**Task 7: Identify and Remove Suspicious Browser Extensions**

## Objective

To develop the ability to review, identify, and remove potentially harmful or unnecessary browser extensions, thereby enhancing browser security, reducing attack surfaces, and improving overall performance.

## Tools Used

• Microsoft Edge  
• Google Chrome

## Procedure

• Access the Extensions/Add-ons Manager in both browsers.

• Inventory all installed extensions.

• Review each extension’s permissions, reviews, developer reputation, and last update date.

• Identify suspicious or unnecessary extensions.

• Remove risky extensions and keep trusted, actively used ones.

• Restart browsers and check for performance improvements.

• Research the risks of malicious extensions, such as data theft, ad injection, or browser hijacking.

## Microsoft Edge

|  |  |  |  |
| --- | --- | --- | --- |
| **Extension Name** | **Status** | **Purpose** | **Reason for Removal / Keep** |
| McAfee® WebAdvisor | ✅ Kept | Provides web security, phishing protection, and malicious link blocking. | Verified safe; actively used for online protection. |
| Microsoft Power Automate (Legacy) | ❌ Removed | Automates workflows and tasks across Microsoft services. | Not in use; legacy version with unnecessary permissions for current workflows. |
| Google Docs Offline | ✅ Kept | Allows editing and viewing of Google Docs files offline. | Trusted extension; useful for offline document work. |
| OKX Wallet | ❌ Removed | Cryptocurrency wallet extension for trading and managing digital assets. | Not in use; high permissions and potential phishing target. |

## Google Chrome

|  |  |  |  |
| --- | --- | --- | --- |
| **Extension Name** | **Status** | **Purpose** | **Reason for Removal / Keep** |
| FoxyProxy | ✅ Kept | Simplifies proxy configuration and switching between multiple proxies. | Verified safe; essential for network testing and secure proxy use. |
| Hack-Tools | ✅ Kept | Collection of penetration testing utilities and bug bounty helper tools. | Trusted by security professionals; actively used in cybersecurity workflows. |

## Outcome

• Reviewed and evaluated all installed browser extensions across Microsoft Edge and Google Chrome.  
• Removed unused high-permission extensions to reduce attack surface.  
• Kept trusted, actively used security and productivity extensions.  
• Improved browser performance and strengthened security posture.