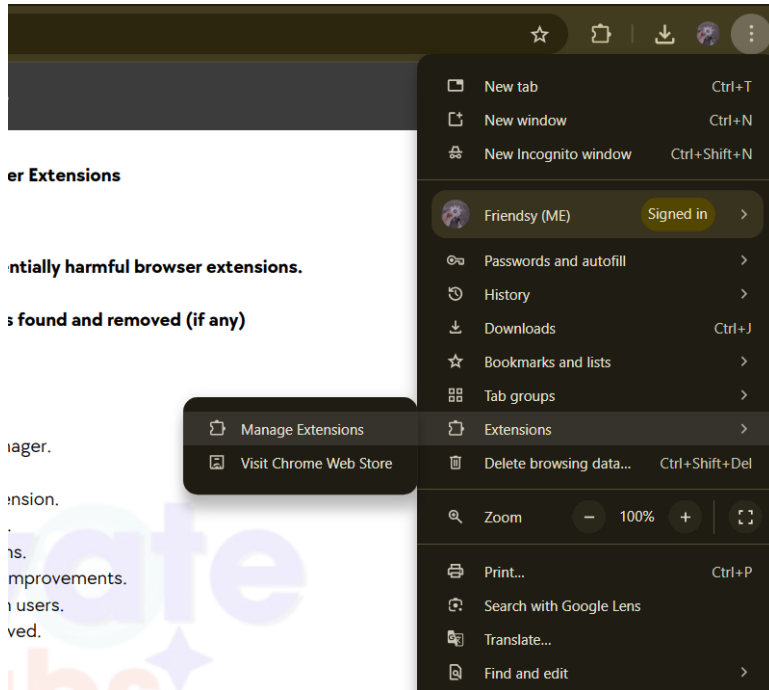
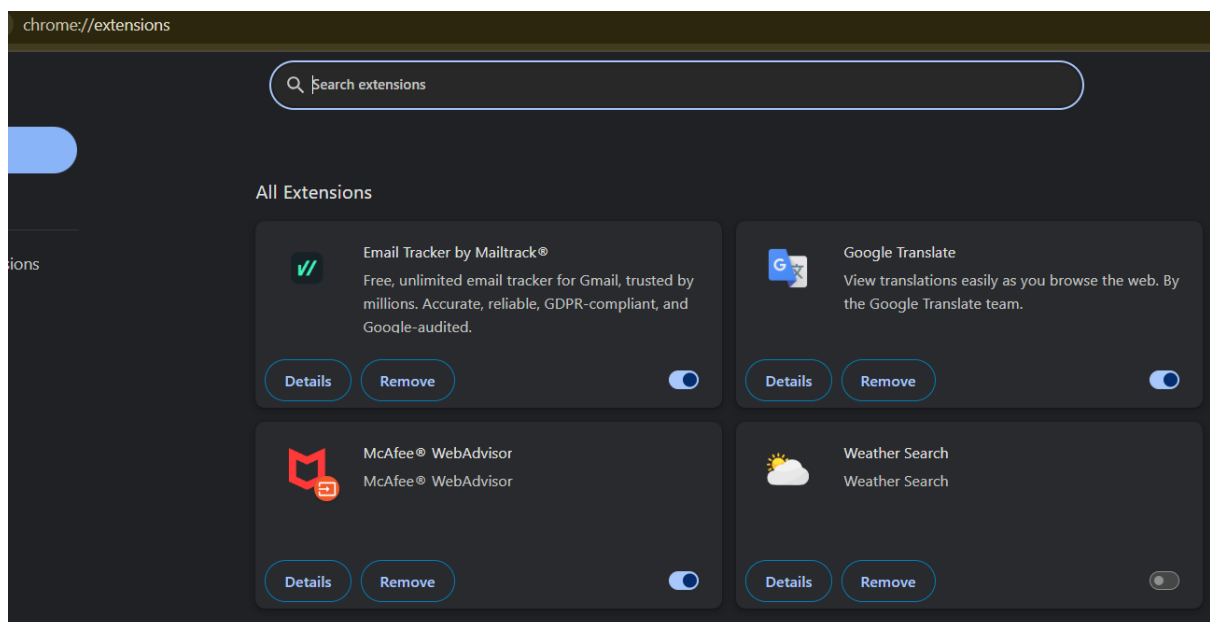


TASK 7

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

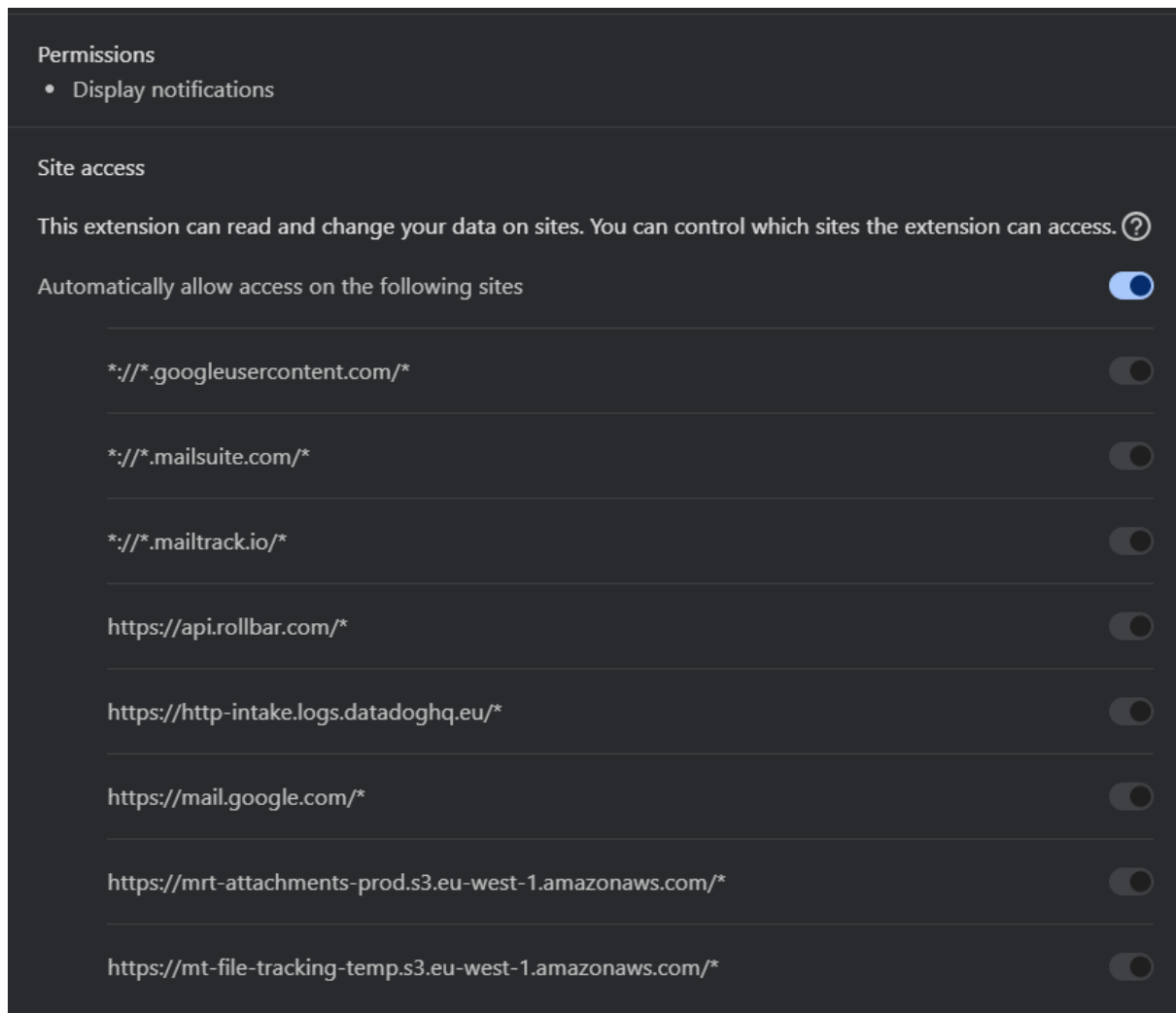


2. Review all installed extensions carefully.



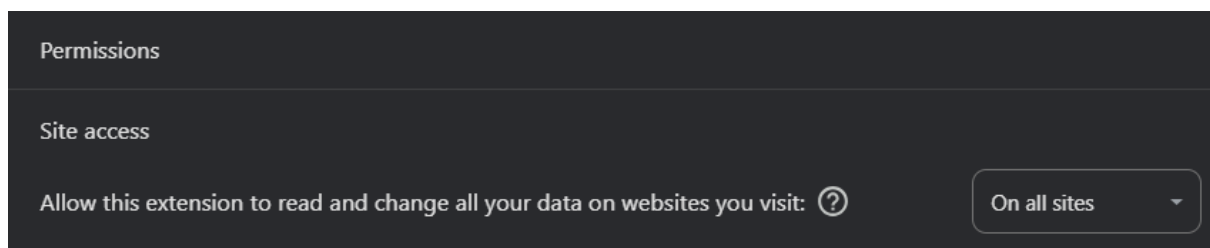
3. Check permissions and reviews for each extension.

Email Tracker by Mailtrack®



Transparency : Limited – Doesn't notify recipients about tracking by default

Google Translate

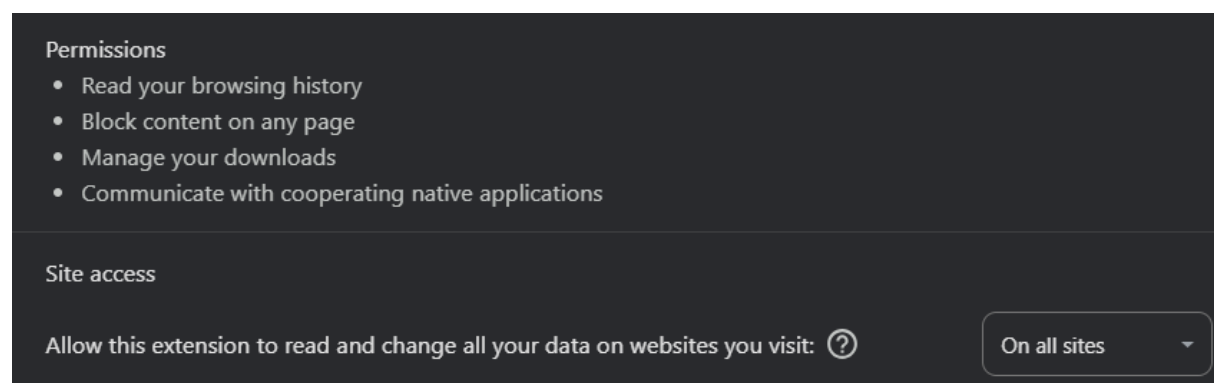


Don't Use It for Sensitive or Private Info

Avoid pasting things like:

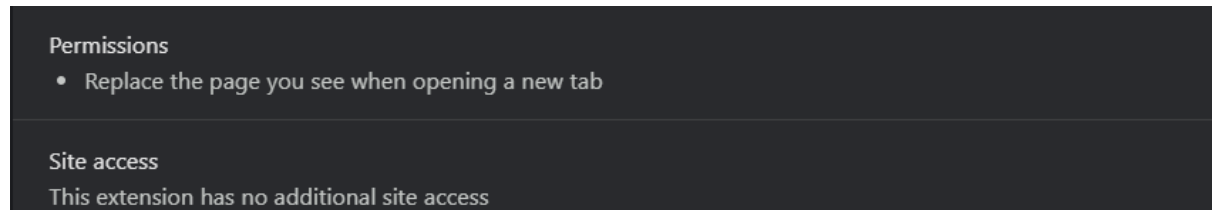
- Passwords or login credentials
- Aadhaar numbers or PAN cards
- Bank account or card details
- Confidential business documents

McAfee® WebAdvisor



Effectiveness	Strong at detecting phishing and malware links
Ease of Use	May be intrusive; alerts and pop-ups could be excessive
Privacy	Tracks downloads for scanning (may be acceptable for most users)
Removal	Users report difficulties uninstalling it

Weather Search



this can be unsafe, especially if:

- It installed **without your permission**
- It changed your **search engine or homepage** (to Bing, Yahoo, or something suspicious)
- It shows **pop-ups, ads, or redirects**
- It's **hard to remove**

4. Identify any unused or suspicious extensions.



There was no unused or suspicious extensions.

5. Remove suspicious or unnecessary extensions.

6. Restart browser and check for performance improvements.

7. Research how malicious extensions can harm users.

Malicious extensions often appear useful (like weather tools, PDF converters, or video downloaders), but once installed, they can exploit your browser to **spy, steal, or hijack** your data and activity.

 Method	 Description
1. Stealing Personal Data	They can read everything you type — including passwords, credit card numbers, or messages — and send it to attackers.
2. Tracking You Across Sites	Even if you're not using the extension actively, it can track your every website visit, search, and click.
3. Inserting Ads (Ad Injection)	They insert ads into websites (even Google or YouTube) to earn money unethically. This slows your browser and may expose you to shady sites.
4. Redirecting Search Results	Your search engine (e.g., Google) gets hijacked and replaced by fake search engines like "Search Baron", "MyWay", or others that collect your data.
5. Auto-installing More Malware	Some extensions download other malware silently, like crypto miners or trojans.
6. Hijacking Social Accounts	Some read cookies and hijack sessions, letting hackers access your social media or email without your password.

7. Fake Security Warnings	They may show fake popups like “Your PC is infected” to trick you into buying fake antivirus software.
8. Crypto Mining (Hidden)	They use your CPU in the background to mine cryptocurrency, slowing your PC. This is called cryptojacking .

Real-Life Examples

1. "Hover Zoom" Extension

- Once popular, it was sold to a shady company that started tracking users and injecting ads.
- ⚠ Used millions of browsers as a surveillance tool.

2. "YouTube Downloader" Clones

- Some contained hidden keyloggers or would hijack search engines.

3. DataSpii Breach (2019)

- Several Chrome extensions were caught leaking users’ sensitive info — including corporate secrets and tax data — all through their browsers.

How to Protect Yourself

Step	Why
Only install from trusted developers	Check reviews, star ratings, and update history

Review permissions carefully	If a weather app wants to “Read all your browsing history” — that’s suspicious
Avoid pirated, cracked, or unofficial browser tools	They're often laced with hidden spyware
Use security tools	Antivirus + browser like Brave/Firefox with privacy focus
Regularly audit extensions	Remove anything unused or unfamiliar

8.Document steps taken and extensions removed.