Task 7 Report – Identify and Remove Suspicious Browser Extensions

Objective:

To identify, evaluate, and remove potentially harmful or unnecessary browser extensions in order to improve browser security and performance.

1. Steps Taken

1. Opened the browser's extensions manager: Chrome (chrome://extensions/) or Firefox (Ctrl+Shift+A).
2. Reviewed all installed extensions and noted their names.
3. Checked details and permissions for each extension.
4. Searched online for reviews and potential security warnings.
5. Identified unused or suspicious extensions.
6. Removed unnecessary or risky extensions.
7. Restarted browser to apply changes.
8. Observed performance improvements and verified safe operation.
9. Researched potential risks of malicious extensions.

2. Extensions Found

Extension Name	Purpose/Description	Permissions Granted	Status
Example Safe Tool	Screenshot capture utility	Access to active tab only	Kept
Example Suspicious	Unknown extension installed with free app	Read and change all data on all websites	Removed
Example Unused Add-on	Old shopping coupon extension	Access to browsing activity	Removed

3. Suspicious Extensions Removed

Name: Example Suspicious
Reason: Unfamiliar, excessive permissions, poor online reviews.

Name: Example Unused Add-on
Reason: No longer used, unnecessary data access.

4. Performance Improvements Observed

- Faster page load times.
- No more unexpected pop-up ads.
- Reduced memory usage.

5. Risks of Malicious Extensions (Research Findings)

- Data Theft: Can steal passwords, credit card numbers, and personal details.
- Tracking: Monitor and log browsing habits without consent.
- Ad Injection: Display unwanted ads or redirect to malicious websites.
- System Misuse: Use CPU for hidden cryptocurrency mining.
- Malware Delivery: Download and install additional harmful programs.

Conclusion:

Regularly reviewing and removing suspicious extensions improves security, protects personal data, and enhances browser performance.