Security Audit: Identifying and Removing Suspicious Browser Extensions

Objective: Detect and remove potentially harmful or unnecessary browser extensions to enhance security and performance.
Browser Used: Google Chrome

Audit Procedure

1. **Accessed Extension Settings:** Navigated to `chrome://extensions/` to view all installed browser extensions.
2. **Evaluated Extensions:** Reviewed each extension's name, permissions, developer information, and recent activity.
3. **Researched Reputation:** Checked online reviews, ratings, and security reports for each extension.
4. **Identified Risks:** Flagged extensions that were unused, inactive, or exhibited suspicious behavior (e.g., excessive permissions, adware concerns).
5. **Removed Suspicious Extensions:** Safely uninstalled flagged extensions from the browser.
6. **Post-Audit Testing:** Restarted Chrome and monitored for improved performance and functionality.

Extension Audit Summary

Extension Name	Status	Action Taken
Google Docs Offline	Safe, verified by Google	Retained
Guardio Protection for Chrome	Suspicious; linked to adware	Removed
Netcraft Extension	Safe, reputable security tool	Retained
OWASP Penetration Testing Kit	Safe, trusted by security community	Retained
Shodan	Safe, well-known security tool	Retained
Sputnik	Inactive, no recent updates	Removed
Vulners Web Scanner	Safe, reputable security tool	Retained
Wappalyzer	Safe, widely used by professionals	Retained

Results and Observations

- **Extensions Removed:** Two extensions (Guardio Protection for Chrome, Sputnik) were removed due to potential risks or inactivity.
- **Performance Improvements:** Post-removal, browser loading times improved, and background activity decreased.
- **Security Enhancements:** Eliminated potential risks of data leakage, unauthorized tracking, or adware from suspicious extensions.

Recommendations

- **Regular Audits:** Review browser extensions quarterly to identify and remove unused or risky extensions.
- **Verify Sources:** Only install extensions from trusted developers or the Chrome Web Store with high ratings and recent updates.
- **Monitor Permissions:** Avoid extensions requesting excessive permissions (e.g., access to all website data) unless necessary.
- **Stay Informed:** Use resources like security blogs or tools (e.g., Netcraft, VirusTotal) to research extension safety.

Conclusion

This audit successfully identified and removed two potentially harmful or unnecessary extensions, improving browser performance and reducing security risks. Regular extension reviews are critical to maintaining a secure and efficient browsing environment.