

Task 7: Identify and Remove Suspicious Browser Extensions

Objective:

To learn how to spot and remove potentially harmful or unnecessary browser extensions that could affect browser performance or compromise user privacy.

Tools Used:

Web Browser: Google Chrome (Windows)

Steps Followed:

1. Opened Chrome's extension page: chrome://extensions.
2. Reviewed all installed extensions: Google Docs Offline and McAfee WebAdvisor.
3. Checked each extension's permissions and source.
4. Kept Google Docs Offline (trusted and useful).
5. Removed McAfee WebAdvisor due to potential redundancy.
6. Restarted the browser to check for performance improvement.
7. Researched how malicious extensions can steal data or impact system performance.

Extensions Review Table:

Extension Name	Status	Trusted	Action	Reason
Google Docs Offline	Active	Yes	Kept	From Google; safe for c
McAfee WebAdvisor	Removed	Mixed	Removed	Can be redundant if and

Reason for Removing McAfee WebAdvisor:

The McAfee WebAdvisor extension, although developed by a reputed security company, was considered for removal due to several reasons. Firstly, the extension adds another layer of protection that may be redundant if the system already has an up-to-date antivirus or browser security enabled, such as Windows Defender or built-in Google Safe Browsing. Secondly, it was observed that such extensions can sometimes slow down browser performance by scanning websites and injecting scripts. Furthermore, McAfee extensions have access to sensitive browsing data, which raises privacy concerns if the user is not actively using the full McAfee suite. Given that browser speed and simplicity are critical for daily use, and the fact that this

Task 7: Identify and Remove Suspicious Browser Extensions

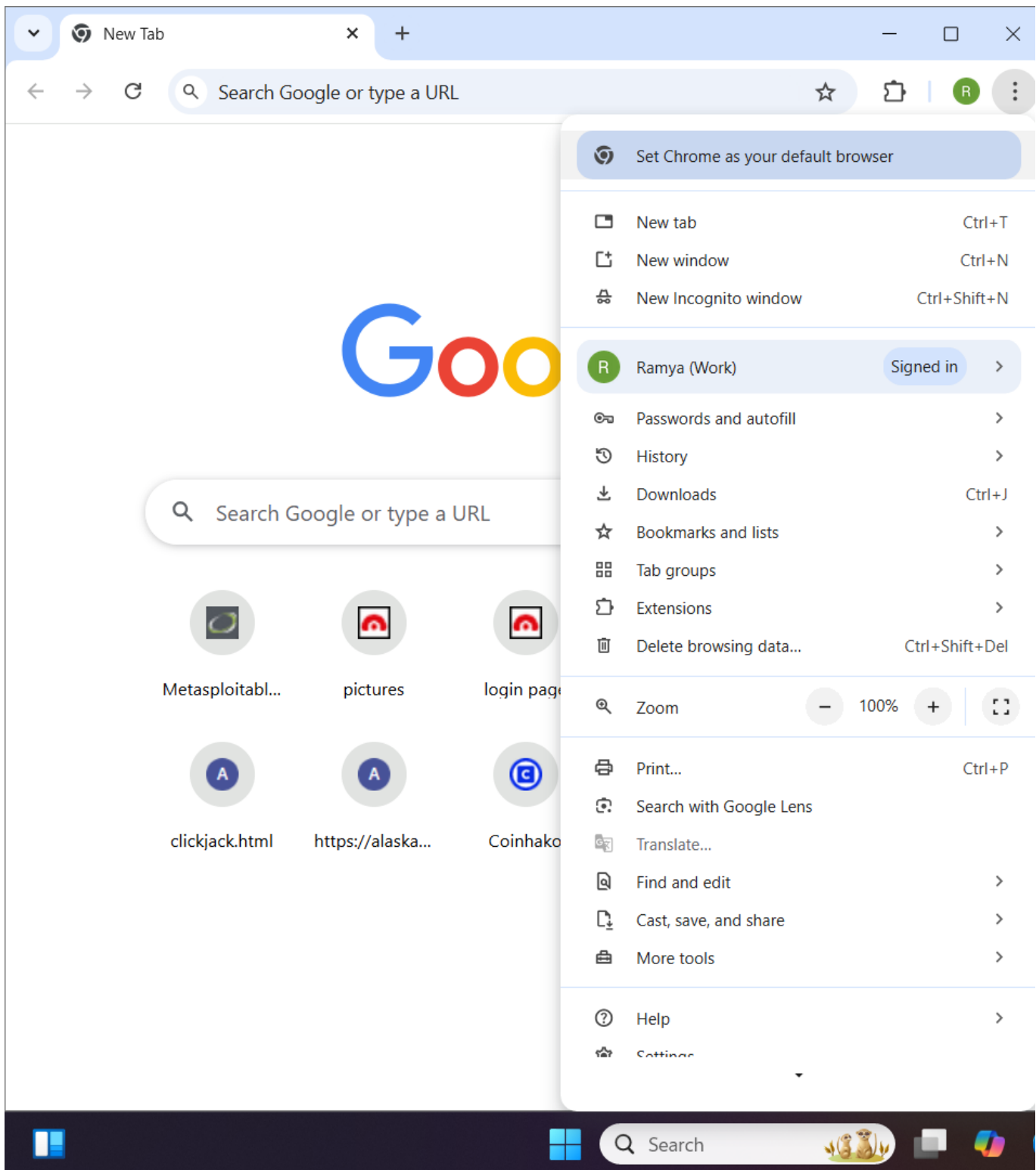
extension was not essential for current tasks, it was deemed unnecessary and safely removed to improve system performance and reduce clutter.

What I Learned:

- Always verify permissions and publisher of extensions.
- Unused or unknown extensions can pose risks.
- Remove extensions that duplicate existing software.
- Some extensions can slow down or expose users to malware.

Screenshots:

Task 7: Identify and Remove Suspicious Browser Extensions




Task 7: Identify and Remove Suspicious Browser Extensions

Extensions

Developer mode ☐

Your [profile is managed](#) by psgrcw.ac.in

All Extensions




Google Docs Offline

Edit, create, and view your documents, spreadsheets, and presentations — all without internet access.

[Details](#) [Remove](#)

☒



McAfee® WebAdvisor

McAfee® WebAdvisor

[Details](#) [Remove](#)

☒

Chrome chrome://extensions/?id=fheoggkfdfchfpheiefdbepaoaicaho

Extensions


Search extensions

[My extensions](#)

[Keyboard shortcuts](#)

Discover more extensions and themes on the [Chrome Web Store](#)

Size	21.5 MB
Permissions	
Site access	<p>This extension can read and change your data on sites. You can control which sites the extension can access. ?</p> <p>Automatically allow access on the following sites <input checked="" type="checkbox"/></p>
Site settings	Site settings
Pin to toolbar	<input type="checkbox"/>
Allow in Incognito	<p>Warning: Google Chrome cannot prevent extensions from recording your browsing history. To disable this extension in Incognito mode, unselect this option.</p> <input type="checkbox"/>
Allow access to file URLs	<input type="checkbox"/>
View in Chrome Web Store	View in Chrome Web Store
Source	Added by a third-party
Remove extension	Remove extension



Remove "McAfee® WebAdvisor"?

☐ Report abuse

[Remove](#) [Cancel](#)

26°C
Haze

Search

ENG IN 22:30 03-07-2025