Task 7: Identify and Remove Suspicious Browser Extensions
Cyber Security Internship – Practical Report
Date: 24/11/2025

Objective:
Check installed browser extensions, find potentially harmful ones, and remove them.

Browser:
Google Chrome Version 119.x

Steps:
1. Open Chrome browser.
2. Clicked on Menu (⋮) → More Tools → Extensions.
3. Reviewed each extension one by one.
4. Checked requested permissions:
   - Access to browsing activity
   - Read and change data on all websites
   - Show notifications / popups
5. Checked Web Store reviews and publisher credibility.
6. Identified risky and unnecessary extensions.
7. Removed suspicious extensions from the browser.
8. Restarted browser and confirmed clean status.

Extensions Removed:
1️⃣Wallpaper HD
- Permission: Read browsing history
- Problem: Unknown developer, adds trackers
- Solution: Removed

2️⃣Free Shopping Helper
- Permission: Change data on visited sites
- Problem: Injects ads
- Solution: Removed

Security Learnings:
- Malicious extensions can steal data or display unwanted ads.
- Always check permissions before installing.
- Prefer trusted, popular extensions only.
- Remove unused extensions regularly.
- Browser extensions can bypass antivirus easily.

Advantages after cleanup:
✔ Faster browsing
✔ No pop-ups
✔ Better privacy and tracking protection

Conclusion:
This task helped me understand browser extension security risks.

I successfully removed suspicious extensions and improved security.