

Task 7: Identify and Remove Suspicious Browser Extensions

Objective

Learn to spot and remove potentially harmful browser extensions.

Browser Used: Google Chrome

Steps Taken

1. Opened Google Chrome and navigated to the Extensions Manager:
 - Clicked the three-dot menu > More tools > Extensions.
2. Reviewed all installed extensions carefully to identify any unknown or unnecessary ones.
3. Checked the permissions and user reviews for each extension by clicking Details.
4. Found an extension named "Auto Skipp for YouTube Ads" that:
 - Requested excessive permissions like "Read and change all your data on all websites."
 - Had negative user reviews mentioning suspicious activity.
5. Marked "Auto Skipp for YouTube Ads" as suspicious.
6. Removed the extension by clicking Remove in the Extensions Manager.
7. Restarted the browser and verified improved performance.
8. Researched and confirmed that malicious browser extensions can:
 - Steal sensitive information (like login credentials).
 - Track browsing activity and inject unwanted ads.

Deliverables

- Suspicious Extension Found: Auto Skipp for YouTube Ads
- Action Taken: Removed
- Reason: Unsafe permissions and bad reviews indicating potential security risks.
- Browser Restarted: Yes

Notes

Regularly reviewing browser extensions is essential to maintaining a secure browsing experience. Avoid installing extensions from unknown or untrusted sources.