Task 7: Identify and Remove Suspicious Browser Extensions

Objective

Understand how browser extensions can pose a threat to online privacy and security, and learn to identify and remove risky ones.

Tools Used

- Google Chrome browser

- Built-in Extension Manager

- Google Search for verification

Steps Followed

1. Opened the Chrome Extension Manager via chrome://extensions.

2. Reviewed the following extensions:

   - Cisco Webex Extension - Safe, official.

   - Google Docs Offline - Trusted by Google.

   - Grammarly - Legitimate writing tool.

   - Dualless - Removed; unused and minimal benefit.

   - WPS PDF - Disabled due to excessive permissions and flagged reports.

   - Norton Safe Web - Disabled; redundant with existing antivirus.

3. Removed/disabled the suspicious ones to enhance privacy and reduce potential attack vectors.

4. Restarted the browser to apply changes.

Learnings

- Extensions can run in the background even when inactive.

- Over-permissioned extensions are a big red flag.

- Always install from known developers and check reviews.

- Less is more: only keep essential extensions.