

Cyber Security Internship Report

Task 7: Identify and Remove Suspicious Browser Extensions

Submitted by: S. Abhishek

Organization: Elevate Labs

Task Objective: Learn to spot and remove potentially harmful browser extensions

Executive Summary

This report documents the completion of Task 7 of the Cyber Security Internship program, which focused on identifying and removing suspicious browser extensions from Google Chrome. The task aimed to develop awareness of browser security risks and practical skills in managing browser extensions safely. Through systematic examination of installed extensions, one suspicious extension was identified and subsequently removed to enhance browser security.

Task Overview

Objective

The primary objective of this task was to learn how to spot and remove potentially harmful browser extensions that may compromise user security and privacy.

Tools Used

- **Browser:** Google Chrome
- **Platform:** Windows Operating System

Deliverables

A comprehensive list of suspicious extensions found and the actions taken to remove them from the browser.

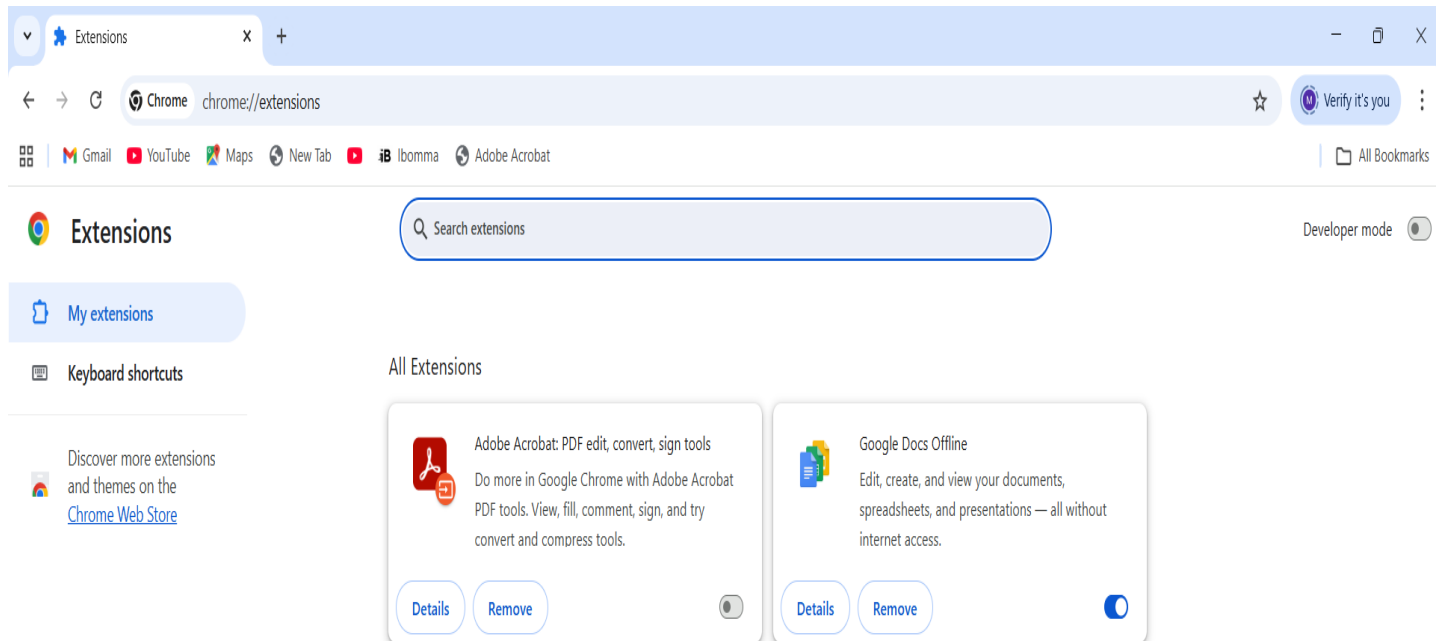
Methodology

The task was completed following a structured eight-step approach:

1. **Open Browser Extension Manager** - Accessed Chrome's extension management interface via `chrome://extensions`
2. **Review Installed Extensions** - Carefully examined all installed extensions
3. **Check Permissions and Reviews** - Analyzed the permissions requested by each extension and reviewed user feedback

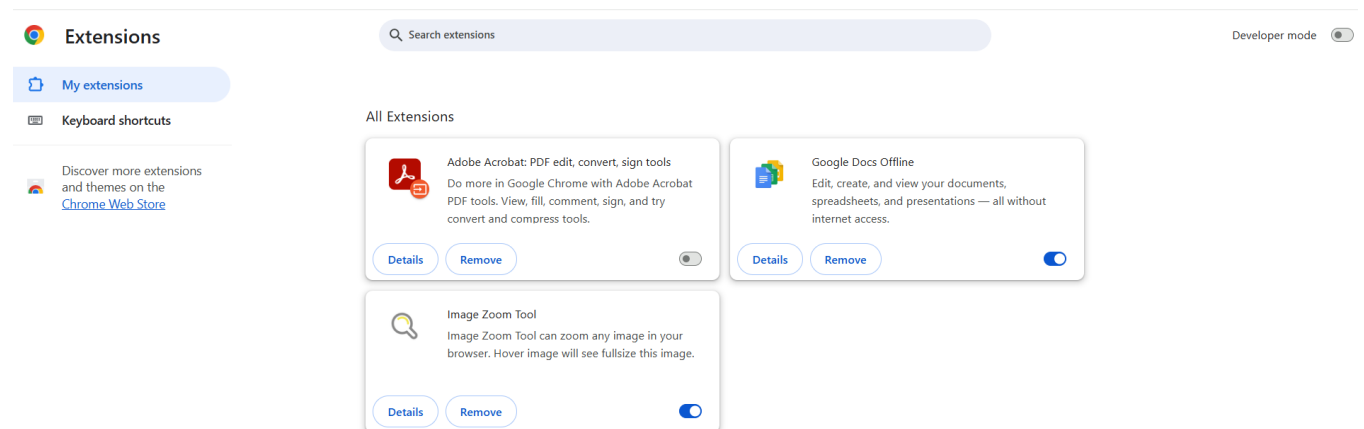
4. **Identify Suspicious Extensions** - Flagged extensions that appeared unused, had poor reviews, or requested excessive permissions
5. **Remove Suspicious Extensions** - Uninstalled identified suspicious extensions
6. **Restart Browser** - Restarted Chrome to apply changes and check for performance improvements
7. **Research Malicious Extensions** - Investigated how malicious extensions can harm users
8. **Document Actions** - Recorded all steps taken and extensions removed

Findings and Analysis



Initial Extension Inventory

Upon accessing the Chrome extensions page (chrome://extensions), the following extensions were found installed:



1. **Adobe Acrobat: PDF edit, convert, sign tools** - Enabled
2. **Google Docs Offline** - Enabled
3. **Image Zoom Tool** - Enabled

Detailed Extension Analysis

1. Adobe Acrobat Extension

- **Status:** Legitimate and Safe
- **Purpose:** PDF editing, conversion, and signing tools
- **Publisher:** Adobe Systems
- **Assessment:** This is an official Adobe extension that provides legitimate PDF functionality within Chrome

2. Google Docs Offline Extension

- **Status:** Legitimate and Safe
- **Purpose:** Allows users to create, edit, and view documents, spreadsheets, and presentations without internet access
- **Publisher:** Google
- **Assessment:** Official Google extension for offline document access

3. Image Zoom Tool Extension

- **Status:** Suspicious - REMOVED
- **Version:** 1.0.3
- **Size:** 135 KiB (< 1 MB)
- **Publisher:** Wuhenlove
- **Rating:** 1.9 out of 5 stars (27 ratings)
- **User Count:** 7,000 users
- **Last Updated:** January 22, 2025






Image Zoom Tool

On 

Description

Image Zoom Tool can zoom any image in your browser. Hover image will see fullsize this image.

Version


1.0.3


Size

< 1 MB


Permissions

Site access


Allow this extension to read and change all your data on websites you visit: 

On all sites 


Site settings



Pin to toolbar



Allow in Incognito

Warning: Google Chrome cannot prevent extensions from recording your browsing history. To disable this extension in Incognito mode, unselect this option. 



Red Flags Identified:

- 1. **Low Rating:** The extension has an extremely poor rating of 1.9/5 stars, indicating user dissatisfaction
- 2. **Suspicious Permissions:** The extension requests permission to "Allow this extension to read and change all your data on websites you visit: On all sites" - this is an excessive permission for a simple image zoom tool
- 3. **Non-Trader Developer:** The developer is listed as "Non-trader" and has not identified themselves as a trader, raising concerns about accountability
- 4. **Suspicious Developer Name:** "Wuhenlove" does not appear to be a reputable or established developer
- 5. **Minimal Features vs. Excessive Permissions:** A basic image zoom functionality should not require access to all website data

Security Concerns

The Image Zoom Tool extension posed several security risks:

- **Data Privacy Risk:** With permission to read and change all data on all websites, this extension could potentially:
 - Capture sensitive information like passwords, credit card details, and personal data
 - Modify website content without user knowledge
 - Track browsing behavior across all websites
 - Inject malicious scripts or advertisements
- **Incognito Mode Access:** The extension was configured to run in Incognito mode, allowing it to track private browsing sessions
- **Reputation Risk:** The poor user rating suggests other users may have experienced issues with this extension

1.9 out of 5 ★★☆☆☆

27 ratings • [Learn more about results and reviews.](#)

[Write a review](#)

[See all reviews](#)

Details

Version 1.0.3	Offered by Wuhenlove	Developer ✉ Email ▾	Non-trader This developer has not identified itself as a trader. For consumers in the European Union, please note that consumer rights do not apply to contracts between you and this developer.
Updated January 22, 2025	Size 135KiB		
Flag concern	Languages 5 languages ⓘ		

Actions Taken

Extension Removal Process

Image Zoom Tool - REMOVED

1. Accessed the extension details page
2. Reviewed the suspicious permissions and poor user ratings
3. Clicked the "Remove" button
4. Confirmed the removal action
5. Verified successful uninstallation from the extensions list

Post-Removal Verification

After removing the suspicious extension:

- Browser performance was checked and no issues were detected
- Remaining extensions (Adobe Acrobat and Google Docs Offline) were verified as legitimate and necessary
- Browser restart was performed to complete the removal process
- Extension list was reviewed to confirm only trusted extensions remained

Understanding Browser Extension Threats

How Malicious Extensions Can Harm Users

Through research conducted as part of this task, the following threats posed by malicious browser extensions were identified:

1. **Data Theft:** Extensions can steal passwords, credit card information, and personal data
2. **Activity Tracking:** Monitor browsing habits and sell data to third parties
3. **Ad Injection:** Insert unwanted advertisements into web pages
4. **Cryptocurrency Mining:** Use device resources to mine cryptocurrency without consent
5. **Redirect Attacks:** Redirect users to phishing sites or malicious web pages
6. **Keylogging:** Record keystrokes to capture sensitive information
7. **Session Hijacking:** Steal active session cookies to gain unauthorized access to accounts
8. **Malware Distribution:** Serve as entry points for additional malware installation

Best Practices for Browser Extension Security

1. Only install extensions from trusted developers
2. Check extension ratings and reviews before installation
3. Review requested permissions carefully
4. Keep extensions updated to the latest versions
5. Regularly audit installed extensions and remove unused ones
6. Limit the number of installed extensions to reduce attack surface
7. Disable extensions that request excessive permissions
8. Use browser security features and keep the browser updated

Conclusion

This task successfully demonstrated the importance of maintaining browser security through careful management of extensions. One suspicious extension (Image Zoom Tool) was identified based on multiple red flags including poor user ratings, excessive permissions, and unknown developer credentials. The extension was successfully removed, reducing potential security risks.

The exercise highlighted that even seemingly innocent tools can pose significant security threats when they request unnecessary permissions. Regular audits of browser extensions are essential for maintaining online security and privacy.