Identify and Remove Suspicious Browser Extensions

Steps to Follow

1. Open Extension Manager

   - Chrome: chrome://extensions/

   - Firefox: about:addons

   - Edge: edge://extensions/

   - Brave: brave://extensions/

2. Review Installed Extensions: Go through each extension listed.

3. Check Permissions and Reviews: Click on 'Details' or 'More Info' for each extension.

4. Identify Unused or Suspicious Extensions: Look for unknown developers, generic names, etc.

5. Remove Unnecessary or Malicious Extensions: Click Remove or Trash Bin icon.

6. Restart Browser: Check for improvements after restarting the browser.

7. Understand the Risks: Extensions can track data, inject ads, steal credentials, etc.

8. Document Your Process:

Example Documentation

Extension Name	Status	Reason Removed
Zoom Scheduler	Kept	Trusted & used regularly
Easy PDF Converter	Removed	Unused, high permissions, no info
Web Shield Pro	Removed	Suspicious behavior, low rating

Best Practices

- Install only from trusted developers.

- Regularly audit extensions.

- Use browser in incognito/private mode to test without extensions.