Task 7: Identify and Remove Suspicious Browser Extensions

1. **Opened the Browser's Extension/Add-ons Manager:**

- I started by opening my browser's extension manager to review all installed extensions.
- I accessed the extensions by clicking on the three vertical dots (menu) in the top-right corner, then going to More Tools > Extensions.
- **Mozilla Firefox**: I accessed the extension page by clicking on the three horizontal lines (menu) in the top-right corner, selecting Add-ons and themes, and then selecting the Extensions tab.

2. **Reviewed All Installed Extensions:**

- After opening the extension manager, I thoroughly reviewed all the installed extensions in browsers Mozilla Firefox.
- I checked for any extensions that were unfamiliar, seemed suspicious, or appeared unnecessary.

3. **Checked Permissions and Reviews:**

- For each extension, I checked the permissions to ensure they only requested access that was relevant to their function. Any extension asking for excessive permissions, such as access to all websites or personal data, was considered suspicious.
- I also searched online for reviews and ratings of the extensions to determine their trustworthiness. This step was essential in identifying potentially harmful extensions.

4. **Identified Suspicious or Unused Extensions:**

- I took note of any extensions that I did not recognize or extensions that appeared unnecessary. I also looked for extensions with poor reviews or those that requested unnecessary permissions.
- Since I found no extensions installed on my browser, I moved on to the next step.

5. **Removed Suspicious or Unnecessary Extensions:**

- In cases where I would have found suspicious or unused extensions, I would have removed them by clicking Remove next to each extension in Mozilla Firefox.
- Since no extensions were found on my browser, there were no extensions to remove.

6. **Restarted Browser and Checked for Performance Improvements:**

- After reviewing extensions and confirming there were no extensions installed, I restarted the browser.
- Since there were no extensions to remove, I didn't notice any performance improvements. However, restarting the browser is always a good practice for improving overall performance.

7. **Researched How Malicious Extensions Can Harm Users:**

- I researched the potential risks of malicious browser extensions. Malicious extensions can:
    - **Steal personal data**, such as login credentials, credit card information, or browsing history.
    - **Inject ads** or change search engine settings to redirect traffic to unwanted sites.
    - **Track user activity** without consent, compromising user privacy.
    - **Install malware** on the computer or browser, leading to further security risks.