■■ Task 7 Report
Identify and Remove Suspicious Browser Extensions

■ Student Name
Jasmine Nisha (Jas Nisha)

■ Task Title
Task 7 – Identify and Remove Suspicious Browser Extensions

■ Objective
The objective of this task is to identify potentially harmful or unnecessary browser extensions, understand the security risks associated with them, and remove suspicious extensions to enhance browser security and overall performance.

■ Tools Used
• Mozilla Firefox Browser
• Google Chrome Browser
• Microsoft Edge Browser

■ Step-by-Step Procedure

Step 1: Review Extensions in Mozilla Firefox
The Mozilla Firefox browser was opened, and the Add-ons and Themes → Extensions section was accessed to review all installed extensions.

Installed Firefox Extensions Observed:
1. FoxyProxy – Used for advanced proxy management
2. Notefox: Website Notes – Used for taking notes directly on websites

Each extension was analyzed based on its purpose, permissions, and trust level. No suspicious behavior or unnecessary permissions were identified.

Step 2: Review Extensions in Microsoft Edge
The Microsoft Edge Add-ons section was reviewed to check installed extensions and recommended add-ons.
• Only trusted and well-known extensions were visible
• No unknown or suspicious extensions were found installed

Step 3: Review Extensions in Google Chrome
The Chrome Extensions → Manage Extensions page was opened to examine installed extensions.

Installed Chrome Extensions:
1. LinkedIn Extension – Provides LinkedIn notifications and activity alerts
2. Google Docs Offline – Allows offline access to Google Docs

Step 4: Identification of Suspicious Extension (Educational Purpose)
For learning and internship task demonstration purposes, the LinkedIn Extension was selected for further analysis.

Reasons for marking it as suspicious (for educational demonstration):
• Runs continuously in the background
• Has access to browsing-related activity
• Not frequently used

Step 5: Removal of Suspicious Extension
The LinkedIn Extension was removed to demonstrate the process of eliminating unnecessary or potentially risky extensions.

Steps followed:
• Clicked on the Remove option
• Confirmed the removal
• Restarted the browser

Step 6: Final Verification
After restarting the browser:
• No suspicious extensions were found
• Browser performance remained stable
• Only trusted extensions were active

■ Summary of Findings
Firefox – No suspicious extensions – Extensions reviewed
Microsoft Edge – No suspicious extensions – Store reviewed
Google Chrome – Yes (LinkedIn Extension – learning purpose) – Removed

■ Key Concepts Learned
• Browser extensions can pose serious security risks
• Excessive permissions may lead to data exposure
• Malicious extensions can track browsing activity or steal sensitive data
• Regular auditing of browser extensions is essential for secure browsing

■ Outcome
By completing this task, I gained practical awareness of browser security risks and learned how to identify, analyze, and remove suspicious browser extensions. This task improved my understanding of secure browsing practices and browser extension management.