🛡️ Task 7: Identify and Remove Suspicious Browser Extensions

Tool Used: Google Chrome
Task Type: Hands-on + Research-Based

🎯 Objective:

To identify and remove potentially harmful or unnecessary browser extensions from Google Chrome, analyze their permissions, and learn how malicious extensions can affect browser security and user privacy.

⬚ Steps Followed:

1. **Opened Chrome Extension Manager:**

   - Visited chrome://extensions/

   - Enabled Developer Mode to view additional details

2. **Reviewed Each Installed Extension:**

   - Inspected names, publishers, and permissions

   - Used Web Store reviews, permission analysis, and manual inspection

3. **Analyzed Permissions:**

   - Flagged extensions with dangerous permissions like:

     - "Read and change all your data on all websites"

     - "Manage downloads"

     - "Access the page debugger backend"

     - "Read your browsing history"

4. **Removed Suspicious or Unnecessary Extensions:**

   - Evaluated if functionality justified the permissions

   - Uninstalled those with unjustified or high-risk permissions

5. **Researched Potential Risks:**

   o Understood how malicious extensions can spy on users, steal data, inject ads, or redirect browsing

6. **Restarted Chrome:**

   o Verified performance improvement and security assurance

🔍 **Extensions Reviewed & Actions Taken:**

Extension Name	Action Taken	Permissions Reviewed
Free VPN for Chrome – VPN Proxy VeePN	✕ Removed	Excessive permissions including all-site access, managing apps, privacy settings
Google Docs Offline	☑ Kept	Trusted Google extension, scoped to docs and drive URLs only
Image Downloader – Save Pictures	☑ Kept	Manages downloads and blocks content — matches intended purpose
Material You NewTab	☑ Kept	Replaces new tab page; accesses a few safe websites like Google, Reddit
McAfee® WebAdvisor	☑ Kept	Trusted security tool from McAfee, used for threat scanning and safe browsing
Web Page Downloader	✕ Removed	Access to browsing history — removed due to privacy concerns
Web to PDF	✕ Removed	Dangerous permissions — DevTools backend access + read/change all website data

---

⊟ What I Learned:

- How to review Chrome extensions for security & privacy risks

- Which permissions are high-risk (e.g., all-site access, download control, history access)

- How browser extensions can track, steal data, or inject malicious code

- Importance of publisher verification and permission minimalism

---

⚲ Final Outcome:

By completing this task, I learned how to critically inspect browser extensions for potential threats, how permissions can be misused, and best practices for browser security hygiene.