# Identify and Remove Suspicious Browser Extensions

## Objective:

Learn to spot and remove potentially harmful browser extensions.

## Tools:

Google Chrome Browser

## Steps Taken:

1. Opened Chrome browser and navigated to the extensions manager (chrome://extensions/).
2. Reviewed all installed extensions for suspicious names, high-risk permissions, and unknown developers.
3. Checked the Chrome Web Store for extension ratings, developer info, and recent updates.
4. Evaluated each extension's purpose, usage, and redundancy given Chrome's capabilities.
5. Removed any redundant or privacy-intrusive extensions.
6. Restarted the browser and monitored performance improvements.
7. Researched how malicious extensions operate (e.g., data harvesting, ad injection, phishing).
8. Documented all findings, extension details, and actions taken in this report.

## Extensions Reviewed:

|  |  |  |  |
| --- | --- | --- | --- |
| Extension Name | Version / ID | Status | Reason / Notes |
| AdBlock for Chrome | v6.23.0 / gighmmpiobklfepjocnamgkkbiglidom | Kept | Verified official version from getadblock.com. Trusted and widely used. |
| Google Docs Offline | v1.93.1 / ghbmnnjooekpmoecnnnilnnbdlolhkhi | Kept | Official Google extension. Enables offline access to Docs/Sheets/Slides. |
| McAfee WebAdvisor | v8.1.0.6256 / fheoggkfdfchfphceeifdbepaooicaho | Removed | Safe but redundant. High-level permissions and overlaps with other protections. |

## Performance After Removal:

After removing McAfee WebAdvisor, there was a slight improvement in browsing speed and fewer background processes were observed. Chrome's built-in protections remained active and functional.

## Risks of Malicious Extensions:

* Can track browsing history and behavior across websites.
* May inject ads, redirect search queries, or slow down system performance.
* Can steal sensitive data such as login credentials and credit card info.
* Often bundled with free software and installed without user knowledge.
* Use permissions to modify or access data on all websites, posing privacy risks.

