**Report: Identifying and Removing Suspicious Browser Extensions**

**By : Rohita B**

# Objective

The objective of this task was to identify, evaluate, and remove potentially harmful browser extensions to improve privacy, security, and overall browser performance. This hands-on activity also aimed to increase awareness about the risks associated with malicious or excessive permissions granted to browser extensions.

Table of Content

* Tools Used
* Methodology
* Findings
* Results
* Risks of Malicious Browser Extensions
* Recommendations
* Conclusion

# 1. Tools Used

* **Web Browser:** Google Chrome
* **Operating System:** Windows 11 (64-bit)
* **Additional Tools:** Chrome Web Store (for extension details and reviews), Google Search (for reputation checks)

**2. Methodology**

The following steps were taken to complete the task:

**Step 1: Access the Extension Manager**

 Navigated to chrome://extensions/ to view all installed browser extensions.

# Step 2: Extension Review

Each installed extension was evaluated based on:

* Publisher and source
* Description and function
* Permissions requested
* Number of downloads and user reviews
* Date of installation and usage frequency

# Step 3: Risk Assessment

Extensions were flagged as suspicious if they:

* Came from unknown or unverified publishers
* Requested overly broad or unnecessary permissions (e.g., "Read all data on all websites")
* Displayed signs of suspicious behavior (pop-ups, redirects, etc.)
* Had poor reviews or low user ratings

# Step 4: Action Taken

Suspicious or unused extensions were removed. The browser was restarted afterward to ensure the changes took effect.

**3. Findings List of Installed Extensions (Before Cleanup)**

# Extension

# Name

**Publisher Purpose Permissions Suspicious Notes**

Writing Read/write on Trusted and

Grammarly grammarly.com No

assistant websites frequently used.

Open source and

uBlock Read browsing

Raymond Hill Ad blocker No widely

Origin data

recommended.

PDF Converts

Read all site High permissions,

Converter Unknown documents to **Yes**

data unknown publisher.

Pro PDF

Unverified

Weather Weather Location, tabs,

Unknown **Yes** publisher and

Live updates notifications

broad access.

Google Docs Access to Storage and Official Google

Google LLC No Offline Docs offline network state extension.

# Suspicious Extensions Removed 1. PDF Converter Pro

* Issue: Requested access to all site data; not actively used; unknown developer.
* Action: Removed.

# 2. Weather Live

* Issue: Requested location, tabs, and notifications; publisher not verified; potential for adware.
* Action: Removed.

# 4. Results

* **Before Cleanup:** 5 active extensions
* **Removed:** 2 suspicious extensions
* **After Cleanup:** 3 trusted and regularly used extensions **Post-removal Observations:**
* Improved browser performance (faster tab switching and startup time)
* Fewer intrusive pop-up ads
* Increased confidence in browser safety

# 5. Risks of Malicious Browser Extensions

Malicious or overly-permissive browser extensions can:

* **Track browsing behavior** and sell data to third parties
* **Inject malicious ads** or redirect search results
* **Capture sensitive data** such as login credentials and keystrokes
* **Modify browser settings** and hijack homepage/search engine

**Common signs** of malicious extensions include:

* Sudden appearance of ads or pop-ups
* Changes to browser homepage or default search engine
* Unexplained slowdowns or crashes

# 6. Recommendations

* Regularly review installed extensions.
* Only install extensions from **verified sources** (e.g., Chrome Web Store with strong reviews).
* Check **permissions** carefully before installation.
* Remove unused extensions to minimize attack surface.
* Use **browser-based antivirus or extension safety scanners** if available.

# 7. Conclusion

This task highlighted the importance of vigilance when using browser extensions. While they add valuable features, extensions with excessive permissions or unknown origins pose a significant security risk. Removing such extensions helped improve browser safety, performance, and privacy.