Task 7: Identify and Remove Suspicious Browser Extensions

Objective: Learn to spot and remove potentially harmful browser extensions.
Tools: Any web browser (Chrome, Firefox)
Deliverables: List of suspicious extensions found and removed (if any)

Step-by-Step Detailed Guide:

- 1. Open your browser’s extension or add-ons manager: - In Chrome: Go to the menu (three dots) > More tools > Extensions. - In Firefox: Menu > Add-ons and Themes > Extensions. - This section shows all extensions currently installed on your browser.
- 2. Review all installed extensions carefully: - Check the name and purpose of each extension. - Remove any that you do not remember installing. - Look for duplicates or extensions with vague names.
- 3. Check permissions and reviews for each extension: - Some extensions request unnecessary permissions (like access to all websites, reading browsing history). - Open the extension’s details and check what data it collects. - Look up reviews on the Chrome Web Store or Mozilla Add-ons page.
- 4. Identify unused or suspicious extensions: - If you haven’t used an extension in a long time, consider it unnecessary. - Suspicious extensions may include: coupon pop-ups, search toolbars, or unknown brand add-ons.
- 5. Remove suspicious or unnecessary extensions: - Use the Remove/Trash icon next to the extension name. - Confirm removal. - Some may require restarting the browser to fully uninstall.
- 6. Restart browser and check for performance improvements: - After removal, restart the browser. - Notice if browsing speed, pop-up frequency, or search redirects improve.
- 7. Research how malicious extensions can harm users: - They may collect private data like passwords and browsing history. - Some redirect traffic to adware or malicious sites. - They can slow down your browser and increase CPU usage.
- 8. Document steps taken and extensions removed: - Keep a small report of extensions reviewed, removed, and reasons for removal. - This helps in case issues reappear later.

Outcome:

By completing this task, you gain awareness of browser security risks and learn practical skills to manage browser extensions. This ensures safer browsing, reduced risk of data theft, and better browser performance.

Example Detailed Report:

Browser: Google Chrome (Version 128.0) Extensions Installed Initially: 1. Grammarly - Trusted, widely used, and verified. 2. AdBlock Plus - Safe and enhances browsing by blocking ads. 3. QuickCouponsNow - Requested unnecessary permissions like accessing all sites, poor reviews, suspicious behavior. 4. SearchOptimizer Pro - Hijacked default search engine, displayed ads and popups. 5. Zoom Scheduler - Safe and required for meetings. Actions Taken: - Removed 'QuickCouponsNow' after verifying suspicious behavior. - Removed 'SearchOptimizer Pro' due to malicious activity reports. - Retained Grammarly, AdBlock Plus, and Zoom Scheduler as safe. Performance Check: - After removal, Chrome startup time reduced. - No more unwanted search redirects. - CPU usage during browsing lowered. Conclusion: Removing suspicious extensions improved security and performance. Awareness of permissions and reviews is crucial before installing any new extensions.