Task 7: Identify and Remove Suspicious Browser Extensions

# Objective

The objective of this task is to learn how to identify and remove potentially harmful browser extensions. This exercise aims to enhance awareness of browser security and the implications of malicious extensions.

# Tools Used

- Google Chrome  
- Mozilla Firefox

# Steps Taken

1. Opened the browser’s extensions or add-ons manager (chrome://extensions and about:addons).  
2. Reviewed all installed extensions.  
3. Checked the permissions and user reviews for each extension.  
4. Identified unused or suspicious extensions.  
5. Removed extensions that were unnecessary or had suspicious permissions.  
6. Restarted the browser to apply changes.  
7. Researched how malicious extensions can impact browser and system security.

# Suspicious Extensions Found and Removed

Google Chrome:  
- Extension: PDF Converter  
 Reason: Excessive permissions, redirects, poor user reviews.  
- Extension: Weather Tab  
 Reason: Requests access to all websites, not used regularly.  
  
Mozilla Firefox:  
- Extension: Video Downloader Pro  
 Reason: Reports of malware behavior, unnecessary permissions.

# Outcome

By completing this task, I gained an understanding of how browser extensions can affect security. I learned to evaluate extensions based on their permissions, origin, and reviews. As a result, I removed suspicious extensions and improved the security posture of my browser.

# Conclusion

Regular auditing of browser extensions is a good practice. Many users unknowingly install extensions that can lead to privacy breaches or security vulnerabilities. This task helped me realize the importance of being cautious with browser add-ons and proactively managing them.