**Task 7 :Identify and Remove Suspicious Browser Extensions**

1. **Open Extensions Manager**

 Chrome: Menu (⋮) → More Tools → Extensions

 Firefox: Menu (☰) → Add-ons and themes → Extensions

1. Review All Installed Extensions

 Look for names you don’t recognize.

 Check when they were installed (recent unknown ones = red flag).

1. Check Permissions

* “Read and change all your data on all websites”
* “Replace your homepage or new tab”
* “Read and change your bookmarks/history”
* “Capture clipboard” or “Manage downloads” unnecessarily

1. Look Up Extensions Online

Search "<extension name> malware" or "<extension name> privacy issues".

1. Decide Which to Remove

 Remove **unused extensions** (even if safe, unused = attack surface).

 Remove **suspicious ones** (bad reviews, shady developer, unnecessary permissions).

1. Remove Extensions

Click **Remove/Delete** in the manager

1. Research – How Malicious Extensions Can Harm Users

Malicious or overly-permissioned browser extensions can:

* **Steal sensitive data** – login credentials, cookies, browsing history.
* **Inject ads or redirect traffic** – replacing search results with ads or phishing sites.
* **Hijack browser settings** – change homepage, search engine, or new tab page.
* **Track user activity** – collect data for profiling or selling to third parties.
* **Install additional malware** – download harmful scripts or open backdoors.
* **Slow down system performance** – by running hidden background tasks.

Document – Steps Taken & Extensions Removed.

**Steps Taken:**

1. Opened extensions manager.
2. Reviewed all installed extensions.
3. Checked permissions and online reviews.
4. Identified unused/suspicious extensions.
5. Removed unnecessary or risky ones.
6. Restarted browser and tested performance.

**Extensions Removed:**

* [Extension Name 1] – Reason (e.g., excessive permissions, unused, negative reviews).
* [Extension Name 2] – Reason.

**Result/Observations:**

* Browser runs faster / fewer pop-ups / cleaner homepage.
* Reduced privacy/security risks.















