Identify and Remove Suspicious Browser Extensions

1. Introduction: The Importance of Browser Extension Security

The goal of this task was to gain a practical understanding of how to audit browser security by checking, identifying, and removing potentially harmful extensions. Browser extensions, while useful for added functionality, represent a significant attack surface that can compromise user privacy and data security if exploited by malicious actors.

2. Browser Extension Audit Methodology and Results

Tools Used: The security audit was performed on two web browsers: **Google Chrome** and **Microsoft Edge**.

Method: The audit followed a comprehensive eight-step guide to review all installed browser add-ons. This involved reviewing every installed item, checking their requested permissions, and searching for any unnecessary or suspicious entries. A system restart confirmed performance stability.

Extensions Reviewed:

- **Google Chrome:** Google Docs Offline.
- **Microsoft Edge:** Cat-in-Tab, Grammarly: AI Writing and Grammar Checker App, Netflix Party is now Teleparty, TwoSeven Extension, and Google Docs Offline.

Audit Conclusion: The audit confirmed that **no suspicious or malicious extensions were present** in either browser. Consequently, the steps for removal were not required, and all installed items were deemed necessary, legitimate, and sourced from official stores.

3. Research Findings: How Malicious Extensions Compromise Users

Research conducted as part of the task highlighted the various methods malicious extensions use to compromise security:

- **Data Theft and Credential Harvesting:** Extensions can exploit broad permissions to read and steal **sensitive information** (passwords and financial data) as it is typed or viewed.
- **Tracking and Surveillance:** They can secretly log the user's **entire browsing history** for user profiling and targeted attacks.
- **Browser Hijacking:** Malicious code can redirect search queries, inject **unwanted advertisements**, or change the user's default homepage.
- **Supply Chain Risk:** Even trusted, popular extensions can become a threat if sold to a bad actor who then pushes a **silent, malicious update** to existing users.

4. Conclusion

The objectives of the task were successfully met. A thorough audit of both Google Chrome and Microsoft Edge extensions was performed, and all installed add-ons were confirmed to be necessary and legitimate. The core deliverable—a list of suspicious extensions found and removed—is **zero**, confirming a baseline of good security posture in the browsers audited. Furthermore, the task provided crucial insights into the risks of malicious extensions, reinforcing the best practice of **only installing extensions from trusted sources** and **regularly auditing installed items** to maintain a minimal and secure attack surface.