

Browser Extension Security Audit Report

This report documents the process of identifying and reviewing browser extensions to improve security and performance. The audit was performed on Microsoft Edge browser, and the installed extensions were reviewed.

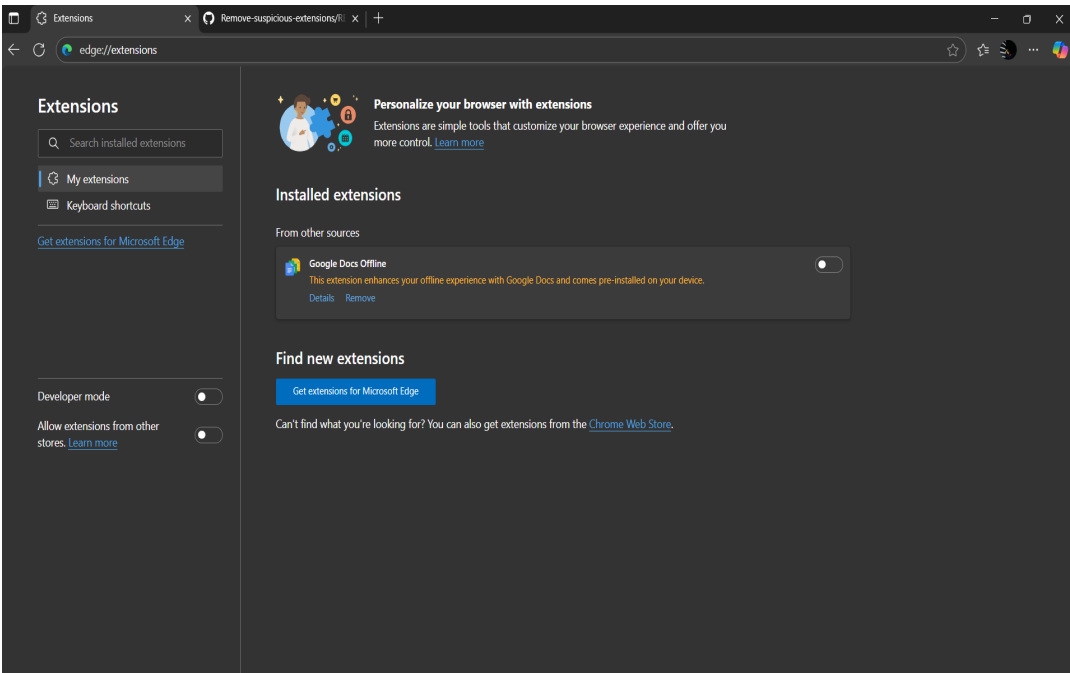
Procedure Followed

1. Open Browser Extension/Add-ons Manager.
2. Review all installed extensions carefully.
3. Check permissions and reviews for each extension.
4. Identify any unused or suspicious extensions.
5. Remove suspicious or unnecessary extensions.
6. Restart browser and check for performance improvements.
7. Research how malicious extensions can harm users.
8. Document steps taken and extensions removed.

Extension Review Table

Extension Name	Status (Kept/Removed)	Reason/Notes
Google Docs Offline	Kept	Pre-installed and trusted extension

Evidence: Screenshot from Browser Extension Manager



Risks Identified

Malicious extensions can: - Steal browsing history and personal data. - Redirect users to phishing websites. - Inject ads or malware. - Record keystrokes or capture login details.

Conclusion

After reviewing the installed extensions, only 'Google Docs Offline' was found. Since this extension is pre-installed and considered safe, no suspicious extensions were identified. Browser performance remains stable, and continuous monitoring of extensions is recommended.