**TASK 7: Identify and Suspicious Browser Extensions**

**How Malicious Browser Extensions Can Harm Users**

Malicious browser extensions pretend to be useful tools but can secretly perform harmful activities. Some common risks include:

1. Data Theft
   * Can read everything you type, including passwords, credit card details, and personal messages.
   * May steal stored autofill data like names, phone numbers, and addresses.
2. Browsing History Tracking
   * Monitors every site you visit.
   * Builds a detailed profile of your interests for targeted ads or selling to third parties.
3. Ad Injection & Pop-Ups
   * Inserts unwanted ads into websites.
   * Redirects you to phishing or scam sites.
4. Security Bypass
   * Disables security warnings or changes browser settings to make you more vulnerable.
5. System Performance Issues
   * Uses excessive memory or CPU, making your browser slow.
   * Runs background scripts even when the browser is closed.
6. Remote Control of Browser
   * Malicious developers can push updates to add new harmful functions without your consent.

**Document steps:**

Date: 15 Aug 2025

Browser Used: Google Chrome

**Steps Taken:**

* Opened chrome://extensions/.
* Reviewed all installed extensions.
* Checked permissions and searched online for suspicious names.
* Identified unused or risky extensions.
* Removed suspicious extensions.
* Restarted browser.
* Researched risks of malicious extensions.

**Extensions Removed:**

* WebAdvisor Extension – Removed due McAfee to being unused and causing potential browser slowdowns.

**Performance After Removal:**

* Browser loads faster.
* Reduced background process.

**Conclusion:**

Regularly reviewing browser extensions helps prevent security risks and improves performance.