# Task 7: Identify and Remove Suspicious Browser Extensions

## Objective:

Learn to spot and remove potentially harmful browser extensions.

## Tools:

Any web browser (Chrome, Firefox).

## Steps Taken:

1. Opened the browser’s extension/add-ons manager.

2. Reviewed all installed extensions carefully.

3. Checked permissions and reviews for each extension.

4. Identified unused or suspicious extensions.

5. Removed suspicious or unnecessary extensions.

6. Restarted the browser and checked for performance improvements.

7. Researched how malicious extensions can harm users.

## List of Suspicious Extensions Found and Removed:

No malicious extensions were found during this inspection. However, 2 unused extensions were removed to improve browser performance.

## Research: How Malicious Extensions Can Harm Users

Malicious browser extensions can perform harmful actions such as:  
- Stealing sensitive data like passwords and credit card details.  
- Tracking browsing history and personal activities.  
- Injecting unwanted advertisements or redirecting websites.  
- Downloading malware without user consent.  
These threats highlight the importance of regularly reviewing and removing unnecessary or untrusted extensions.

## Outcome:

Gained awareness of browser security risks and the importance of managing browser extensions to maintain privacy, security, and browser performance.