Task 7 – Browser Extension Security Audit Report

1. Overview
This report documents the process of reviewing and securing the browser by identifying, analyzing, and removing suspicious or unnecessary browser extensions. The objective was to enhance browser security, reduce attack surfaces, and prevent potential data breaches caused by malicious browser add-ons.

2. Steps Taken
1. Opened the browser’s extension manager via the settings menu.
2. Reviewed all installed extensions by checking:
- Extension name and description.
- Permissions requested.
- Developer information.
- Installation date.
3. Cross-checked suspicious extensions by searching online for reviews and developer reputation.
4. Marked extensions as either *Safe*, *Suspicious*, or *Unused*.
5. Removed or disabled suspicious and unused extensions.
6. Restarted the browser to finalize changes and ensure no residual malicious code was running.

3. Extensions Removed

Extension Name	Reason for Removal	Permission Concern
Example Helper	Unknown developer and purpose	Read all site data
Old VPN	No longer in use	Full unrestricted web access

4. Risks of Malicious Browser Extensions
- Stealing login credentials and other sensitive data.
- Injecting ads or tracking scripts into web pages.
- Redirecting users to phishing or malicious sites.
- Mining cryptocurrency using system resources without consent.
- Logging keystrokes and capturing clipboard contents.

5. Conclusion
The audit identified and removed browser extensions that posed potential security and privacy risks. This proactive measure helps in preventing unauthorized access to sensitive data, improving browser performance, and reducing vulnerabilities that could be exploited by cyber attackers.