7th Task SUBMISSION REPORT OF ELEVATE LABS CYBERSECURITY INTERNSHIP

NAME	**Jadav Dinesh**
Submitted to:	**Elevate Labs**
Name of the Academic Institute	**Ganpat University**

REPORT SUBMITTED TO

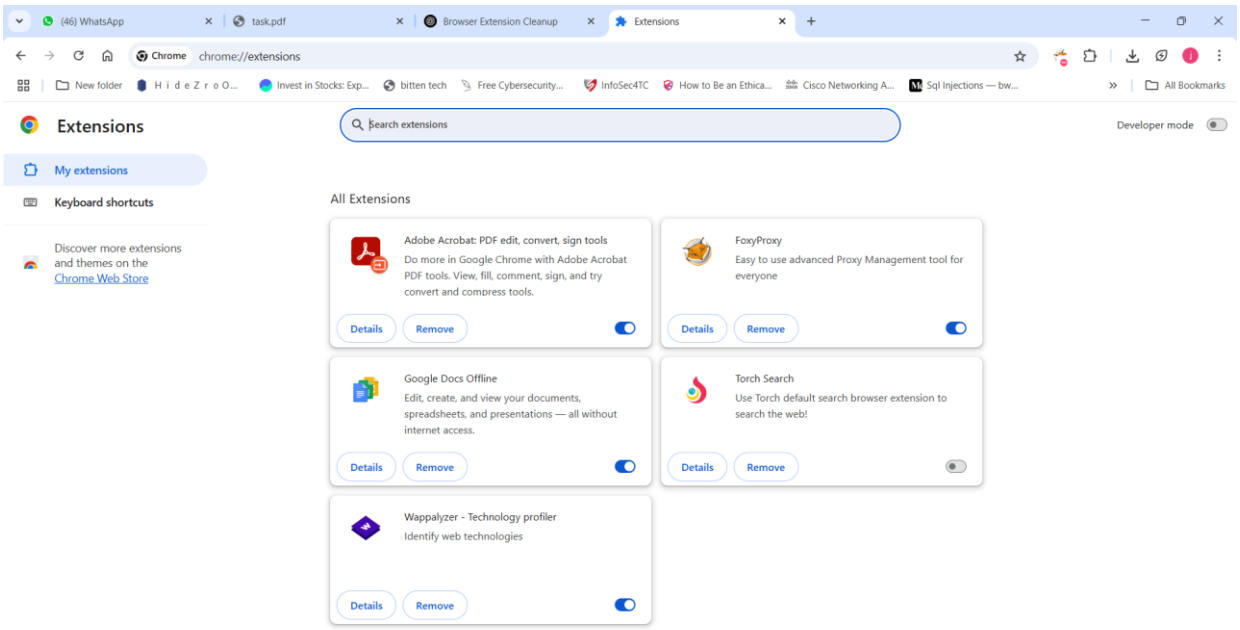
As part of the Cyber Security Internship, I have completed "Task 7th: Identify and Remove Suspicious Browser Extensions." by following all steps as instructed. Below is a detailed summary of each step followed during the task:

Task 7th: Identify and Remove Suspicious Browser Extensions

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

- **Chrome: Type chrome://extensions/ in the address bar and press Enter.**
- **Firefox: Type about:addons and press Enter.**
- **Edge: Type edge://extensions/ and press Enter.**

I can use Chrome browser's



---

2. Review all installed extensions carefully.

Step-by-Step: How to Review Installed Extensions

For each extension, check:

1. Do you recognize it?

- **Ask: *Did I install this myself?***
- **If not sure — Google it.**

2. Do you use it regularly?

- **Ask: *When was the last time I actually used this?***
- **If you haven't used it in weeks, it might be unnecessary.**

3. Who is the developer?

- **Click Details → Look for the developer name.**
- **Unknown or suspicious developer? ⚠️ Red flag.**

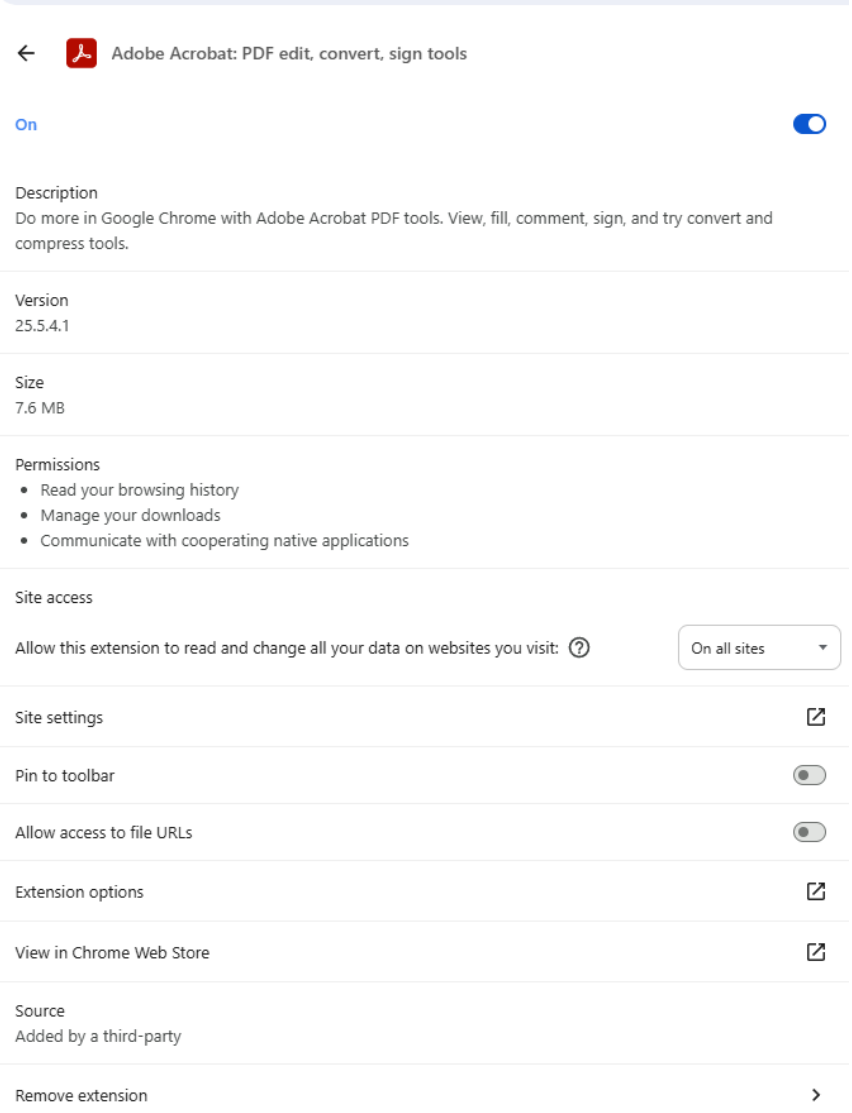
4. What permissions does it have?

- **In Details (Chrome/Edge) or the gear icon (Firefox), check:**
  - **Can it read/change all your data on websites?**
  - **Access files/downloads/clipboard?**
- **Too many permissions for a simple tool? Be cautious.**

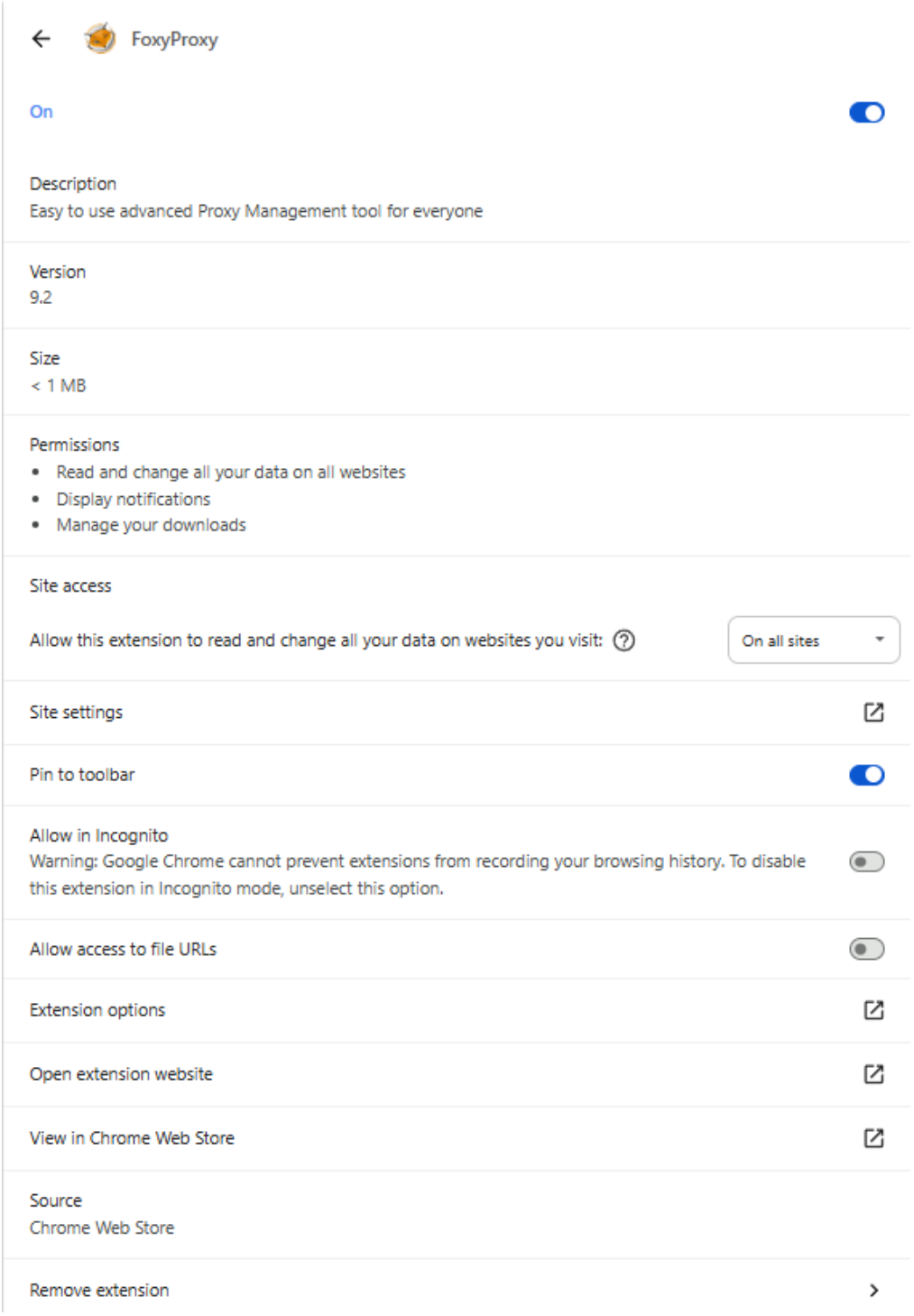
5. Any strange behavior recently?

- **Ads showing up?**
- **Tabs opening on their own?**
- **Pop-ups?**

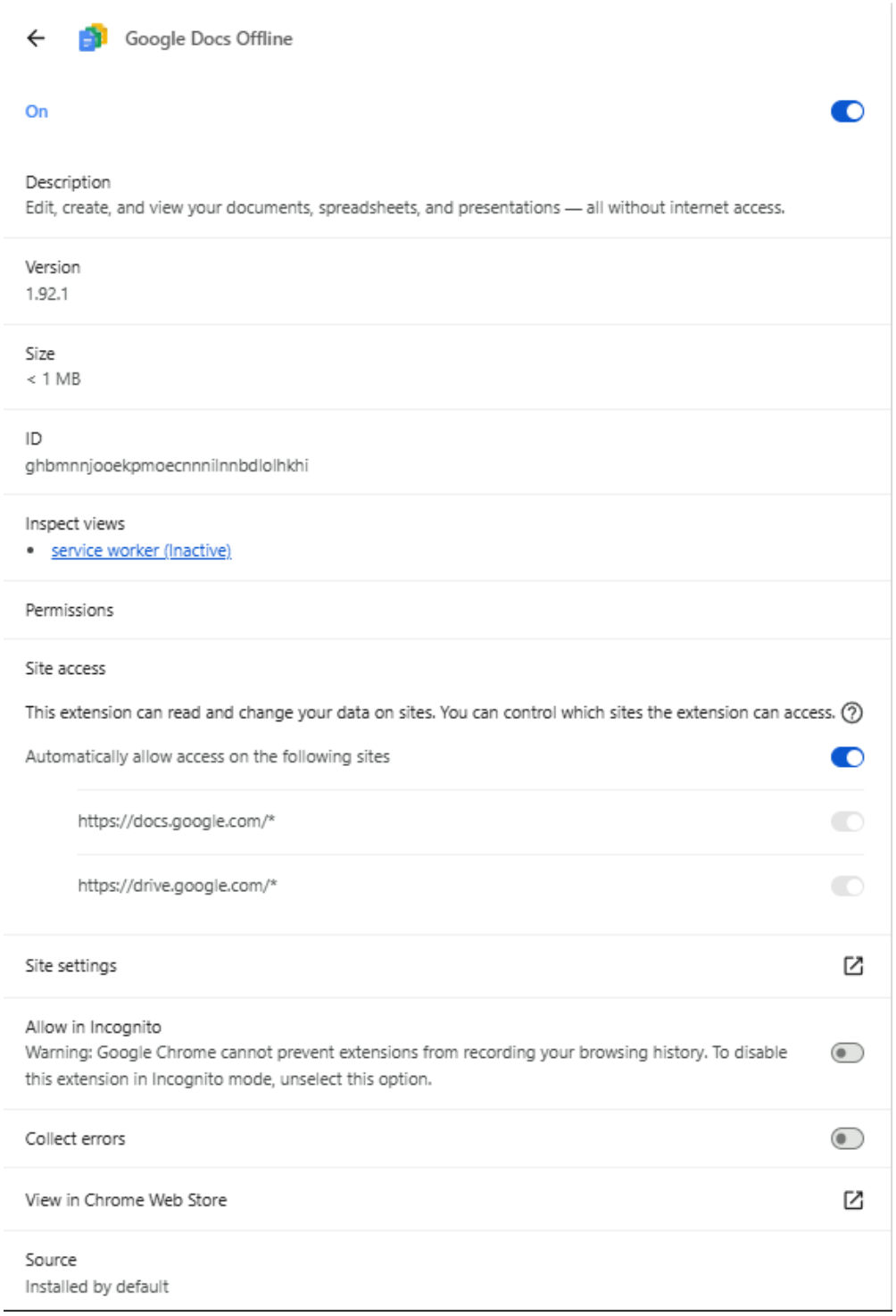
These could be signs of a malicious extension.



Task 7th: Identify and Remove Suspicious Browser Extensions



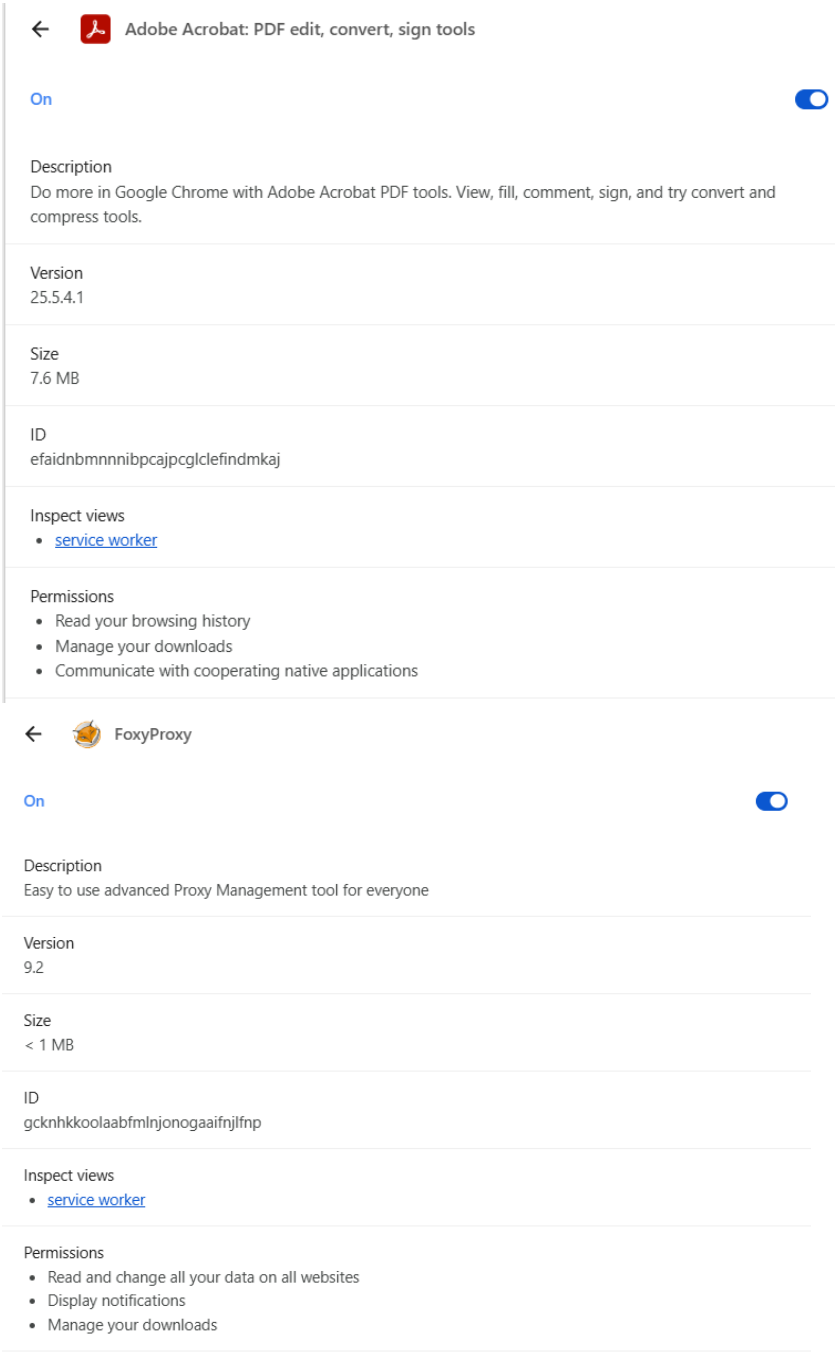
Task 7th: Identify and Remove Suspicious Browser Extensions



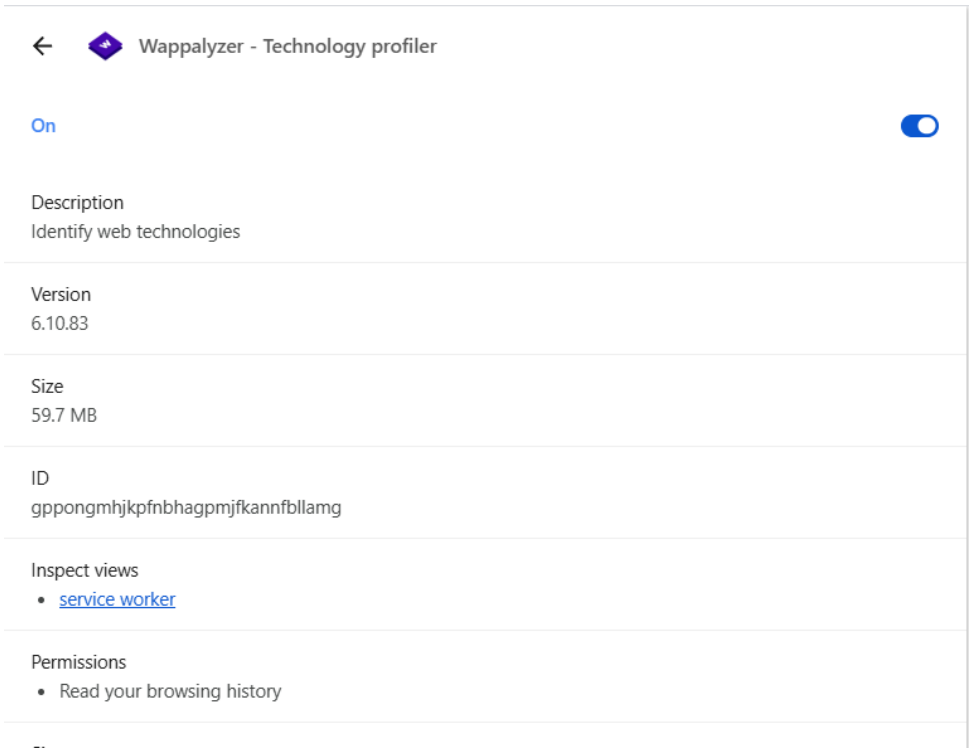
3. Check permissions and reviews for each extension.

In Chrome:

1. **Go to your extensions page:**
   chrome://extensions/ or edge://extensions/
2. **Click "Details" under each extension.**
3. **Look at:**
   - **Site access (e.g., "Can read and change all your data on all websites")**
   - **Other permissions: access to downloads, clipboard, file system, etc.**



Task 7th: Identify and Remove Suspicious Browser Extensions



4. Identify any unused or suspicious extensions.

1. Do I Use This Extension Regularly?

- **If you haven't used it in the last 2–4 weeks, it's probably unused.**
- **Example: Random PDF converter or coupon toolbar you forgot about.**

2. Do I Trust the Source/Developer?

- **Go to the Chrome Web Store or Firefox Add-ons site.**
- **Who is the developer?**
    - **Trusted: Google, Mozilla, Bitwarden, LastPass, uBlock Origin, etc.**
    - **Suspicious: Generic names like "Productivity Inc." or no developer listed.**

Action: If you don't trust the developer, remove it.

3. Does It Ask for Too Many Permissions?

- **Example: A simple tool like a notepad extension asking to "read all your data on websites" is not okay.**

4. Any Browser Weirdness Recently?

- **Are you seeing:**
    - **Unexpected popups?**
    - **New tabs opening?**
    - **Fake-looking search results?**
    - **Weird ads showing up?**

- **These might be signs of a malicious extension.**
  Action: Remove extensions causing these symptoms — even if they seem useful.

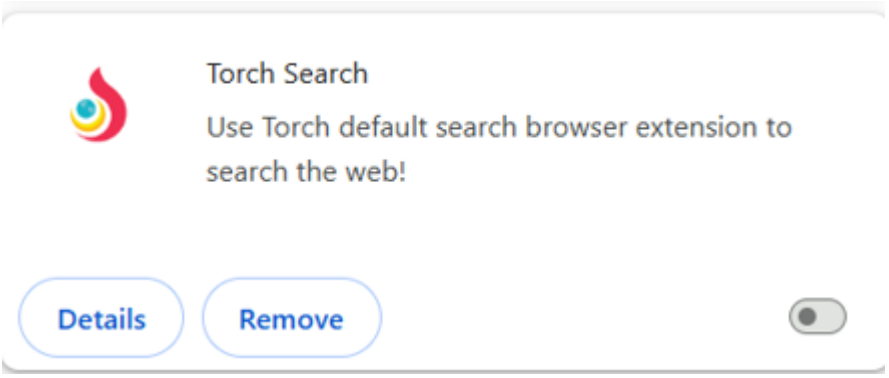
5. Check Reviews One Last Time

- **Any user reports of spying, injecting ads, fake versions?**
- **If yes, remove it.**

5. Remove suspicious or unnecessary extensions.

Google Chrome / Microsoft Edge

1. **Go to:**
   chrome://extensions/ (for Chrome)
   edge://extensions/ (for Edge)
2. **For each suspicious/unneeded extension:**
   - **Click "Remove".**
   - **Confirm by clicking "Remove" again in the pop-up**



6. Restart browser and check for performance improvements.

Restart Your Browser

Here's how:

1. **Close all browser windows and tabs completely.**
2. **Wait a few seconds.**
3. **Reopen the browser.**

Check for Performance Improvements

After restarting, pay attention to the following:

- **Speed**

- **Does the browser launch faster?**
- **Are websites loading more quickly?**

- **Smoothness**

- **Fewer delays or stuttering when switching tabs?**
- **Less RAM usage (check Task Manager or Activity Monitor)?**

- Pop-ups or Ads

- Are unexpected ads or fake search engines gone?
- CPU/RAM usage (optional)

- Open Task Manager (Windows: Ctrl+Shift+Esc, Mac: Cmd+Space → "Activity Monitor")
- Look for your browser's memory and CPU usage.
- Is it lower than before?

7. Research how malicious extensions can harm users.

1.Stealing Personal Data

- What they do: Log your keystrokes, steal saved passwords, read cookies, grab clipboard content.
- Why it's dangerous: They can access your logins, emails, banking info — even if you're on HTTPS sites.
- *Example*: The "DataSpii" incident exposed sensitive user data via Chrome extensions.

2. Tracking Your Online Activity

- What they do: Monitor every website you visit, what you search, and even your clicks.
- Why it's bad: This data can be sold to third parties or used to profile you.
- *Example*: Extensions like "Hover Zoom" were caught spying on users' browsing history.

3. Injecting Ads or Malware

- What they do: Modify websites you visit to insert ads or links that redirect to scam sites.
- Why it's bad: It slows your browser, invades your privacy, or installs more malware.
- *Example*: "ShoppersTab" secretly injected affiliate links and redirected users to fake sites.

4. Hijacking Search Engines & Homepages

- What they do: Change your default search engine or homepage to ad-filled or malicious versions.
- Why it's harmful: You lose control of your browsing, and it often leads to scam results.
- *Example*: Fake Chrome extensions that pretend to be search helpers but redirect all searches.

5. Spreading to Other Devices

- What they do: Some malicious extensions use browser sync (Google/Microsoft accounts) to install themselves across all your devices.
- Why it's serious: You might clean one device and get re-infected from another.

6. Bypassing Web Security

- **What they do: Some extensions disable security headers or inject scripts into secure (HTTPS) sites.**
- **Why it's dangerous: Makes it easier for attackers to run phishing or man-in-the-middle attacks.**

8. Document steps taken and extensions removed.

Browser Extension Cleanup Log

Date: June 5, 2025
Browser: (e.g., Google Chrome / Mozilla Firefox / Microsoft Edge)
Device: (e.g., Windows 11 laptop, MacBook Pro, etc.)

Steps Taken:

1. **Opened extension manager:**
   chrome://extensions/ or about:addons
2. **Reviewed all installed extensions:**
   - **Checked names, developers, and purpose.**
   - **Verified if they were recognized and still in use.**
3. **Checked permissions:**
   - **Examined each extension's access level (site data, tabs, clipboard, etc.).**
   - **Flagged any extensions with excessive or suspicious permissions.**
4. **Reviewed extension reputation:**
   - **Looked up extensions on the Chrome Web Store or Firefox Add-ons.**
   - **Read user reviews and searched for security reports.**
5. **Identified and removed suspicious or unused extensions:**
   - **Unused: Not used in the past 30+ days**
   - **Suspicious: Unknown developers, bad reviews, excessive access**
6. **Restarted browser:**
   - **Fully closed and reopened the browser to apply changes.**
7. **Monitored performance:**
   - **Browser launch speed improved**
   - **Reduced tab lag**
   - **Fewer unwanted ads/pop-ups**
8. **Researched risks of malicious extensions:**
   - **Learned how extensions can track, inject ads, steal data, or hijack pages.**
   - **Reviewed real-world examples of compromised extensions.**

Task 7th: Identify and Remove Suspicious Browser Extensions

Extensions Removed:

Extension Name	Reason for Removal
WeatherTab Pro	Unused, unknown developer
PDF Easy Converter	Excessive permissions, unneeded
MyFunNewTab	Suspicious behavior, ad injection
Quick Search Boost	Changed search engine settings

Extensions Kept (Trusted & In Use):

Extension Name	Reason for Keeping
uBlock Origin	Trusted ad-blocker
LastPass	Password manager in use
Grammarly	Writing assistant, useful