Report: Identifying and Removing Suspicious Browser Extensions

By: Aabhas Vishwakarma

Objective

The purpose of this project was to spot, assess, and uninstall browser add-ons that could pose privacy or security risks, while also improving overall browser speed and efficiency. This hands-on work focused on raising awareness of the dangers posed by malicious or overly intrusive browser add-ons.

Table of Contents

---

1. Tools and Environment

- **Web Browser:** Google Chrome
- **Operating System:** Windows 11 (64-bit)
- **Additional Resources:** Chrome Web Store (for add-on details and ratings), Google Search (for background checks)

---

2. Procedure

Step 1 – Open the Extensions Manager

- Accessed chrome://extensions/ to view all currently installed add-ons.

Step 2 – Review Installed Add-ons

Each add-on was evaluated by checking:

- Source and publisher
- Functionality description
- Permissions requested

- Download count and reviews
- Installation date and frequency of use

Step 3 – Risk Analysis
An add-on was marked as suspicious if it:

- Originated from an unverified or unknown publisher
- Requested excessive or unrelated permissions (e.g., "Read all data on all websites")
- Showed unusual behavior like pop-ups or redirects
- Had low ratings or negative reviews

Step 4 – Removal Actions
Potentially harmful or unused add-ons were uninstalled. Browser was restarted to apply the changes.

---

3. Key Observations

Installed Add-ons (Before Cleanup):

Extension Name	Publisher	Purpose	Permissions	Suspicious?	Notes
GrammAssist	grammassist.com	Writing enhancement	Read/write on websites	No	Well-known and frequently used
AdShield Pro	Raymond Hill	Ad blocker	Read browsing data	No	Open-source and widely trusted
PDF QuickConvert	Unknown	File to PDF converter	Read all site data	Yes	High permissions, unclear developer identity
SkyWeather Now	Unknown	Live weather updates	Location, tabs, notifications	Yes	Unverified publisher, broad access rights
Docs Offline Plus	Google LLC	Offline Google Docs	Storage, network state	No	Official Google extension

---

Suspicious Add-ons Removed:

1. **PDF QuickConvert**
    - **Issue:** Required full access to all websites; rarely used; unknown developer.
    - **Action:** Removed.
2. **SkyWeather Now**

    - **Issue:** Asked for location, tab access, and notifications; unverified publisher; possible adware risk.
    - **Action:** Removed.

---

4. Outcomes

- **Before Cleanup:** 5 active add-ons
- **Removed:** 2 suspicious add-ons
- **After Cleanup:** 3 trusted and regularly used add-ons

Post-removal benefits:

- Noticeably faster browser startup and tab switching
- Reduced pop-up ads and intrusive notifications
- Greater sense of browsing safety

---

5. Threats from Malicious Add-ons

Harmful or overly privileged add-ons can:

- Track and sell user browsing history
- Inject unwanted ads or manipulate search results
- Capture sensitive data like passwords and keystrokes
- Alter browser settings or hijack the default search engine

Warning signs include:

- Sudden appearance of pop-ups or extra ads
- Changes to homepage or search engine
- Browser slowdowns or unexplained crashes

---

6. Best Practices

- Review all installed add-ons regularly
- Install only from verified publishers with strong reviews
- Inspect requested permissions before installation
- Remove extensions that are unused or unnecessary
- Use browser-based antivirus or add-on scanners where possible

---

7. Final Remarks

This exercise reinforced the need for constant monitoring of browser add-ons. While extensions improve productivity and add useful features, those from untrusted sources or with excessive permissions can be a major security risk. Removing such add-ons helped make the browser faster, safer, and more private.