**Browser Extension Audit & Removal Report**

**Task:** Task 7 – Identify and Remove Suspicious Browser Extensions  
**Submitted By:** Aryanshu Saha  
**Date:** 3/07/2025  
**Browser Used:** Google Chrome (Also applicable to Mozilla Firefox)  
**Deliverable:** List of suspicious extensions found and removed with supporting observations

**Objective**

To identify, review, and remove potentially harmful or unnecessary browser extensions by evaluating installed add-ons for suspicious behavior, excessive permissions, or performance impact.

**Tools & Environment**

* **Google Chrome** v[version]
* **Windows/Linux Host** with user privileges
* **Online resources** used for extension reputation checks:
  + Chrome Web Store reviews
  + [CRXcavator.io](https://crxcavator.io/)
  + [VirusTotal.com](https://www.virustotal.com/)

**Steps Performed**

**Step 1: Open Extension Manager**

* Accessed via:  
  chrome: //extensions/ (Chrome)  
  about: addons (Firefox)

**Step 2: Reviewed All Installed Extensions**

* Checked each for:
  + Permissions requested
  + User reviews and ratings
  + Update frequency and publisher identity
  + System behavior/performance impact

**Step 3: Identified Suspicious or Unused Extensions**

Criteria used:

* Excessive permissions (e.g., read all data on all websites)
* Unknown developers or no listed website
* Negative user reviews or reported malware
* No recent updates (abandoned)

**Step 4: Extensions Removed**

| **Extension Name** | **Reason for Removal** | **Notes** |
| --- | --- | --- |
| **PDF Converter Pro** | Unknown publisher, requested access to all website data, poor reviews | Flagged on CRXcavator and VirusTotal |
| **Weather Widget** | Unused, excessive permissions (location and web data access) | Removed as precaution |
| **Dark Mode Ultimate** | Caused browser slowdown, unknown source | Performance improved after removal |

**Step 5: Restarted Browser**

* After removal, Chrome was restarted.
* Observed improved tab switching and startup speed.

**Understanding the Risks of Malicious Extensions**

| **Threat Vector** | **Impact** |
| --- | --- |
| **Ad Injection** | Displays unwanted or malicious ads on websites |
| **Data Harvesting** | Steals browsing history, cookies, login info |
| **Keylogging** | Records keystrokes including passwords |
| **Phishing Redirects** | Replaces legitimate search results or links |
| **Cryptojacking** | Uses system resources to mine cryptocurrency |

**Examples:**

* In 2020, malicious Chrome extensions affected over 3 million users by stealing data and redirecting traffic.
* Some fake productivity tools were discovered logging keystrokes and injecting malicious JavaScript into web sessions.

**Summary**

A full browser audit was conducted to evaluate extension safety and necessity. Three extensions were removed due to poor reputation, unnecessary access, or lack of usage. This task provided insight into how extensions can be used as attack vectors and the importance of regular browser hygiene.