Identify & Remove Suspicious Browser Extensions

Objective:

To identify potentially harmful or unused browser extensions, remove them, and enhance browser security and performance.

Tools Used:

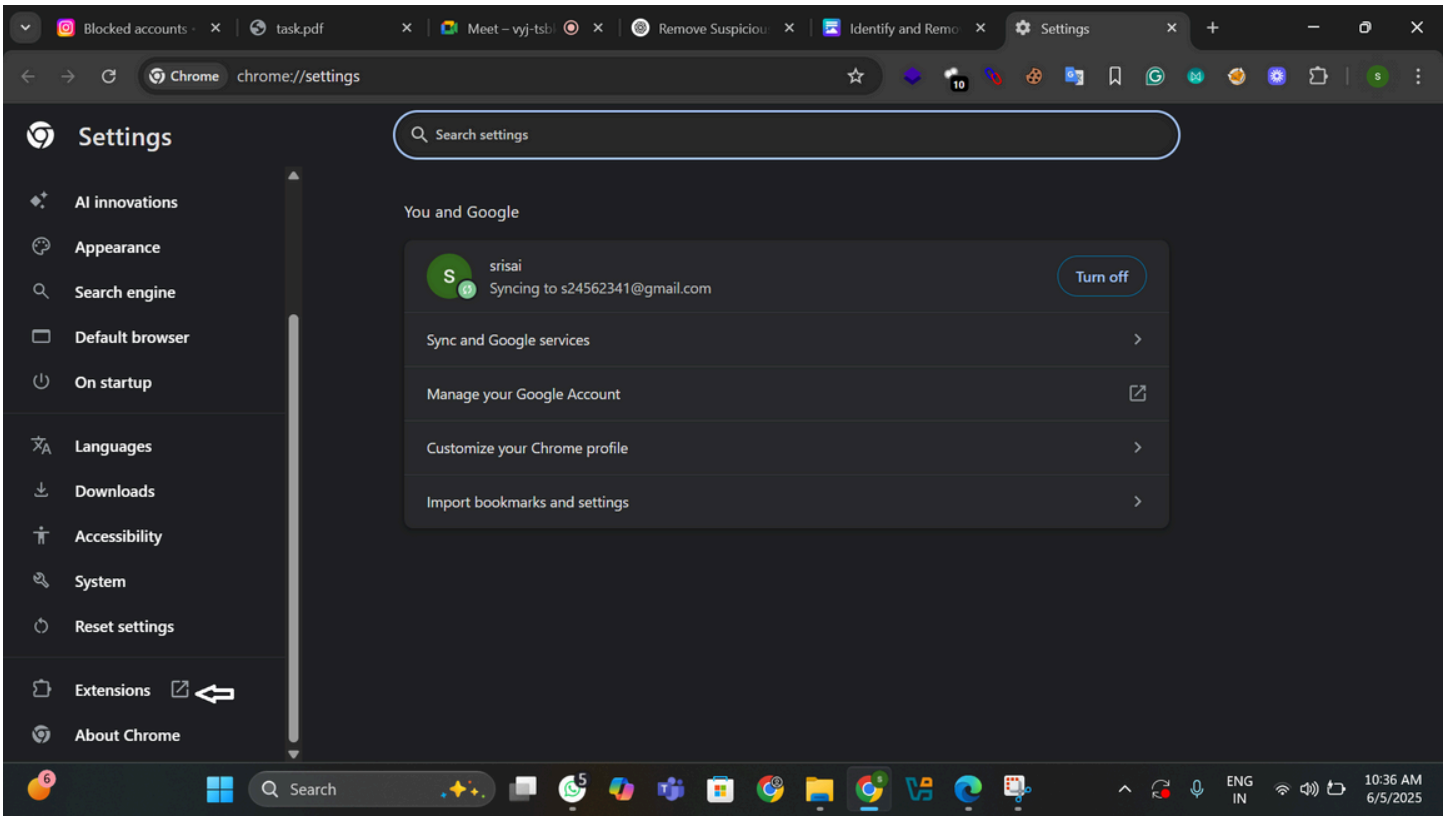
- **Browser:** Google Chrome (latest version)
- **Built-in Tool:** Chrome Extensions Manager (chrome://extensions)

Steps Taken:

Step 1: Open Extension Manager

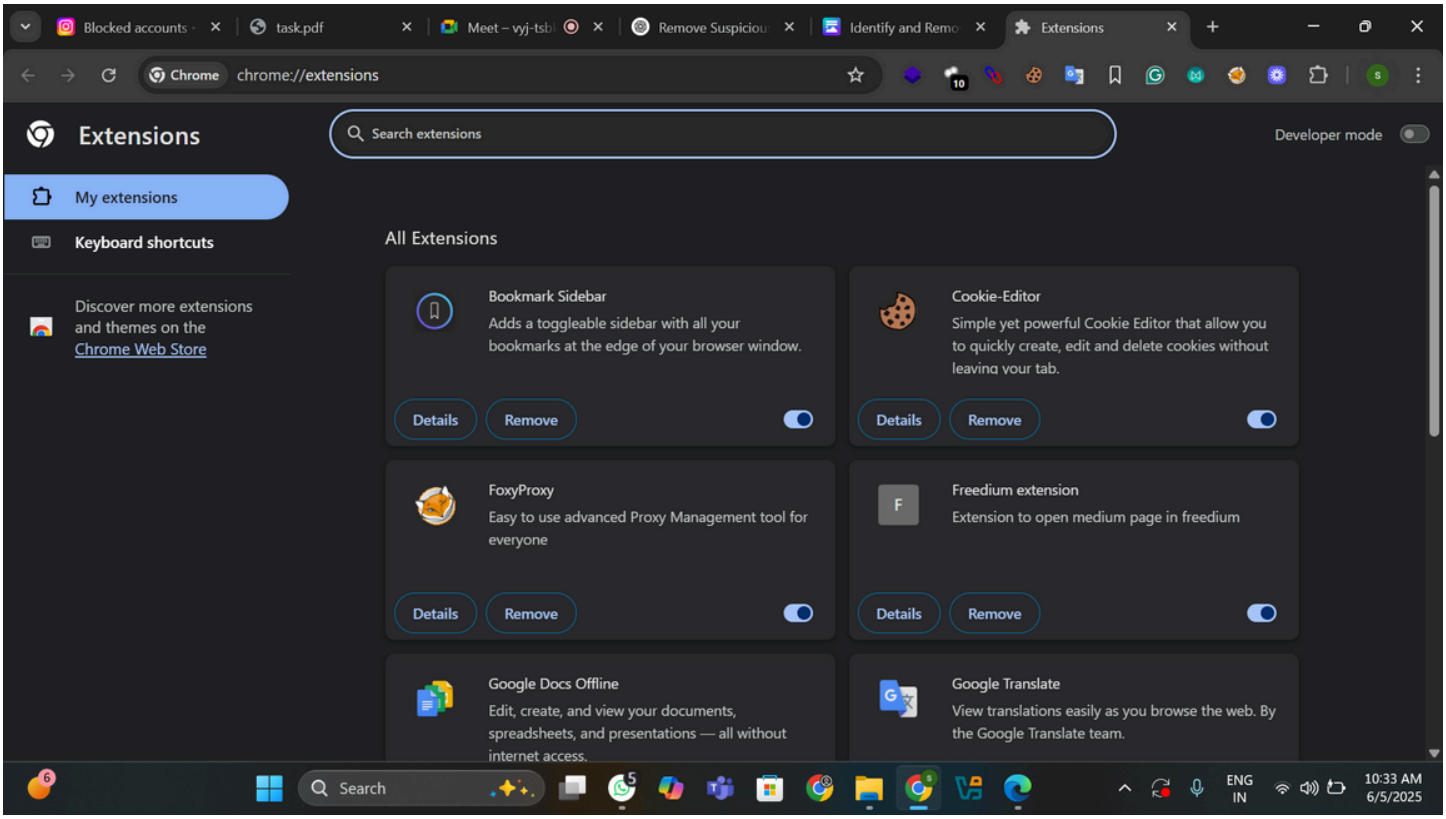
Chrome:
Go to chrome://extensions
Or click the 3 dots (⋮) → *Extensions* → *Manage Extensions*

Firefox:
Go to about:addons
Or click the 3 lines (≡) → *Add-ons and themes* → *Extensions*



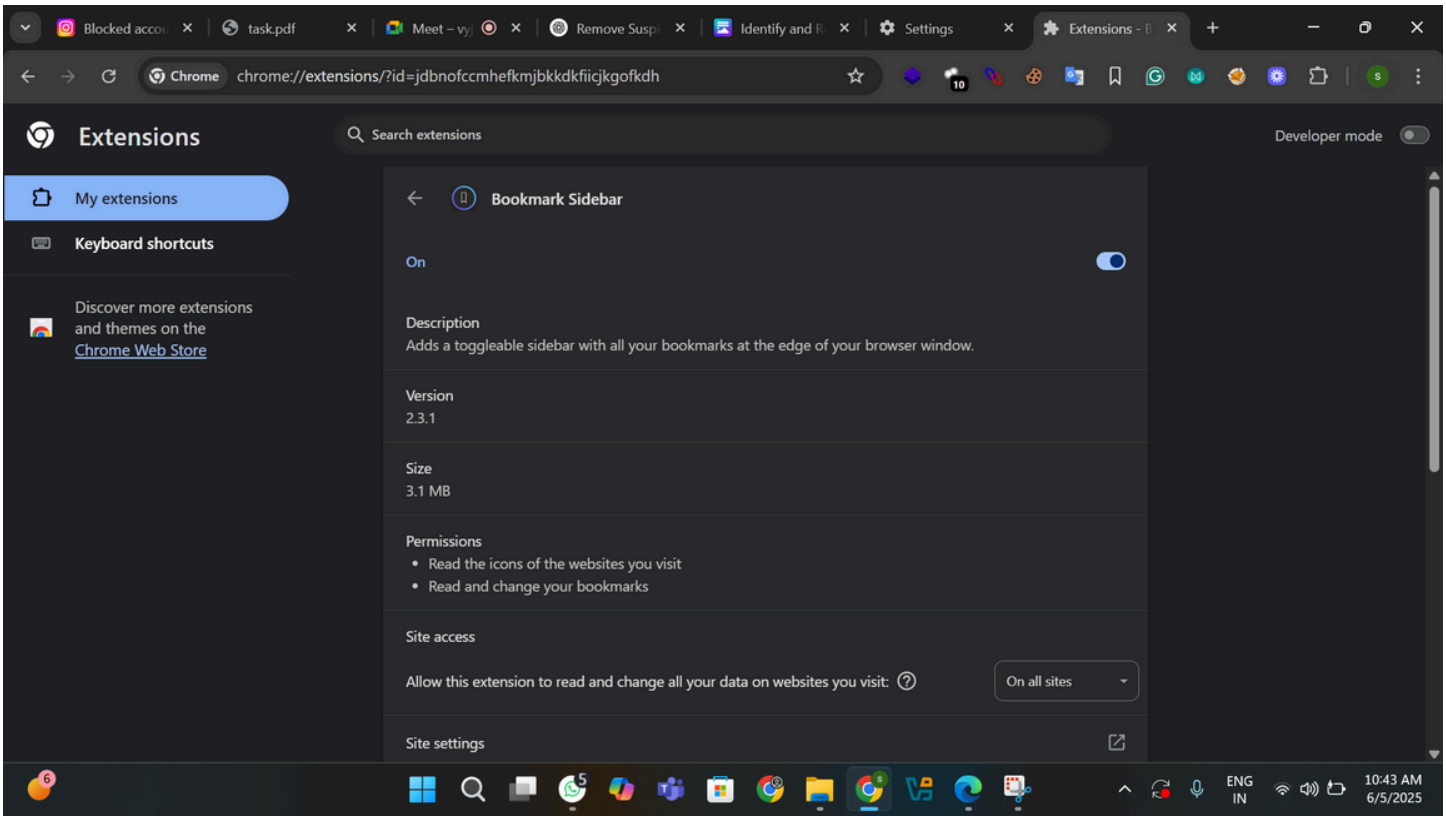
Step 2: Review All Installed Extensions

- Carefully look through the list.
- Ask yourself:
  - Do I use this extension regularly?
  - Do I remember installing it?
  - Does it look suspicious or unfamiliar?



Step 3: Check Permissions

- In Chrome, click **“Details”** on each extension → check:
  - “Can read and change all your data on the websites you visit” — 🚩 suspicious
  - “Access to file URLs” or clipboard — 🚩 check why it's needed
- In Firefox, click the **gear icon** near the extension → View permissions.



Step 4: Google the Extension Name

- Search for things like:
  - "[Extension name] malware"
  - "[Extension name] suspicious behavior"
- Check the Chrome Web Store or Mozilla reviews.

Step 5: Remove Suspicious/Unused Extensions

- In Chrome: Click **Remove** next to the extension
- In Firefox: Click the **three dots** next to the extension → **Remove**

Step 6: Restart the Browser

- Fully close and reopen the browser.
- Monitor for performance changes, pop-ups, or redirection issues.

Step 7: Research Risks of Malicious Extensions

Malicious extensions can:

- Steal login credentials or clipboard content
- Inject ads or redirect search queries
- Act as keyloggers or spyware
- Track your online behavior

Step 8: Document Findings

Example documentation:

Extension Name	Status	Reason for Removal
PDF Converter Pro	Removed	High permissions, bad reviews
Grammarly	Kept	Trusted, well-known, regularly used
Weather Wizard	Removed	Not in use, unknown source

OUTCOME:

- Gained awareness of **browser extension threats**
- Practiced safe extension management
- Improved browser performance and reduced attack surface

Conclusion:

This task highlighted the importance of regularly auditing browser extensions to maintain a secure and efficient browsing environment. By carefully reviewing installed extensions, analyzing their permissions, and removing those that were unnecessary or suspicious, I was able to reduce potential security risks and slightly improve browser performance. The activity reinforced that even small browser add-ons can pose significant threats if not properly managed. Going forward, I will adopt a more cautious approach to installing extensions and periodically review them to ensure continued browser safety.