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

**Objective:** Learn to spot and remove potentially harmful browser extensions.

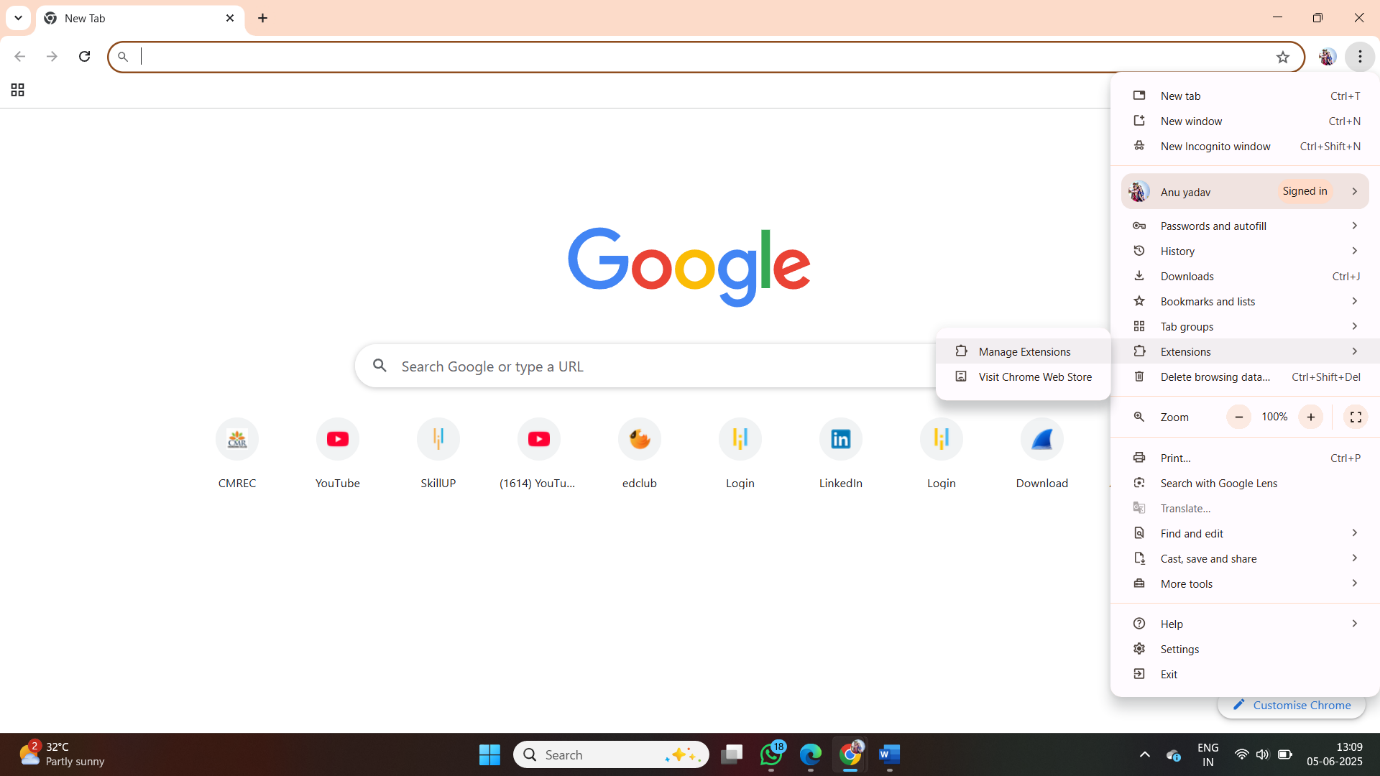
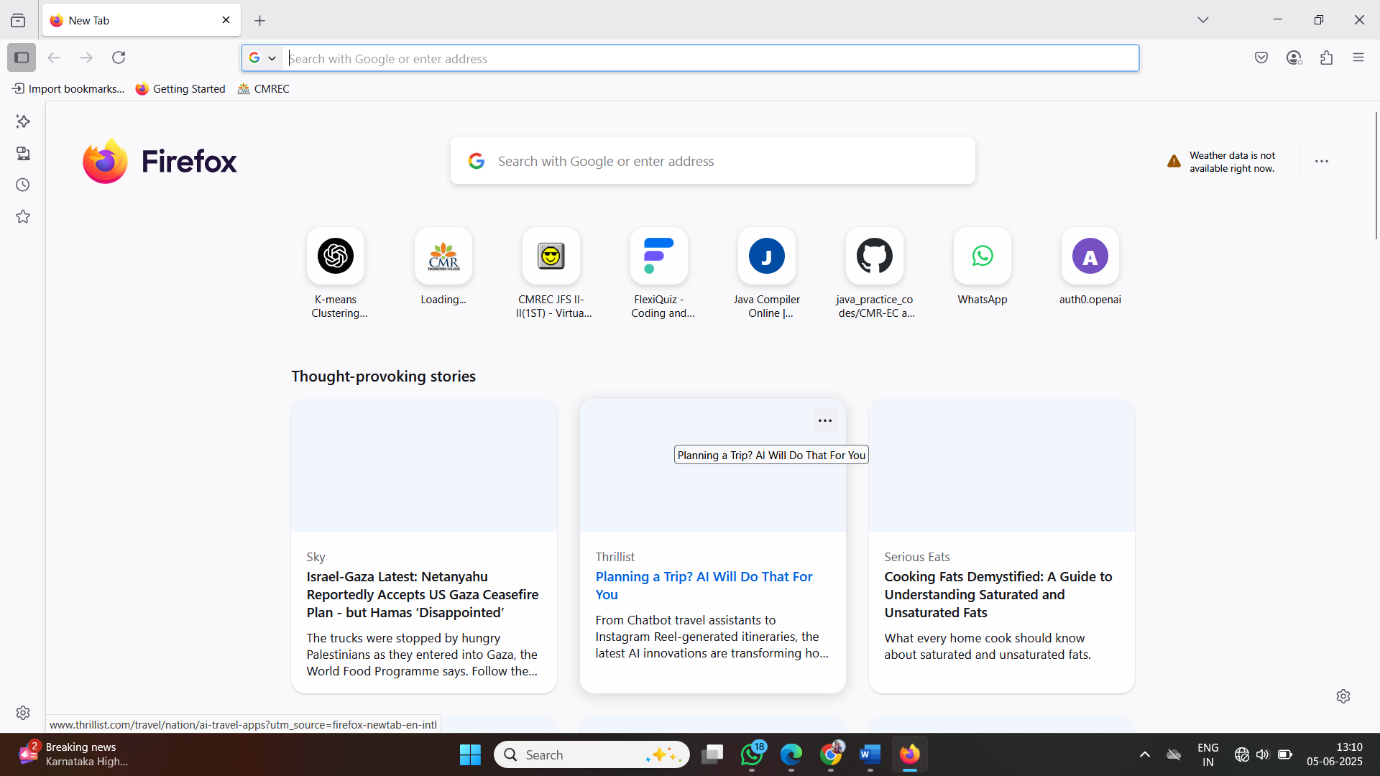
**Tools:** Any web browser (Chrome, Firefox)

**Deliverables:** List of suspicious extensions found and removed (if any)

**PROCEDURE:**

**Step 1: Open Extension/Add-ons Manager**

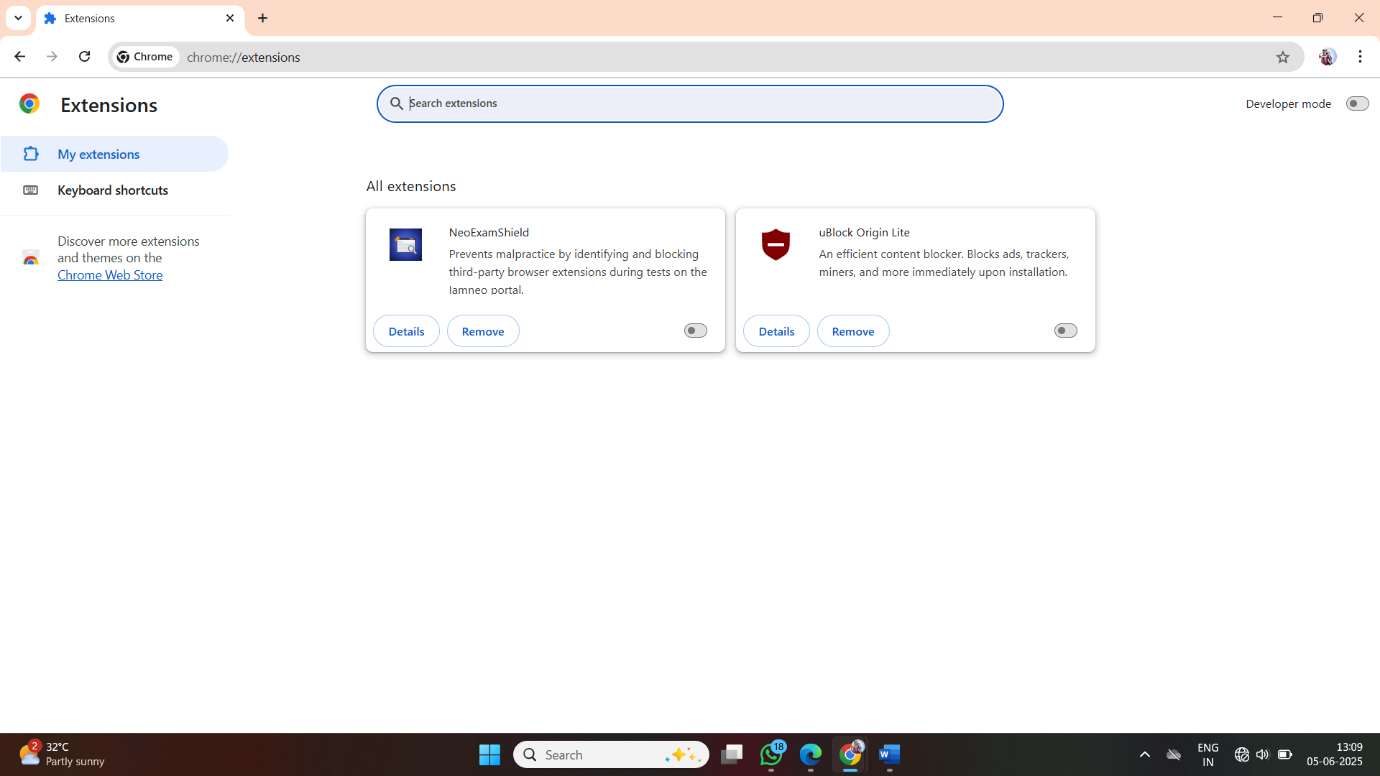
**Why:** This is the control panel where all browser extensions (or add-ons) are listed. You can manage, disable, or remove them here.

* **In Chrome:**
  + Click the three dots menu (⋮) at the top-right corner.
  + Go to Extensions > Manage Extensions, or directly open: chrome://extensions/
* 
* **In Firefox:**
  + Click the menu icon (☰).
  + Go to Add-ons and Themes > Extensions, or open: about:addons
* 

**Step 2: Review All Installed Extensions**

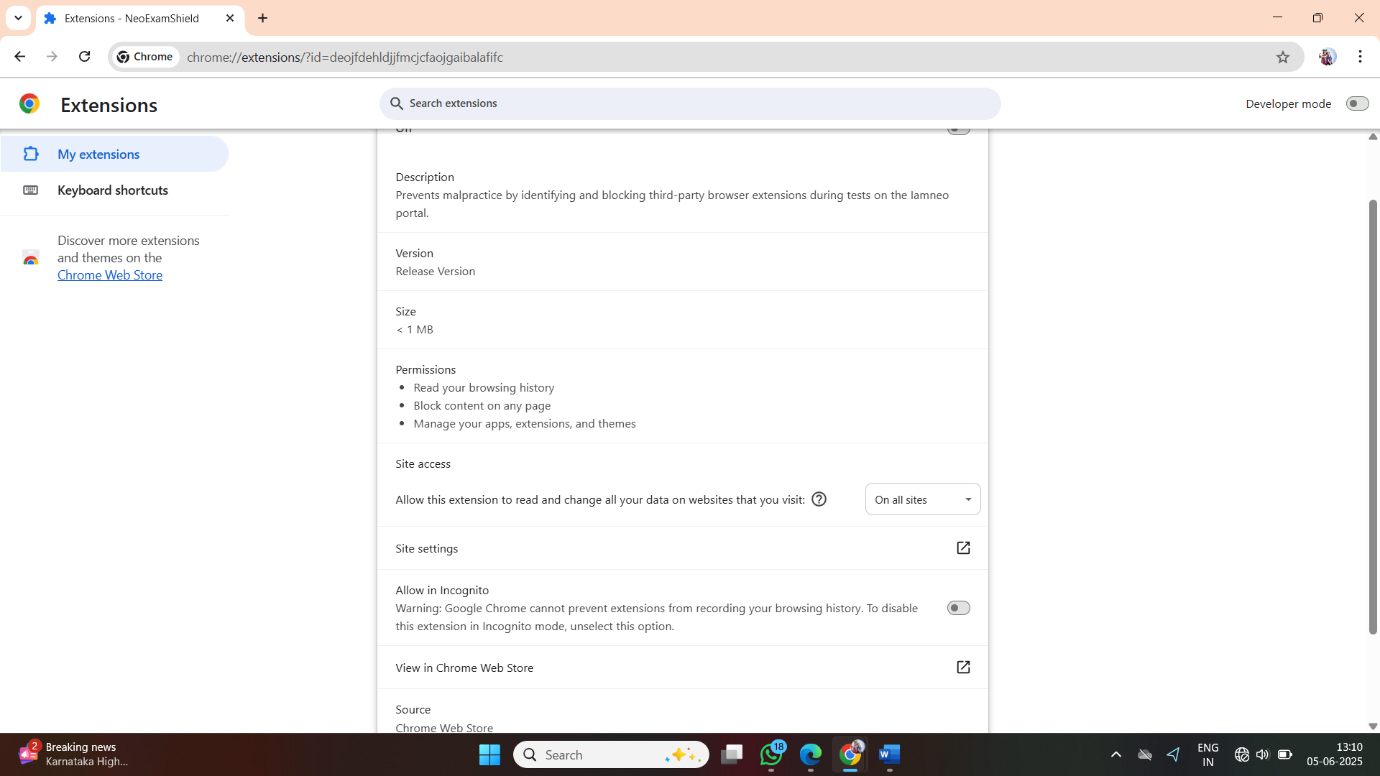
**Why:** You need to identify which extensions are installed, especially those you don’t recognize or use.

* Read each extension’s name and purpose.



**Step 3: Check Permissions and Reviews**

**Why:** Malicious extensions often ask for permissions they don’t need.

* Click on the **“Details”** or **“More”** link for each extension.
* Review:
  + **Permissions** (e.g., “Read your browsing history” or “Access to all sites”)
  + **Number of downloads**
  + **Ratings and user reviews**
* Look for suspicious behavior mentioned by others.
* 

**Step 4: Identify Any Unused or Suspicious Extensions**

**Why:** Extensions that are no longer needed or look suspicious may pose security or privacy risks.

🔎 Look for signs like:

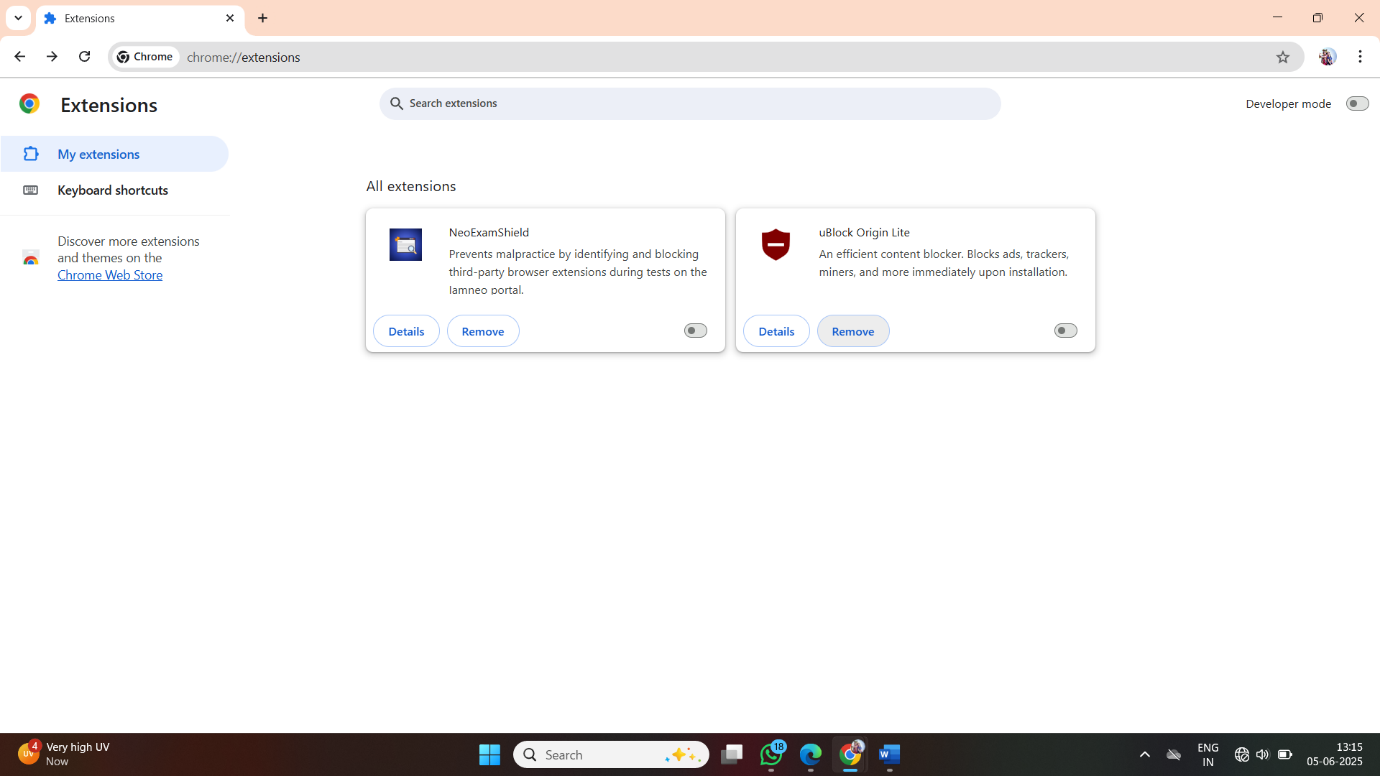
* Generic names like “PDF Helper” or “Video Downloader Pro”
* Typos or strange grammar in the description
* Recently added (without your knowledge)
* Unknown publisher or no official website

**Step 5: Remove Suspicious or Unnecessary Extensions**

**Why:** Unused or malicious extensions should be removed to prevent tracking, pop-ups, or even malware.

* Click the **“Remove”** button beside the extension.
* Confirm the removal when prompted.

🗑️ It's better to be cautious. You can always reinstall later if needed.



**Step 6: Restart Your Browser**

**Why:** Restarting ensures all changes are applied and helps clear any active processes the extension may have been using.

* Close all browser windows.
* Open the browser again.
* Check if performance improved (fewer pop-ups, faster load times, no weird redirections).

**Step 7: Research How Malicious Extensions Harm Users**

**Why:** Understanding the threat helps prevent future risks.

🔍 Common harms include:

* **Tracking** your activity and stealing login details
* **Injecting ads** or pop-ups into websites
* **Redirecting** search results or hijacking homepage
* **Installing malware** or acting as a backdoor for other attacks

**Conclusion: Identify and Remove Suspicious Browser Extensions**

Through this task, I gained a practical understanding of how browser extensions can affect system performance, privacy, and security. By carefully reviewing all installed extensions, analyzing their permissions, and researching their reputation, I was able to identify and remove potentially harmful or unnecessary extensions.

This process improved my awareness of how easily malicious extensions can be installed—often without clear user consent—and the kind of risks they pose, such as data theft, ad injection, and browser hijacking.

After removing suspicious extensions and restarting the browser, I observed better performance and fewer unwanted pop-ups. This exercise emphasized the importance of regularly auditing browser extensions and being cautious about what is installed.

Overall, the task helped me build better habits for maintaining a secure browsing environment and highlighted the critical role of user vigilance in browser security.