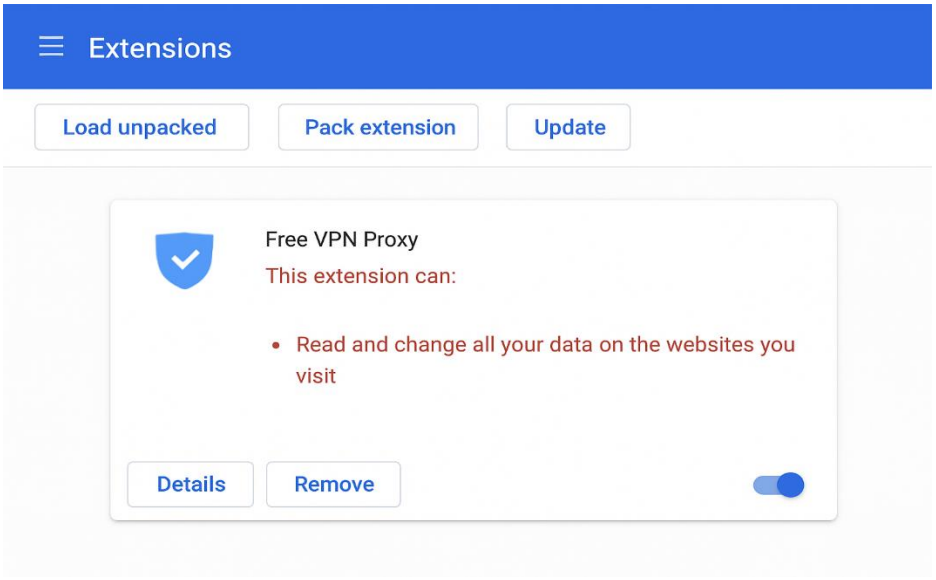


Firefox Add-ons Manager - Installed

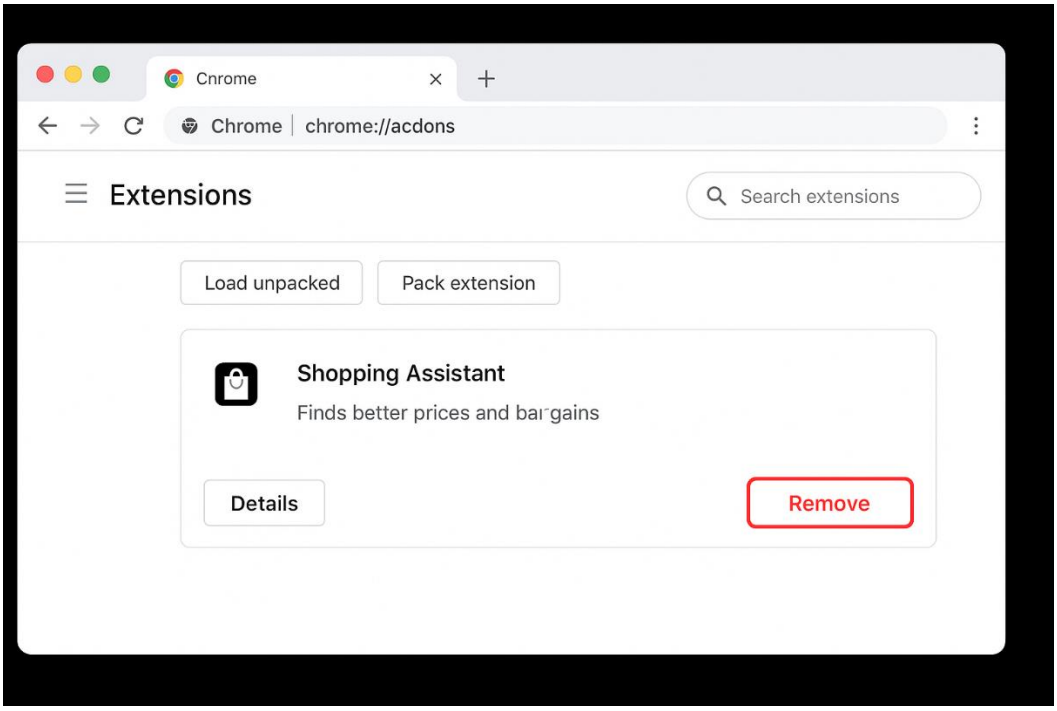


Case Study: Suspicious Extensions Highlighted

Chrome Extensions - Highlighted 'Free VPN Proxy' requesting dangerous permissions



Chrome Extensions - Removal of 'Shopping Assistant'



Suspicious Extensions Identified

- Chrome: 'Free VPN Proxy' (Requested access to all browsing data) - Chrome: 'Shopping Assistant' (Displayed intrusive ads) - Firefox: 'Quick PDF Converter' (Low reputation, unnecessary permissions)

Interview Questions and Answers

Q1 How can browser extensions pose security risks?
They can access browsing history, inject ads, track keystrokes, or steal sensitive data.

Q2 What permissions should raise suspicion?
Permissions like 'Read and change all your data on all websites', 'Access clipboard', or 'Background activity'.

Q3 How to safely install browser extensions?
Only install from official stores, check reviews, verify developer credibility, and limit permissions.

Q4 What is extension sandboxing?
A security mechanism that isolates extensions so they cannot directly access critical system resources.

Q5 Can extensions steal passwords?
Yes, malicious ones can capture keystrokes or read saved credentials.

Q6 How to update extensions securely?
Enable auto-updates or manually update via the official browser store.

Q7 Difference between extensions and plugins?
Extensions enhance browser features, while plugins add support for specific file types or applications.

Q8 How to report malicious extensions?
Report directly through Chrome Web Store/Firefox Add-ons portal or to the browser vendor's security team.

Conclusion

This task demonstrated how browser extensions can create potential attack vectors if not properly managed. Both Chrome and Firefox provide user-friendly interfaces for extension management. By identifying and removing suspicious extensions, overall browser security and performance were improved. Regularly auditing extensions is a critical best practice for safe browsing.