# Browser Extension Security Report

## Objective

The objective of this task is to identify, analyze, and remove suspicious or unnecessary browser extensions from Google Chrome and Mozilla Firefox to improve browser performance and enhance security.

## Tools Used

• Google Chrome  
• Mozilla Firefox

## Steps Followed

1. Opened the browser extension manager (chrome://extensions/ or about:addons).

2. Reviewed all installed extensions and their permissions.

3. Checked the developer’s name, reviews, and ratings for each extension.

4. Identified any unused, suspicious, or unverified extensions.

5. Removed suspicious or unnecessary extensions.

6. Restarted the browser to apply changes.

7. Noted performance improvements and reduced unwanted ads or pop-ups.

## Extensions Found and Actions Taken

|  |  |  |  |
| --- | --- | --- | --- |
| Browser | Extension Name | Status | Reason for Removal |
| Chrome | PDF Converter Pro | Removed | Unknown developer, access to all sites |
| Chrome | Grammarly | Kept | Trusted, verified |
| Firefox | Free VPN | Removed | Unverified publisher, performance issues |
| Firefox | uBlock Origin | Kept | Trusted, open-source |

## How Malicious Extensions Can Harm Users

• Steal personal data such as passwords, browsing history, or payment details.

• Inject unwanted ads or redirect to malicious websites.

• Spy on user activity and compromise privacy.

• Modify search engine or homepage settings.

• Slow down browser performance or cause crashes.

## Conclusion

After removing suspicious extensions, the browsers showed better performance and fewer unwanted ads. Regularly checking and cleaning browser extensions is an important security practice to stay safe online.