Task 7: Identify and Remove Suspicious Browser Extensions

Objective: Learn to spot and remove potentially harmful browser extensions.

Steps Taken:

1. Opened Google Chrome.
2. Accessed Extensions page via chrome://extensions.
3. Reviewed all installed extensions, checking permissions and user reviews.
4. Identified suspicious extensions based on excessive permissions and poor reviews.
5. Removed 'PDF Converter Pro' and 'Video Downloader X' extensions.
6. Restarted the browser to apply changes.

Installed Extensions (Before Removal):

Extension Name	Permissions	Status
Grammarly	Read and change text on visited sites	Safe
uBlock Origin	Block ads and trackers	Safe
PDF Converter Pro	Read and change all your data on all websites	Suspicious
Video Downloader X	Access browser history, manage downloads	Suspicious
Google Docs Offline	Access Google Drive files offline	Safe

Installed Extensions (After Removal):

Extension Name	Permissions	Status
Grammarly	Read and change text on visited sites	Safe
uBlock Origin	Block ads and trackers	Safe
Google Docs Offline	Access Google Drive files offline	Safe

Detailed Reasoning and Observations:

- 'PDF Converter Pro' requested full access to all website data, which is unnecessary for its function. Many reviews flagged it as malware.
- 'Video Downloader X' asked for access to browser history and downloads management — common traits of malicious extensions.
- Safe extensions like 'Grammarly' and 'uBlock Origin' have transparent permissions and good reviews.

Interview Preparation Questions & Answers:

Q: How can browser extensions pose security risks?
A: They can read/modify data on visited sites, track browsing activity, and inject malicious scripts.

Q: What permissions should raise suspicion?
A: Full access to all websites, managing downloads, reading browser history.

Q: How to safely install browser extensions?
A: Only from trusted sources, check reviews, verify developer, and review permissions before installing.

Q: What is extension sandboxing?
A: A security model that isolates extensions from the core browser to limit damage if compromised.

Q: Can extensions steal passwords?
A: Yes, if given permissions to read form data or access all websites.

Q: How to update extensions securely?
A: Enable automatic updates via the Chrome Web Store and only update from official sources.

Q: Difference between extensions and plugins?
A: Extensions modify browser behavior, plugins handle specific content types like Flash or Java.

Q: How to report malicious extensions?
A: Through the Chrome Web Store's 'Report abuse' option or Google's security reporting page.