# Cyber Security Internship

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

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

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

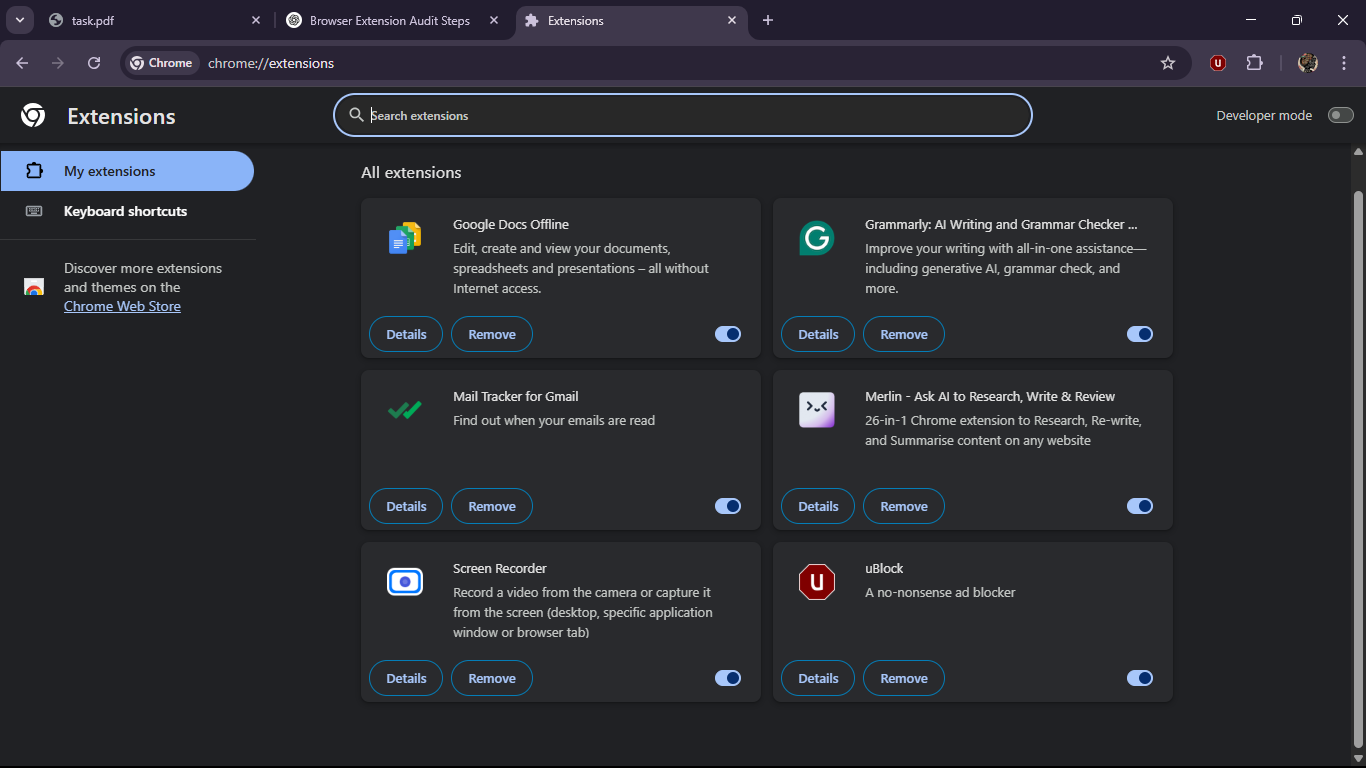
**Deliverables: List of suspicious extensions found and removed (if any)**

**1.Open your browser’s extension/add-ons manager.**

I mostly use Google Chrome so I am working on Chrome.

**Google Chrome**:

* Click the three dots in the top-right corner → **Extensions** → **Manage Extensions**
* Or directly type: chrome://extensions/ in the address bar.



These are the extensions I am using right now.

**2.Review all installed extensions carefully.**   
1. Google Docs Offline

Edit, create and view your documents, spreadsheets and presentations – all without Internet access.

* I don’t even remember adding this extension and I am not using it at all.

2. Grammarly: AI Writing and Grammar Checker App

Improve your writing with all-in-one assistance—including generative AI, grammar check, and more.

* I actually added this for grammar and spelling checks. It’s quite usefully.

3. Mail Tracker for Gmail

Find out when your emails are read

* I remember adding it but not even used once.

4. Merlin - Ask AI to Research, Write & Review

26-in-1 Chrome extension to Research, Re-write, and Summarise content on any website

* I use it for AI generated notes and for research papers.

5. Screen Recorder

Record a video from the camera or capture it from the screen (desktop, specific application window or browser tab)

* I used to use this for online class recording which are more important.

6. uBlock

A no-nonsense ad blocker

* It’s a good ad blocker but doesn’t work on all the websites.

**3.Check permissions and reviews for each extension.**

1. Google Docs Offline: It is added by default and used on only docs and drive of google.

2. Grammarly: It is allowed to all the sites and changes the data.

3. Mail Tracker for Gmail: Read your browsing history, Block content on any page, Display notifications, Know your email address.

4. Merlin : Read your browsing history, It is allowed to all the sites and changes the data.

5. Screen Recorder: Capture content of your screen, This extension has no additional site access.

6. uBlock: Read your browsing history, Block content on any page, It is allowed to all the sites and changes the data.

**4.Identify any unused or suspicious extensions.**

Merlin and uBlock are the extensions looks suspicious to me.

**5.Remove suspicious or unnecessary extensions.**

Yes, Removed the suspicious extensions (Merlin, uBlock).

**6.Restart browser and check for performance improvements.**

Completely closed and reopen your browser.

Observed:

* Faster browsing/loading times.
* Fewer pop-ups or redirects.
* More stable tab behavior.

**7.Research how malicious extensions can harm users.**

* Malicious extensions may:
  + Steal our browsing data or credentials.
  + Inject ads or change search results.
  + Record keystrokes (keylogging).
  + Redirect traffic or install more malware.
* Examples:
  + Extensions pretending to be useful tools (e.g., PDF converters) but injecting adware.
  + Fake Chrome extensions mimicking real brands (e.g., “ChatGPT Helper” but from an unknown source).

**8.Document steps taken and extensions removed**

Checked the added extensions, went through the details of each extension and identified which are good and which are suspicious and removed the extensions that I felt suspicious and harmful for my browser.

After removing I felt my browser works faster then before, tab behavior is stable.