Identify and Remove Suspicious Browser Extensions

1. Open your browser's extension/add-ons manager.

* Action Taken: Located and accessed the extensions/add-ons manager in the primary browser used for work/internship activities (e.g., Chrome, Firefox, Edge).

* Path Taken (Example): Browser Settings/Menu \right arrow More Tools \right arrow Extensions or Add-ons.

2. Review all installed extensions carefully.

* Action Taken: Made a complete list of every installed extension before any removals.

  * Total Extensions Found: [Insert Number]

  * Initial Review Status: *[Insert brief observation, e.g., "Most appear to be productivity tools and ad blockers."] *

3. Check permissions and reviews for each extension.

* Action Taken: Clicked on the "Details" or "Permissions" setting for each extension to see what data they access (e.g., "read and change all your data on the websites you visit"). Also checked the extension's listing page for user reviews, download count, and date of last update.

* Key Finding: Permissions are often the biggest security risk. An extension that doesn't need to read all your browsing data (like a simple spell checker) but asks for it is suspicious.

4. Identify any unused or suspicious extensions.

* Action Taken: Categorized extensions into one of three groups:

  * Trusted/Essential: Daily use, well-known developer (e.g., official password manager).

  * Unused/Redundant: Not used in the last 30 days, or a feature already provided by the browser.

  * Suspicious: Unknown developer, low number of reviews/downloads, outdated, or requesting excessive permissions.

5. Remove suspicious or unnecessary extensions.

* Action Taken: Uninstalled or disabled extensions identified in the previous step.

  * Extensions Removed/Disabled (Document these names):

    * [Extension Name 1] \right arrow Reason: [e.g., Unnecessary, Unknown developer]

    * [Extension Name 2] \right arrow Reason: [e.g., Excessive permissions]

    * [Extension Name 3] \right arrow Reason: [e.g., Adware detected previously]

  * Total Extensions Remaining: [Insert Number]

6. Restart browser and check for performance improvements.

* Action Taken: Closed all browser windows, restarted the computer/browser, and monitored performance.

* Observation: [State the result, e.g., "Browser start-up time was noticeably faster," or "A persistent background process is no longer running," or "No change observed."]

7. Research how malicious extensions can harm users.

* Action Taken: Conducted a brief search to understand common attack vectors.

* Summary of Harm (Simple Definitions):

  * Data Theft (Keylogging/Credential Harvesting): Extensions can capture every keystroke, including passwords and credit card numbers, and send them to an attacker.

  * Adware/Click Fraud: Injecting unwanted advertisements onto trusted websites or running hidden processes to automatically click on ads, generating revenue for the attacker at the cost of the user's performance and security.

  * Session Hijacking: Stealing session cookies to take control of a logged-in account (like banking or social media) without needing the password.

8. Document steps taken and extensions removed.

* Action Taken: This completed report serves as the final documentation.

Outcome: Awareness and Security Summary

The successful completion of this task has resulted in:

* A clean, optimized browser environment with reduced potential attack surfaces.

* Increased awareness of the importance of the Principle of Least Privilege when granting permissions to extensions (i.e., only grant what is absolutely necessary).

* A foundational understanding of how browser extensions can be weaponized in a cyber-attack.