Task 7: Identify and Remove Suspicious Browser Extensions

Name: G Vishwak

Date: 03-07-2025

Objective

Learn how to identify and remove potentially harmful browser extensions that may compromise privacy, security, or performance.

Tools Used

Google Chrome (same process applies for Firefox/Edge)

Steps Taken

1. Opened Extension Manager:
   - Chrome: chrome://extensions/
   - Firefox: about:addons

2. Reviewed Installed Extensions:
   - Checked each extension's name, publisher, and description.
   - Verified number of downloads, ratings, and user reviews from Chrome Web Store or Mozilla Add-ons.

3. Checked Permissions:
   - Looked for permissions like:
     - 'Read and change all your data on the websites you visit'
     - 'Access your clipboard'
     - 'Monitor browsing activity'

4. Identified Suspicious or Unused Extensions:
   - Unfamiliar names or vague descriptions.
   - High permissions with unclear purpose.
   - No or poor user reviews.
   - Last updated years ago.

5. Removed Extensions:
   - Clicked 'Remove' for extensions flagged as suspicious or unused.

6. Restarted Browser:
   - To ensure performance resets and updates took effect.

7. Checked Performance & Behavior:

  - Faster load times.

  - No pop-ups or redirects.

  - Cleaner browsing interface.

8. Researched Impact of Malicious Extensions:

  - Can log keystrokes or steal passwords.

  - Inject ads or redirect searches.

  - Slow down browser or cause crashes.

  - Serve as spyware or part of botnets.

Suspicious Extensions Removed (Example)

Extension Name	Issue Identified	Action Taken
PDF Converter Pro	Too many permissions, poor reviews	Removed
Easy Weather Tracker	Unknown source, injected ads	Removed
Tab Organizer Pro	Never used, unnecessary	Removed

Post-Cleanup Improvements

Faster browser startup.

Fewer crashes.

Improved tab loading speed.

No unexpected ads/pop-ups.

Outcome

Gained awareness of browser security risks, improved system performance, and learned to safely manage browser extensions.