

Task 7 — Identify and Remove Suspicious Browser Extensions

Author: Yuvraj Yadav

Date: 30-10-2025

Browser Used: Google Chrome (v129+)

Platform: macOS

1 Objective

The objective of this task was to review all installed **Google Chrome extensions**, evaluate their permissions, and identify any potentially suspicious or unnecessary ones.

The task aimed to improve awareness of **browser-level security**, understand how extensions interact with user data, and practice safe extension management.

2 Tools and Environment

- **Browser:** Google Chrome (macOS version)
- **Tools:** Chrome Settings → Extensions Manager
- **System:** macOS (Intel-based)

3 Steps Performed

Step 1 — Access Extensions Manager

1. Opened Chrome browser.

Navigated to:

`chrome://extensions/`

- 2.

3. Viewed the list of all installed extensions and their permissions.




Step 2 — Review Each Extension

Checked each extension for:

- Developer source (published by Google or verified publisher).
- Required permissions (e.g., “Read and change data on all websites”).
- User ratings and reviews in the Chrome Web Store.
- Update the status and last modified date.

Step 3 — Identify Suspicious Extensions

Flagged extensions that requested excessive permissions or had poor reviews.

Extension Name	Publisher	Permissions	Risk Level	Action Taken
“Video Downloader Pro”	Unknown	Access to all websites, read browsing history	 High	Removed
“Dark Theme for YouTube”	Unverified	Modify data on YouTube	 Medium	Kept after review
“Google Docs Offline”	Google LLC	Offline access only	 Safe	Kept

⚠ Extensions requesting “Read and change data on all sites” can pose privacy risks and should be audited carefully.

Step 4 — Remove Unnecessary Extensions

Removed “Video Downloader Pro” and other unused tools using the **Remove** button in <chrome://extensions>.

Restarted the browser to complete the cleanup.

Step 5 — Verify and Monitor

Reopened `chrome://extensions` to confirm remaining extensions were verified and essential only.

Checked performance improvement — page load time and CPU usage reduced slightly (~10-12%).

4 Key Findings

Category	Observation	Action
Suspicious Permissions	Some extensions requested full data access	Removed
Unused Extensions	Found 2 that were inactive for months	Removed
Trusted Extensions	Kept Google-verified and productivity tools	Retained
Performance Impact	Browser start time improved after the cleanup	Positive

5 Security Insights and Learnings

- Extensions can act like mini-applications inside the browser and access sensitive data such as cookies and form inputs.
- **Malicious extensions** can inject ads, steal credentials, or track browsing activity.
- **Warning signs:** unverified publisher, excessive permissions, redirect behavior.
- Always install extensions **only from the official Chrome Web Store**.
- Check permissions before installing and review regularly to maintain browser hygiene.

6 Outcome

Successfully identified and removed unnecessary and suspicious extensions from Google Chrome.

Browser performance and security posture improved after cleanup.

Skills Gained:

- Extension security analysis
- Permission evaluation and risk assessment
- Safe extension management practices
- Browser performance optimization

7 Attachments (for GitHub Repo)

1. **screenshots/** — includes:
 01_extensions_list.png, 02_permissions_check.png,
 03_remove_extension.png, 04_final_review.png
2. **report.md** — this document
3. **README.md** — task summary and findings