**Task 7: Identify and Remove Suspicious Browser Extensions**

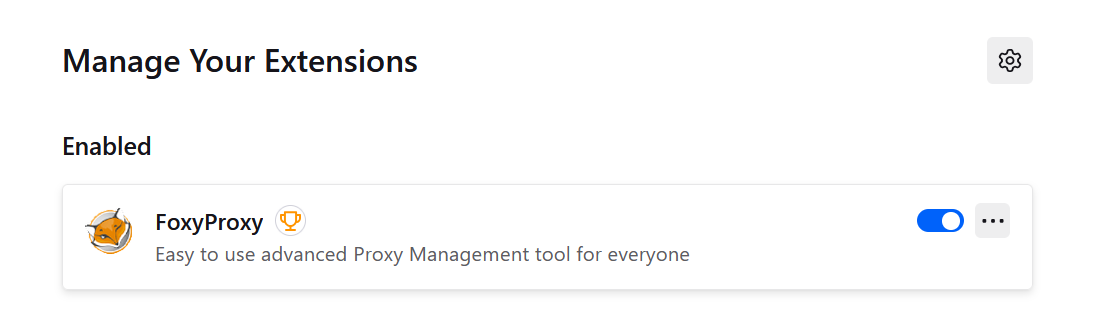
**Objective**:

Review your browser extensions, remove anything unfamiliar or untrusted, check permissions and reviews, and restart the browser to ensure smooth and safe performance.

**Tools used:**

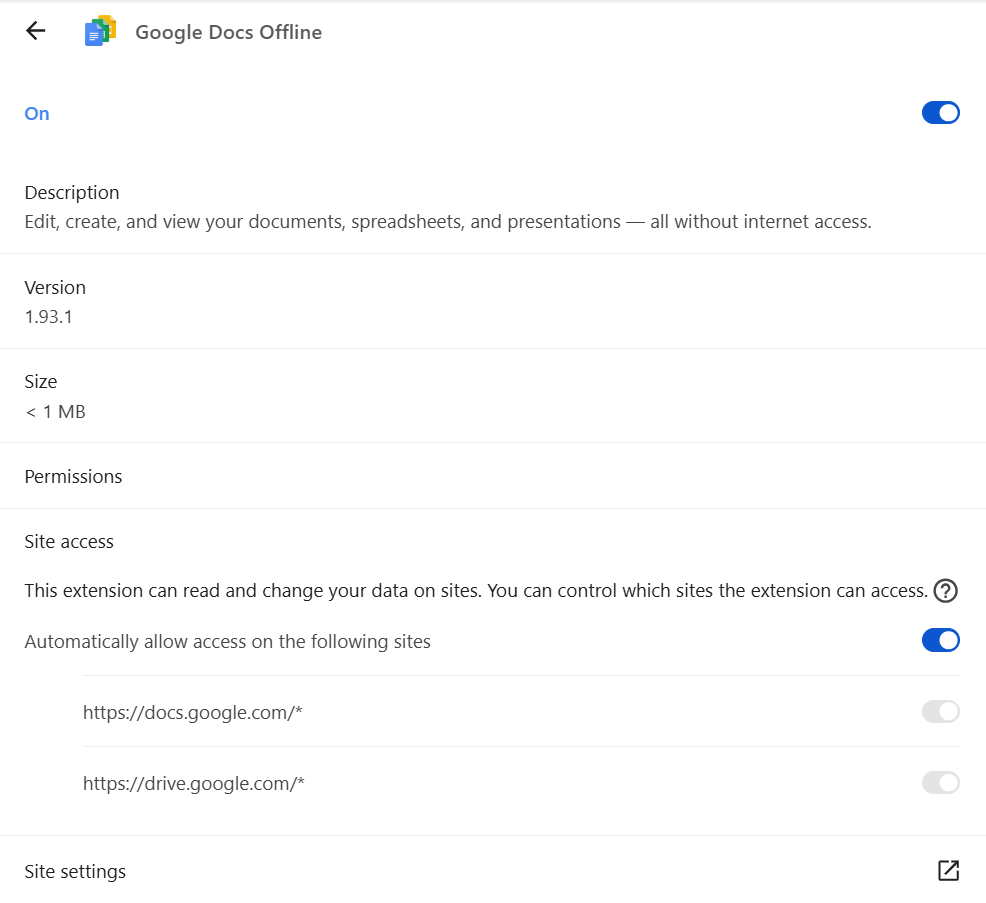
Chrome, Firefox

**Firefox:**

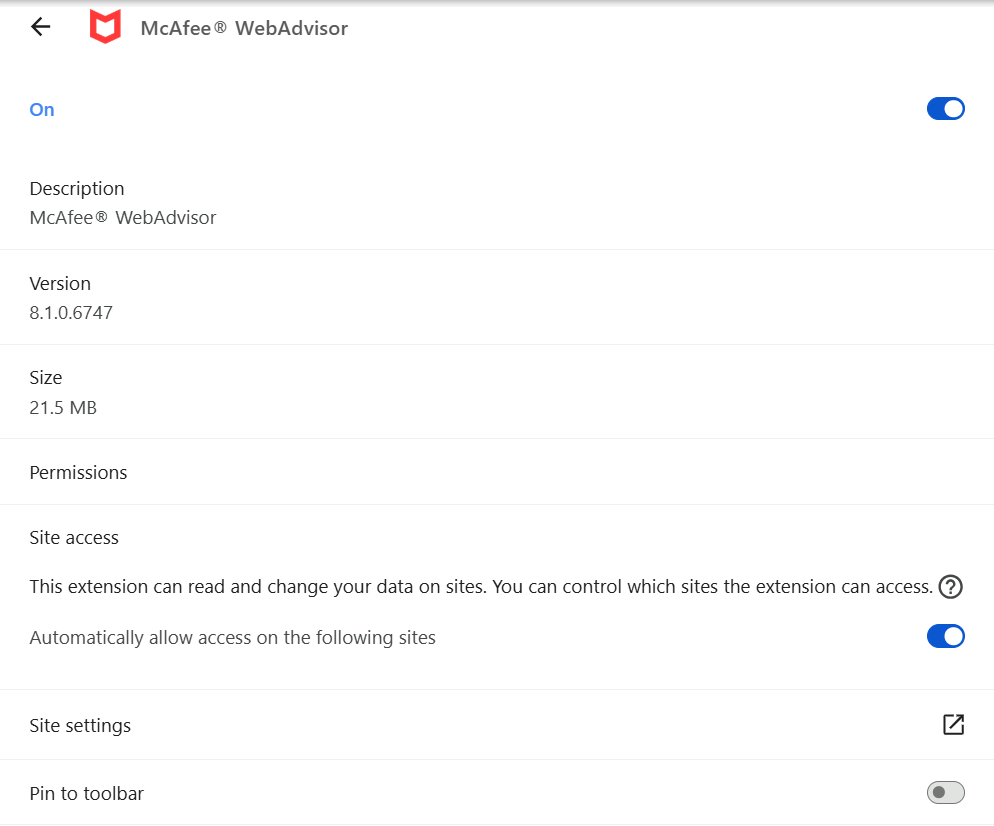
****

**Permissions for extensions:**

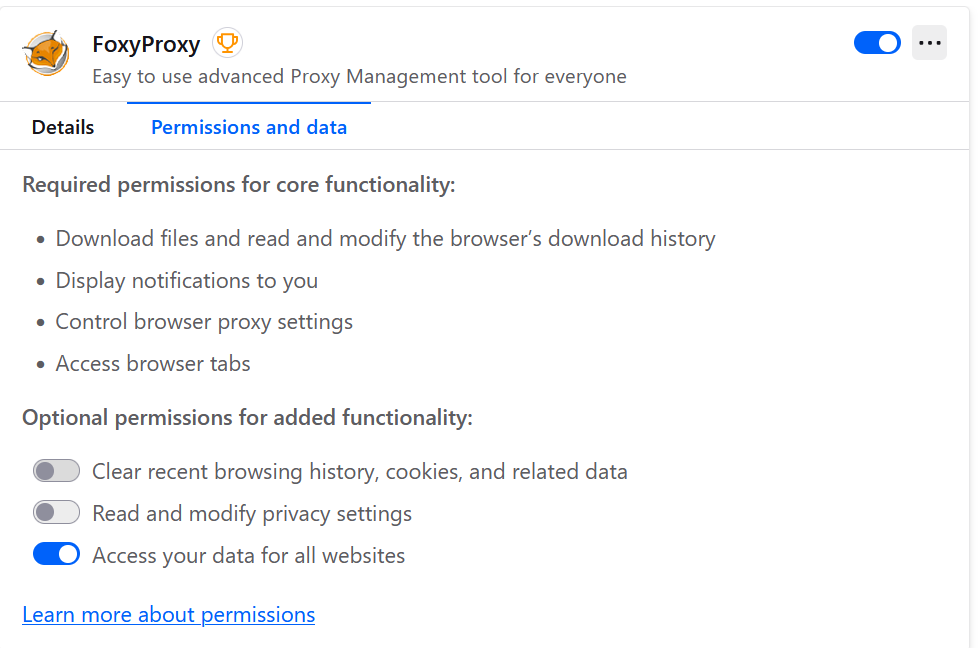
**1.Google Docs Offline:**

****

**Mcafee:**

****

**FoxyProxy:**

****

**Performance Check Summary**

* I reviewed all my installed browser extensions.
* All of them are currently in use and come from trusted sources.
* I didn’t remove any extensions, but I restarted the browser to check for any performance changes.
* After restarting, I didn’t notice any issues like slow loading, memory lag, or crashes.
* This shows that my current extensions are not affecting the browser's performance in a negative way.

**How Malicious Browser Extensions Can Harm Users**

1. **They Can Steal Sensitive Information**
   * Some extensions ask for permissions to read and change data on all the websites we visit.
   * If the extension is fake or harmful, it can misuse these permissions to steal things like passwords, session cookies, and personal details.
   * *Example:* A fake version of the “Google Translate” extension was once caught stealing data from Gmail users by secretly running background scripts.
2. **They Can Track Your Browsing Activity**
   * Some extensions secretly keep track of which websites you visit and what you do online.
   * This data is often sold to third-party companies to build user profiles and target you with ads.
3. **They Inject Ads and Redirect You**
   * Malicious extensions can insert annoying ads into websites you visit, making pages load slower and affecting your experience.
   * Some even redirect you to dangerous websites without your permission, which can lead to scams or malware.

**Actions Performed**

1. Opened the extension settings in both Chrome and Firefox browsers.
2. Carefully went through each extension to understand its function.
3. Checked the permissions and who developed the extension to ensure it’s trustworthy.
4. Looked out for any tools that weren’t being used or seemed suspicious.
5. Chose to keep the ones that are useful and regularly used.
6. Restarted both browsers to see if performance improved.
7. Confirmed that everything ran smoothly — no slowdowns or errors noticed.