ELEVATE LABS Harshitha M

TASK 7 Report:

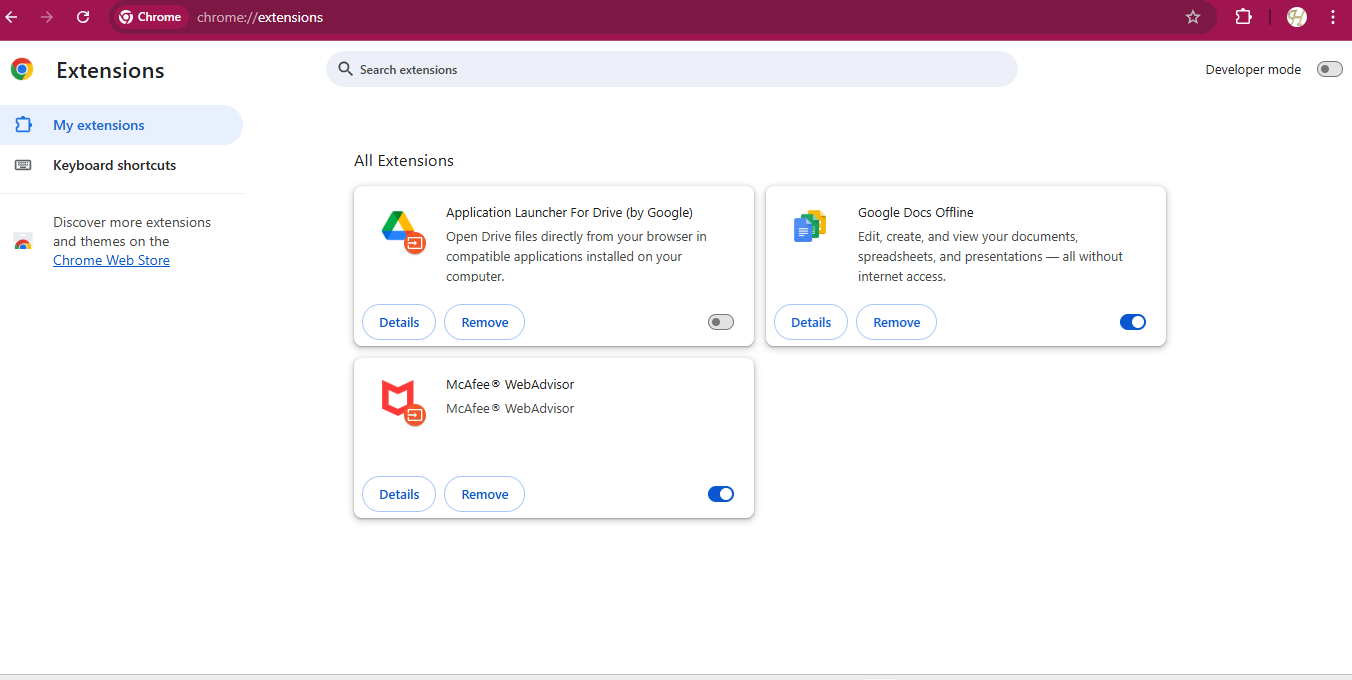
Identify and Remove Suspicious Browser Extensions

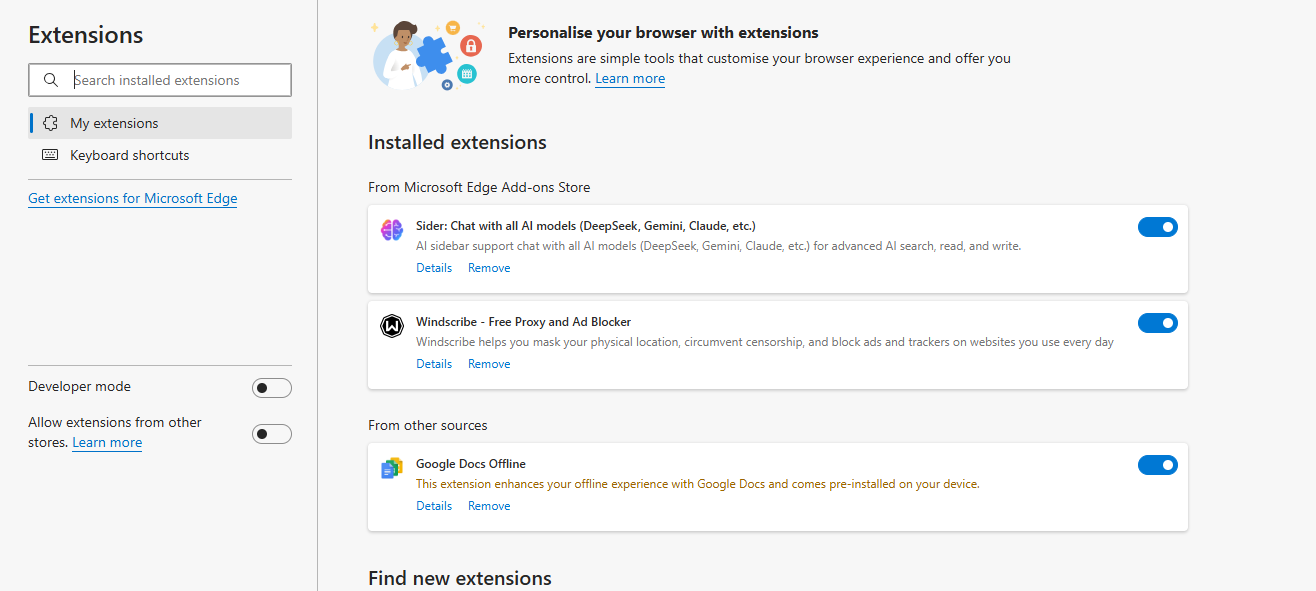
Step 1

Select a browser of your choice and check for extensions

Step 2

Check if any suspicious extensions available

Snippet of Chrome extensions



Snippet of Microsoft Edge extensions

**Findings:**

Not much extensions available in my browsers

**Awareness of Browser Security Risks**

**1. Malicious Extensions**

* Some extensions can steal data, track your activity, or inject ads.
* Attackers may disguise malware as useful tools.

**2. Phishing and Malicious Websites**

* Fake websites may look real and steal your login credentials.
* Unsafe links can install malware without your knowledge.

**3. Insecure HTTPS Connections**

* Browsing on sites without HTTPS exposes your data to interception (especially on public Wi-Fi).

**4. Cookies and Tracking**

* Third-party cookies track your behavior across sites.
* Advertisers and trackers build profiles using your data.

**5. Browser Exploits**

* Outdated browsers can be vulnerable to zero-day exploits.
* Attackers can run malicious scripts (cross-site scripting/XSS).

**Managing Browser Extensions (Safely)**

**Best Practices**

1. **Install Only from Official Stores**
   * Use Chrome Web Store, Firefox Add-ons, or trusted sources.
   * Avoid downloading extensions from third-party websites.
2. **Review Permissions**
   * Check what data the extension can access (e.g., read browsing history, access tabs).
   * If it asks for more than it needs—avoid it.
3. **Regularly Review and Remove**
   * Go to your extensions page (chrome://extensions/, about:addons) and remove unused or suspicious ones.
4. **Keep Extensions and Browser Updated**
   * Updates patch security vulnerabilities.
5. **Read Reviews and Developer Info**
   * Look for red flags in user reviews or suspicious developer names.
6. **Use Minimal Extensions**
   * Fewer extensions mean fewer risks. Stick to essentials only.

**Tools to Help**

* **Browser Security Extensions:** (ironically) some extensions help:
  + *uBlock Origin* (ad and script blocker)
  + *HTTPS Everywhere* (forces HTTPS)
  + *Click&Clean*, *Privacy Badger*
* **Built-in Browser Features:**
  + Chrome’s "Safety Check" and Firefox’s "Enhanced Tracking Protection" help you stay secure.