**TASK-7**

**1. Open Chrome’s Extension Manager**

* Navigate to chrome://extensions/ in the address bar.
* This opens the list of all installed extensions.

**2. Review All Installed Extensions**

Let’s say the following extensions are installed: | Extension Name | Description | Installed By | |----------------------|------------------------------------|--------------| | Grammarly | Writing assistant | User | | Adblock Plus | Blocks ads | User | | PDF Converter Pro | Converts files to PDF | Unknown | | Weather Forecast | Shows weather updates | User |

**3. Check Permissions & Reviews**

* **Grammarly**: Requests access to all websites. Verified developer. Excellent reviews.
* **Adblock Plus**: Minimal permissions. Trusted by millions.
* **PDF Converter Pro**: Requests access to browsing history, clipboard, and downloads. Poor reviews. Developer unknown.
* **Weather Forecast**: Requests location access. Mixed reviews.

**4. Identify Suspicious or Unused Extensions**

* **PDF Converter Pro** stands out:
  + Excessive permissions
  + Poor reviews
  + Unknown developer
  + Not used recently

**5. Remove Suspicious or Unnecessary Extensions**

* Click **“Remove”** next to *PDF Converter Pro*.
* Confirm removal.

**6. Restart Browser**

* Close all Chrome windows.
* Reopen Chrome.
* Observe:
  + Faster startup
  + Fewer pop-ups
  + No unexpected redirects

**7. Research: How Malicious Extensions Harm Users**

* Log keystrokes and steal credentials
* Redirect traffic to phishing sites
* Inject ads or trackers
* Access sensitive data like clipboard contents

**8. Document Actions Taken**

| **Date** | **Action Taken** | **Extension Name** | **Reason for Removal** |
| --- | --- | --- | --- |
| 14-Aug-2025 | Reviewed permissions and reviews | PDF Converter Pro | Excessive permissions, poor reputation |
| 14-Aug-2025 | Removed extension | PDF Converter Pro | Potential security risk |
| 14-Aug-2025 | Restarted browser | — | Performance check |

**Interview questions:**

**1.How Can Browser Extensions Pose Security Risks?**

Extensions run with elevated privileges and can:

* Access sensitive data like browsing history, clipboard, or cookies
* Inject malicious scripts into web pages
* Redirect traffic to phishing sites
* Track user behavior or sell data to third parties
* Exploit vulnerabilities in the browser or OS

**2.What Permissions Should Raise Suspicion?**

Be cautious of extensions requesting:

* **Access to all websites** (Read and change all your data on the websites you visit)
* **Clipboard access**
* **Download management**
* **Keystroke logging**
* **Access to cookies or passwords**
* **Remote code execution** or background script injection

**3**.**How to Safely Install Browser Extensions?**

* Use official browser stores (Chrome Web Store, Firefox Add-ons)
* Check developer reputation and extension history
* Read user reviews and ratings
* Verify update frequency and changelog
* Avoid extensions with vague descriptions or excessive permissions

**4**.**What Is Extension Sandboxing?**

Sandboxing isolates the extension’s code from the rest of the browser and system:

* Prevents direct access to system files
* Limits interaction with other extensions
* Reduces risk of privilege escalation

**5.Can Extensions Steal Passwords?**

Yes, if granted access to:

* Web page content (can read login forms)
* Clipboard (can capture copied passwords)
* Cookies or session tokens

**6.How to Update Extensions Securely?**

* Enable **automatic updates** in browser settings
* Manually check for updates via the extension manager
* Review changelogs for permission changes
* Avoid sideloading updates from unofficial sources

**7.Difference Between Extensions and Plugins**

| **Feature** | **Extensions** | **Plugins** |
| --- | --- | --- |
| Purpose | Enhance browser functionality | Enable specific content (e.g., Flash) |
| Installation | Through browser store | Often external installers |
| Security Model | Sandboxed, permission-based | Historically more vulnerable |
| Examples | Adblock, Grammarly | Flash Player, Java Plugin |

**8.How to Report Malicious Extensions?**

* **Chrome**: Go to the extension’s page → Click “Report abuse”
* **Firefox**: Visit the add-on page → Scroll down → Click “Report this add-on”
* Include:
  + Description of suspicious behavior
  + Screenshots or logs if available
  + URLs affected or redirected