Browser Extensions Security Audit Report

Date: 2025-07-03

Browser Used: Google Chrome

Performed By: Srishti Pandey

# 🎯 Objective

To identify and remove potentially harmful or unnecessary browser extensions to enhance security and browser performance.

# 🔧 Tools Used

- Web Browser: Google Chrome

- Extension Manager (chrome://extensions)

# 📋 Steps Followed

1. Opened Extension Manager: Navigated to chrome://extensions to view all installed browser extensions.
2. Reviewed Installed Extensions: Carefully reviewed the list of installed extensions. Checked the permissions granted and looked up user reviews on the Chrome Web Store.
3. Checked for Suspicious/Unused Extensions: Marked extensions with excessive permissions or low ratings as suspicious. Identified unused extensions as unnecessary.
4. Removed Unnecessary/Suspicious Extensions:  
    - Removed extensions that hadn’t been used in a while.  
    - Uninstalled one extension with high permissions and vague functionality.
5. Restarted the Browser: Restarted Google Chrome to complete the removal process.
6. Checked Browser Performance: Observed slight improvement in browser startup and page load times.
7. Research on Risks of Malicious Extensions:  
    - Malicious extensions can track browsing activity, steal login credentials, insert ads, or redirect traffic.  
    - Some extensions can even inject scripts into visited websites to exploit browser vulnerabilities.

# 🧹 Suspicious or Unused Extensions Removed

|  |  |
| --- | --- |
| Extension Name | Reason for Removal |
| PDF Converter Tool | Unused and requested excessive permissions |
| Shopping Helper Pro | Vague functionality, many negative reviews |

# ✅ Conclusion

Regularly reviewing browser extensions is a good cybersecurity practice. This simple audit improved browser performance and reduced potential security risks.

Report generated manually by reviewing the local Chrome browser extensions and documenting all actions taken.