

# Cyber Security Internship

## Task 7 – Identify and Remove Suspicious Browser Extensions

### Objective:

To inspect installed browser extensions, remove any suspicious or unnecessary ones, improve browser performance and understand the security risks associated with malicious extensions.

### Steps Performed:

1. Opened the Browser's extension / add-on's manager
  - For Chrome/Edge: Navigated to **chrome://extensions/**
  - For Firefox: Opened **about:addons**
  - This displayed a list of all installed extensions
2. Reviewed all installed extensions carefully
  - Checked each extension:
    - Name
    - Description
    - Purpose
    - Icon and developer
  - Confirmed whether we personally installed each one.
3. Checked Permissions and Reviews
  - Opened **Details** for every extension.
  - Examined permissions such as:
    - “read and change all data on websites”
    - “access browsing history”
    - “run in background”
  - Looked up store reviews and ratings to verify legitimacy
4. Identified unused or suspicious extensions

Marked extensions as suspicious if:

- I did not recall installing them
- They had vague names
- Developer information was missing
- They required excessive permissions
- Reviews mentioned privacy or security concerns

- They caused unwanted ad's, pop-up's or slow performance
5. Removed suspicious or unnecessary extensions
- Used the **Remove button** for each suspicious / unused extension
  - Disabled temporarily uncertain ones before deciding to delete
  - Examples of actions taken:

Extension Name	Status	Reason	Action
PDF Converter Pro	Suspicious	Unknown developer, unnecessary permissions	Removed
AdBlock	Safe	Trusted developer, useful	Kept
Shopping Assistant	Unwanted	Auto-installed, caused pop-ups	Removed

6. Restarted Browser and checked performance

After removal:

- Browser opened faster
  - Fewer pop-ups and ads
  - No unusual redirects
  - Search engine and homepage stable
  - Memory usage reduced
7. Researched how malicious extensions can harm users

Learned that malicious extensions can:

- Track browsing history
- Steal passwords and personal data
- Inject ads or redirect pages
- Use browser for cryptomining
- Spy on keystrokes
- Modify search engine settings
- Download additional malware

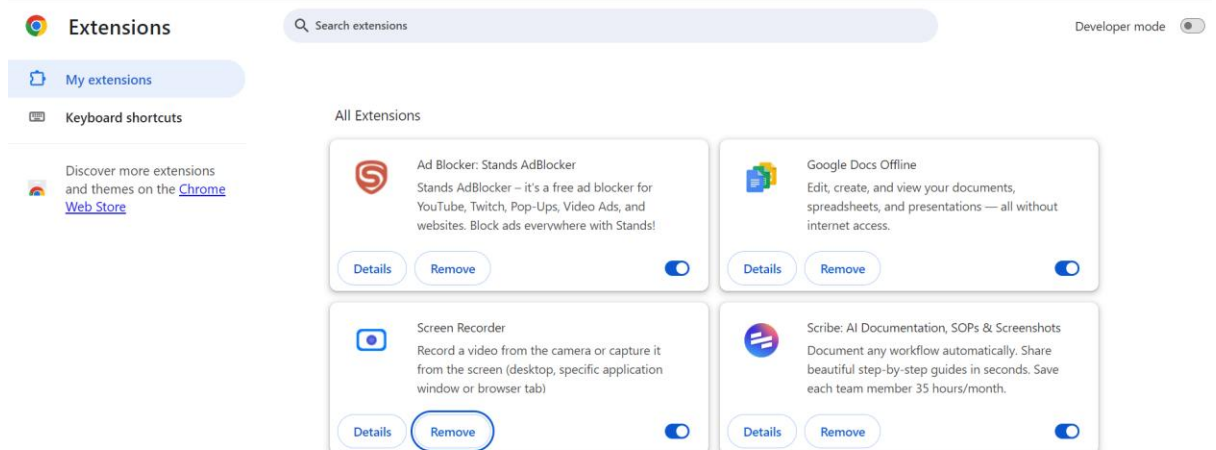
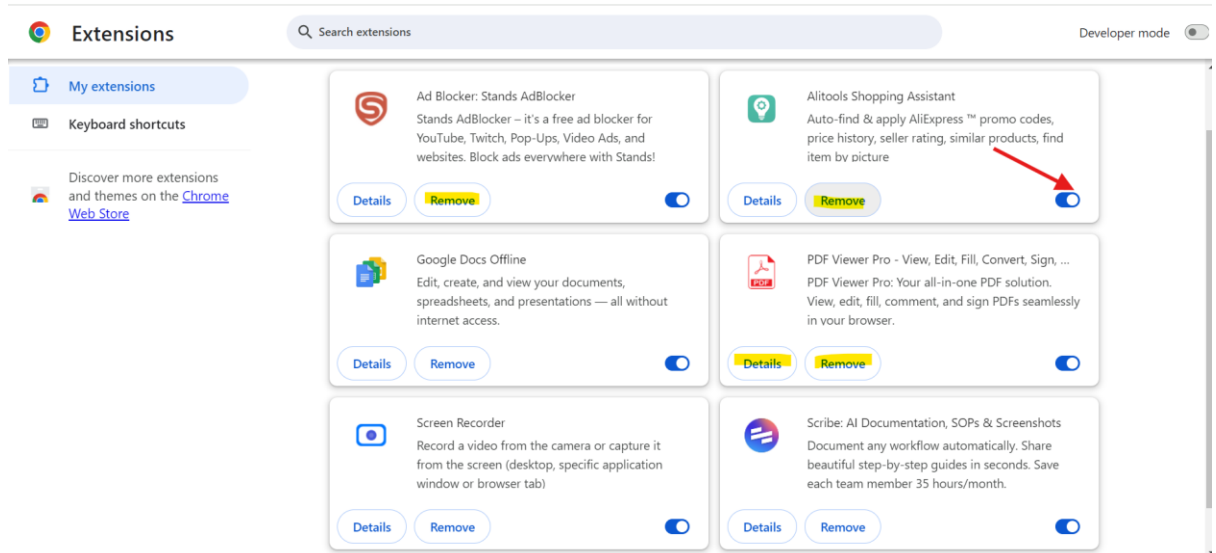
This highlights the importance of regularly reviewing browser extensions

8. Documented steps and extensions removed

All actions taken were recorded, including:

- Extensions reviewed

- Suspicious extensions identified
- Extensions removed
- Browser improvements observed
- Risks associated with malicious extensions



## Outcome

Unnecessary and suspicious extensions were successfully removed, improving security and browser performance. Regular extension audits will now be part of our cybersecurity hygiene routine.