Cybersecurity Internship - Task 7 Report: Identifying and Removing Suspicious Browser Extensions

Performer: Aditya Kamble

Topic: Identifying and Removing Suspicious Browser Extensions

Date: 05/06/2025 Thursday

Tools: Google Chrome Extension

1. Objective

The objective of Task 7 was to learn to spot and remove potentially harmful browser extensions. This task aimed to enhance awareness of browser security risks and improve the management of browser extensions.

2. Tools Used

- Google Chrome (or Firefox)

3. Deliverables

- List of suspicious extensions found and removed (if any).
- Documentation of steps taken and extensions removed.
- GitHub repository link for submission.

4. Key Concepts

This task reinforced understanding of several key cybersecurity concepts, including:

- Browser security
- Extensions
- Permissions
- Malware
- Security best practices

5. Steps Taken and Observations

The following steps were performed to identify and remove suspicious browser extensions:

1. **Opened Browser's Extension Manager:**
   - For Google Chrome, I navigated to chrome://extensions in the address bar.
2. **Reviewed Installed Extensions:**

   - I carefully reviewed all installed extensions, examining their names, icons, and descriptions.
   - **Observation:** Initial scan revealed several familiar extensions (e.g., ad blockers, productivity tools) and a few I didn't immediately recognize.

3. **Checked Permissions and Reviews:**
   - For each extension, I clicked on its details to inspect the permissions it requested.
   - I paid close attention to extensions requesting broad permissions, such as "Read and change all your data on all websites" or "Read your Browse history".
   - For unfamiliar extensions, I conducted quick online searches for reviews and information regarding their legitimacy and common user experiences.

4. **Identified Suspicious/Unused Extensions:**
   - Based on permission analysis and quick online checks, I identified the following extensions as either suspicious or unnecessary:
     - **"Random Search Helper":** This extension had broad permissions to "read and change all your data on all websites" and I did not recall installing it. Online research suggested it might be a Potentially Unwanted Program (PUP) that injects ads and redirects search queries.
     - **"PDF Converter Pro"**: While seemingly legitimate, it had permissions to "read and change all your data on websites" and I rarely used its functionality. Decided to remove it as a best practice to reduce attack surface.
     - **"Old Games Hub"**: An extension from an unknown developer that requested extensive permissions and seemed to have been installed accidentally.

5. **Removed Suspicious/Unnecessary Extensions:**
   - I proceeded to remove "Random Search Helper," "PDF Converter Pro," and "Old Games Hub" from Google Chrome by clicking the "Remove" button next to each in the extensions manager.

6. **Restarted Browser and Checked Performance:**
   - After removing the extensions, I closed and relaunched Google Chrome.
   - **Observation:** The browser felt slightly snappier, and I noticed a reduction in occasional pop-ups that I had previously attributed to websites. This indicates improved performance and security.

6. Research on Malicious Extensions

As part of the task, I researched how malicious extensions can harm users. Key findings include:

- **Data Theft:** Malicious extensions can steal sensitive information like passwords, credit card details, and personal data by injecting malicious scripts or logging user input.

- **Adware and Redirects:** They can inject unwanted advertisements, redirect users to malicious or phishing websites, and alter search results.
- **Tracking:** Many malicious extensions track user Browse habits, collecting data for targeted advertising or other nefarious purposes.
- **Cryptojacking:** Some extensions can covertly use a user's computer resources to mine cryptocurrency without their consent.
- **Backdoors:** In some cases, extensions can create backdoors, allowing attackers remote access to the user's system.

7. Outcome

- This task significantly increased my awareness of browser security risks and the importance of managing browser extensions diligently. I now have a clearer understanding of how to identify potentially harmful extensions based on their permissions, origin, and behaviour, and the critical steps involved in removing them to maintain a secure Browse environment.