Task 7 :Identify and Remove Suspicious Browser Extensions

➢ Ways How Malicious Extensions Harm Users -

1. Data Theft

- **Access to all sites**: Many extensions request permissions like "Read and change all your data on the websites you visit".
- **Credential harvesting**: They can monitor form fields (usernames, passwords) and exfiltrate credentials.

2. Session Hijacking

- Extensions can read session cookies or tokens stored in the browser and send them to an attacker.
- This allows hijacking of authenticated sessions (e.g., banking, Gmail, social media).

3. Browser Hijacking

- **Search engine redirection**: Altering search engine results or default search provider.
- **Homepage manipulation**: Setting malicious homepages with ads or phishing links.
- **Ad injection**: Injecting ads or affiliate links into legitimate web pages.

4. Surveillance & Keylogging

- Extensions can log every keystroke and mouse movement.
- Screenshots or clipboard data may be captured silently.

5. Phishing & Malware Delivery

- Injects phishing forms into trusted sites.
- Replaces or adds links to malicious downloads.
- Opens background tabs to drive-by download pages or exploit kits.

➢ Steps Taken :

1. Accessed chrome://extensions/.
2. Reviewed all installed extensions manually.
3. Checked extension permissions and user reviews.
4. Evaluated necessity and security posture of each extension.
5. Removed any that appeared unnecessary or had questionable behavior.
6. Restarted browser and confirmed stability/performance.

➢ Extensions Removed :

Date: 2025-07-03
Browser: Chrome

Actions Taken :

- Removed 2 extensions
- Restarted browser
- Noted slight performance improvement.

These are Extensions **:**

- **"AdBlock" –**

  Permissions:
  - Read and change all your data on all websites
  - Display notifications.

- **"WA Plus" –**

  Permissions:
  - Know your email address.