Browser Extension Security & Performance Check Report

Date: 02-Oct-2025
Conducted By: Sameer Chavan
Browser: Google Chrome

1. Accessed Extension Manager

Opened Chrome’s extension manager (chrome://extensions) to review all installed extensions.

2. Extensions Reviewed

Reviewed each installed extension for authenticity, purpose, and last update history.

3. Permissions and Reviews

Checked requested permissions and verified reviews from Chrome Web Store. Ensured only trusted developers were allowed.

4. Identified Suspicious/Unused Extensions

Example: Found 'PDF Converter Free' extension installed, which had no reviews, excessive permissions (access to all sites, clipboard), and a suspicious publisher.

5. Removed Extensions

Removed the following unnecessary/suspicious extensions: - PDF Converter Free (excessive permissions, unknown publisher) - Duplicate Ad Blocker (multiple similar extensions installed) Kept only trusted ones like uBlock Origin, Grammarly, and LastPass.

6. Restart & Performance Check

Restarted browser. Observed faster startup time, lower memory usage, and smoother browsing performance.

7. Research on Risks of Malicious Extensions

Malicious browser extensions can: - Steal passwords & browsing data - Inject ads or redirect websites - Track user activity - Cause slowdowns or crashes Example: In 2020, the 'Great Suspender' Chrome extension was caught injecting malicious code and was removed by Google.

8. Documentation

Steps taken were recorded. Extensions removed: PDF Converter Free, Duplicate Ad Blocker. Extensions kept: uBlock Origin, Grammarly, LastPass.

Conclusion

The cleanup improved security and browser performance. Regular monitoring is recommended, and extensions should only be installed from official trusted sources.