Browser Extension Audit Report

Task: Identifying and Removing Suspicious Browser Extensions

Objective: Learn how to review and remove unnecessary or risky browser extensions to improve browser safety and performance

Browser Used: Google Chrome

1. Introduction

Browser extensions add extra features to browsers, but some can create security and privacy risks. These risks may come from extensions that are unsupported, untrusted, or ask for too many permissions. The goal of this task was to inspect all installed Chrome extensions, check their trust and usefulness, and remove anything suspicious or outdated.

2. Methodology

Steps followed:

- Opened Chrome and visited chrome://extensions
- Reviewed all installed extensions
- Checked if they were enabled or disabled
- Looked into the developer, popularity, recent updates, and how often they are used
- Searched online for unknown extensions to see if they had any issues
- Removed anything suspicious or no longer useful
- Restarted Chrome to observe any changes

3. Extensions Reviewed

Extension Name	Status	Usage	Suspicious?	Review Summary
BuiltWith Technology Profiler	Enabled	Regularly Used	No	A trusted tool for checking website technologies. Safe and commonly used.
Cookie Notice Blocker	Disabled	Not Used	Yes	Disabled by Chrome. Not supported and outdated. Removed.
Google Docs Offline	Disabled	Rarely Used	No	Official Google extension. Safe but inactive.
Mailvelope	Disabled	Rarely Used	No	Secure email extension using PGP. Open-source and trusted.
UltraSurf VPN	Enabled	Occasionally	Maybe	Free VPN with limited developer transparency. Needs further review.
Wappalyzer	Enabled	Regularly Used	No	A popular tool for tech profiling. Actively maintained and safe.

4. Actions Taken

- Removed Cookie Notice Blocker as it was unsupported and unused.
- Kept trusted or official extensions like BuiltWith, Wappalyzer, and Google Docs Offline.
- Mailvelope was kept but remains inactive.
- UltraSurf VPN is still installed for now but flagged for future review due to limited information about its developer.

5. Post-Cleanup Observations

- Extensions list looks cleaner and easier to manage
- No unusual pop-ups or behavior after the cleanup
- Chrome startup seemed slightly faster

6. Risks of Malicious Extensions

Extensions with bad code or hidden purposes can:

- Steal login details and browsing history
- Inject ads or trackers into web pages
- Redirect users to fake websites or phishing pages
- Slow down the browser or cause crashes
- Gain high-level permissions that bypass browser controls

Even good extensions can become risky after updates or ownership changes. That’s why it’s important to review extensions regularly.

7. Conclusion

This task showed the importance of checking browser extensions every now and then. By removing the ones that are not needed or no longer supported,

browser speed and safety can improve. Only install extensions from known and trusted sources. Unused ones should be reviewed often or removed.

Staying alert helps avoid silent risks caused by unknown or outdated extensions. Keeping just the useful and safe ones is the best way to browse securely.