Task 7 Report: Identify and Remove Suspicious Browser Extensions

Objective:

The objective of this task is to learn how to identify potentially harmful browser extensions and remove them to ensure a secure browsing environment.

Steps Taken:

- Opened Microsoft Edge and navigated to the Extensions page (edge://extensions).
- Reviewed all installed extensions carefully.
- Checked permissions, origin, and description of each extension.
- Identified whether any extensions were suspicious or unnecessary.

Findings:

Only one extension was found installed on Microsoft Edge:

- Google Docs Offline – This extension enhances the offline experience with Google Docs and comes pre-installed on the device. It is safe, trusted, and published by Google.

No suspicious or malicious extensions were identified. Therefore, no extensions needed to be removed.

How Malicious Extensions Can Harm Users:

- Tracking browsing history and stealing sensitive data such as passwords or credit card details.
- Injecting ads or redirecting to malicious websites.
- Reducing browser performance and causing instability.
- Installing backdoors that allow attackers to gain unauthorized access to user systems.

Conclusion:

The review of installed browser extensions showed only one trusted extension (Google Docs Offline). No suspicious or harmful extensions were present, so no removals were required. Regularly auditing browser extensions is a good practice to maintain privacy, security, and overall system performance.