✅ Task 7 Report: Identify and Remove Suspicious Browser Extensions

🎯 Objective:

To learn how to detect and remove browser extensions that may pose a security risk.

🧰 Tools Needed:

- **Any Web Browser (Google Chrome or Mozilla Firefox)**

📝 Steps to Perform the Task:

1. Open Extensions Manager

- Chrome: Click ⋮ > Extensions > Manage Extensions
  Or directly go to: chrome://extensions/
- Firefox: Click ≡ > Add-ons and themes > Extensions

---

2. Review Installed Extensions

- **Go through the list of all extensions.**
- **Ask yourself:**
  - Did I install this?
  - Do I use it regularly?
  - Is it from a trusted developer?

---

3. Check Permissions and Reviews

- **Look for extensions asking excessive permissions (like reading all your data on all websites).**
- **Google the extension name + "review" to check if others reported it as malicious or unnecessary.**

---

4. Identify Suspicious/Unused Extensions

- **Examples of suspicious signs:**
  - Poor reviews or no reviews

    - Strange names
    - Unknown publisher
    - Asking for access to all data without a valid reason
    - You don't remember installing it

---

5. Remove Unnecessary or Harmful Extensions

- **Click on "Remove" next to each untrusted or unused extension.**

---

6. Restart the Browser

- **After removal, close the browser and reopen it to ensure everything runs smoothly.**

---

7. Document the Task

Prepare a short report with:

- Extensions found installed
- Which ones were suspicious
- Which were removed
- Reasons for removal
- Improvement after removal (if noticed)

# What I Researched on my browser:

Browser Used: Google Chrome (or Firefox – replace as needed)

Extensions Found:

1. Grammarly – Verified and Safe
2. Adblock Plus – Trusted and widely used
3. Google Docs Offline – Developed by Google
4. Dark Reader – Open-source and well-reviewed

Extensions Removed:
None – All extensions were verified to be safe and necessary.

Actions Taken:

- Opened extension manager and reviewed all installed extensions.
- Checked publisher details and permission levels for each extension.
- Read online reviews and verified legitimacy from trusted sources.
- No suspicious or unnecessary extensions found.
- Restarted the browser to confirm performance remains optimal.

Risks of Malicious Extensions (researched):
Malicious browser extensions may:

- Track browsing behavior
- Steal sensitive information like passwords or credit card details
- Redirect websites or show malicious ads
- Slow down browser performance

Conclusion:
All installed browser extensions were reviewed and found to be safe. No action was required. The task helped reinforce the importance of regularly auditing browser extensions for improved security and performance.

# Here’s an example of sample report.

Browser Used: Google Chrome

Extensions Found:

1. Grammarly – Safe

2. Adblock Plus – Safe

3. PDF Viewer – Suspicious

4. Weather Checker – Suspicious

Extensions Removed:

- **PDF Viewer –** Unknown publisher, required access to all data

- **Weather Checker –** No reviews, didn’t remember installing

Actions Taken:

- **Removed suspicious extensions.**

- **Restarted browser.**

- **Observed faster performance and fewer pop-up ads.**

Risks of Malicious Extensions:

Malicious extensions can collect sensitive data, redirect traffic, show ads, or install malware.
