Identify and Remove Suspicious Browser Extensions

Objective

Learn how to identify, evaluate, and remove suspicious or unnecessary browser extensions to improve browser security and performance.

Tools Used

- Google Chrome (can be replaced with Firefox or other browsers)
- Internet (for research on extensions)

Steps Performed

1. Opened the Extensions Manager
   - Chrome: chrome://extensions/
   - Firefox: about:addons

Text

2. Reviewed Installed Extensions
   - Checked usage and purpose of each extension.

3. Checked Permissions & Reviews
   - Looked into permissions, developer, and online ratings.

4. Identified Suspicious or Unused Extensions
   - Criteria: excessive permissions, poor reviews, unknown source.

5. Extensions Identified for Removal
   - XYZ Ad Blocker Clone: Unofficial version, suspicious permissions
   - PDF Converter Free: Unused, high data access permissions
   - Shopping Deals Tracker: Injects ads, poor user reviews

6. Removed Extensions
   - Removed using browser UI, restarted browser.

7. Post-Removal Check

- Improved performance, fewer pop-ups.

8. Research on Threats

- Risks: data theft, ad injection, spyware, cryptomining

Outcome

- Increased awareness of malicious browser extensions.
- Improved browser performance and privacy.
- Developed a regular extension audit habit.

Tips for Extension Security

- Install only from trusted developers.
- Avoid extensions requesting broad access.
- Regularly audit your extensions.
- Keep browser and extensions updated.