8/14/2025

Identify and Remove Suspicious Browser

@SRCybersecurity

Task 7: Identify and Remove Suspicious Browser Extensions

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

Tools: Any web browser (Chrome, Firefox, Microsoft Edge)

Deliverables: Documented PDF file listing the extensions found and removed if any suspicious.

Identify and Remove Suspicious Browser Extensions step-by-step. Google Chrome , Mozilla Firefox, Microsoft Edge.

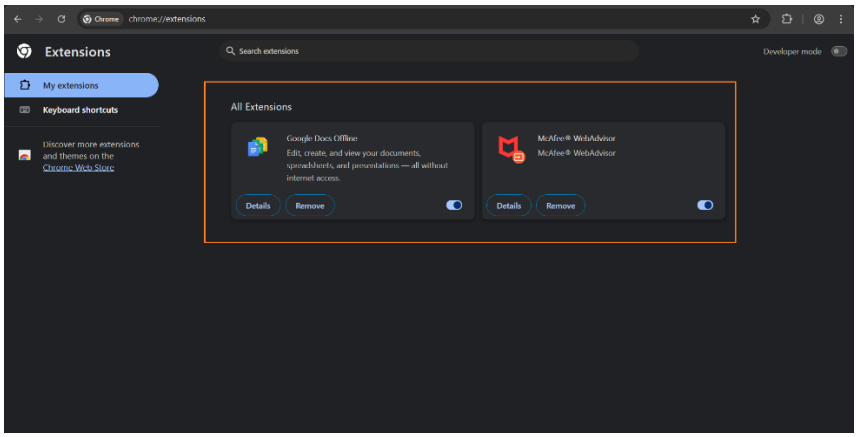
1. Open your browser's extension/add-ons manager

- **Chrome:**
  - Click the **three dots** in the upper-right corner.
  - Go to **Extensions** via: More Tools > Extensions
  - Or type **chrome://extensions** in the address bar and hit Enter.
- **Firefox:**
  - Click the **three horizontal lines** in the upper-right corner.
  - Choose **Add-ons and themes** > Extensions
  - Or type **about:addons** in the address bar and hit Enter.
- **Microsoft Edge:**
  - Click the **three-dot menu (⋯)** in the top-right corner.
  - Select **Extensions** from the dropdown.
  - In the Extensions panel, click **"Open Microsoft Edge Add-ons website"** at the bottom.
  - Or you can go directly to: **https://microsoftedge.microsoft.com/addons**

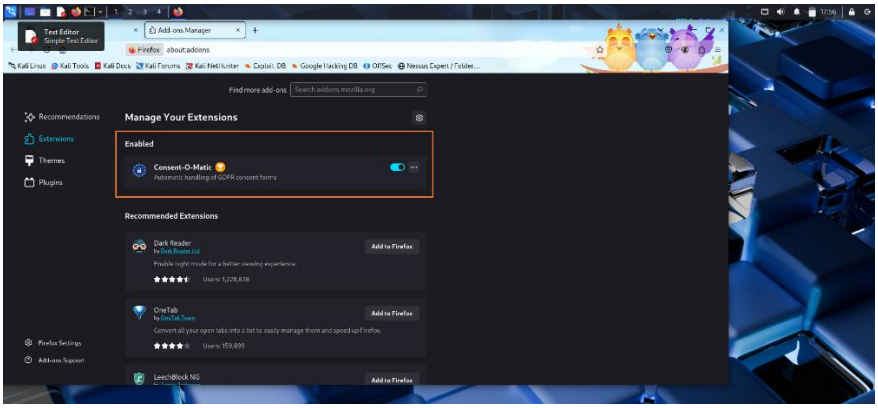
2. Review all installed extensions carefully

List of each installed extension:

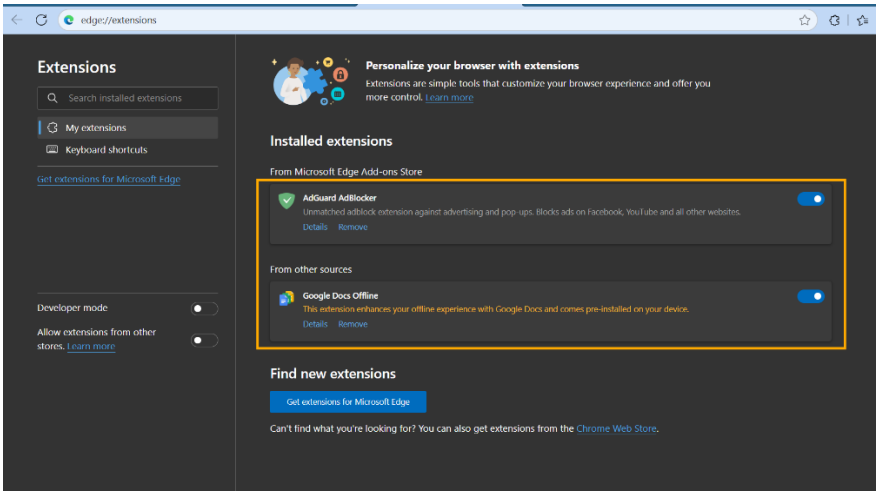
- **Google Chrome**



- **Mozilla FireFox**

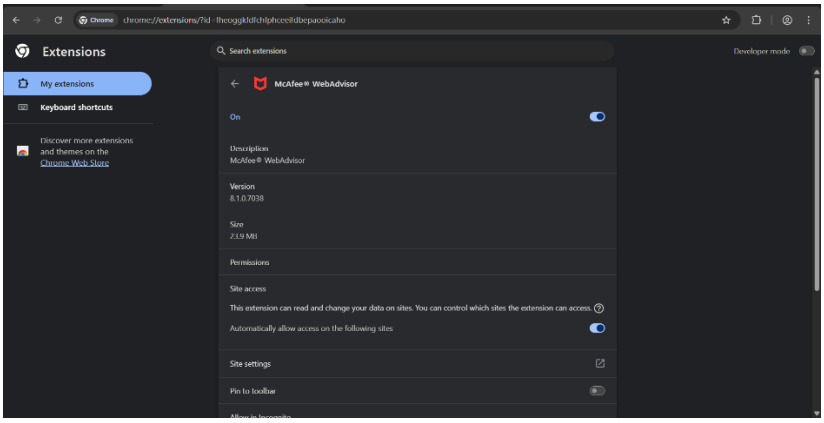


- **Microsoft Edge**

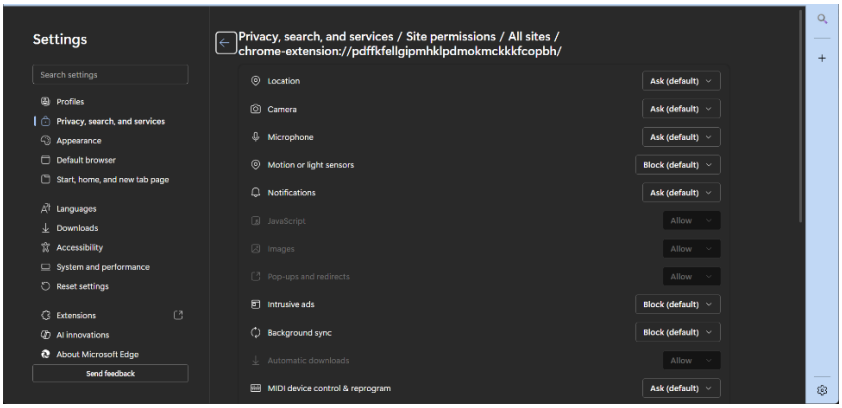


3. Check permissions and reviews for each extension

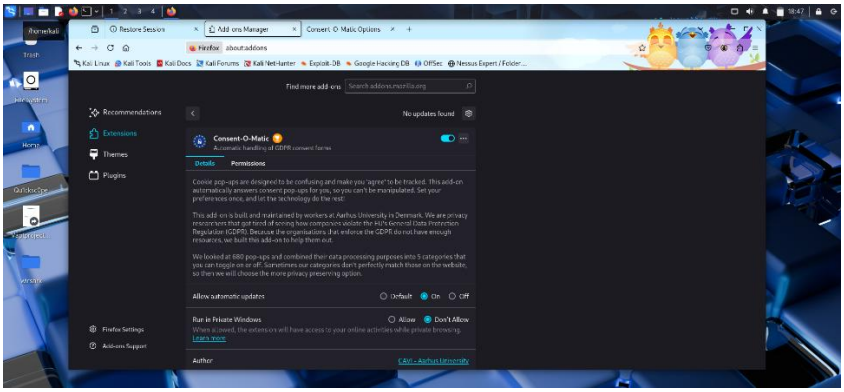
- In **Chrome**, click “Details” on each extension to see:
    - What permissions it has (e.g. "Read and change all your data on websites").
    - Links to the **Chrome Web Store** – check user **ratings and reviews**.



- In **Firefox**, click the gear icon next to the extension > **Manage** to view:
    - Permissions and user reviews.



- **Microsoft Edge Add-ons website:** https://microsoftedge.microsoft.com/addons
    - Search for the extension you're interested in.
    - Click on the **extension** to open its details page.
    - **Scroll down** to the section labelled as **“Permissions”** (you'll usually find it just below the description).
    - It will list what data the extension can access, such as:
        - "Read and change all your data on the websites you visit"
        - "Read your browsing history"
        - "Access your tabs"
        - Pay attention here, especially for extensions that request broad or sensitive access.
    - On the **extension's details page**, scroll to the **“Ratings and reviews”** section



4. Identify any unused or suspicious extensions

Look for red flags like:

- Unknown developer
- Poor reviews or low ratings
- Unnecessary access (e.g. access to all websites, clipboard, etc.)
- You don't remember installing it
- It’s not from a trusted source

5. Remove suspicious or unnecessary extensions

- Click **Remove** or **Trash icon** next to the extension.

7. Research how malicious extensions can harm users

Malicious extensions can:

- Track browsing activity
- Steal personal data or login info
- Inject ads or redirect traffic
- Hijack browser settings / History / Cookies (homepage, search engine).
- Install malware

Good sources to read:

- Google Security Blog
- Mozilla Security Blog

Browser Used: Microsoft Edge/ Chrome / Firefox.

Extensions Found:

Browser	Extension Name	Used?	Trusted?	Action Taken
Microsoft Edge	AdGuard AdBlocker AdBlock	Yes	Yes	Kept
Microsoft Edge	Google Docs Offline	Yes	Yes	Kept
Chrome	McAffe WebAdvisor	Yes	Yes	Kept
Chrome	Google Docs Offline	Yes	Yes	Kept
FireFox	Consent-O-Matic	Yes	Yes	Kept

Permissions Reviewed:

- Checked for access to data, websites, or personal information.
- Browser opens faster
- No suspicious extensions found
- Tabs load smoothly

From what I Learned:

- Not all browser extensions are safe.
- Some can collect private data or slow down the browser.
- It’s important to review/update extensions regularly.

THANK YOU

END