Task 7: Identification and Removal of Suspicious Browser Extensions

---

Objective

To identify, analyze, and remove potentially harmful or unnecessary browser extensions from a web browser in order to enhance system security, safeguard user privacy, and improve browser performance.

Tools & Environment

- Web Browser: Google Chrome (v125+)
- Operating System: Windows 10 (64-bit)
- Extensions Evaluated:
  - Adobe Acrobat: PDF edit, convert, sign tools
  - Google Docs Offline
  - McAfee® WebAdvisor

Execution Steps

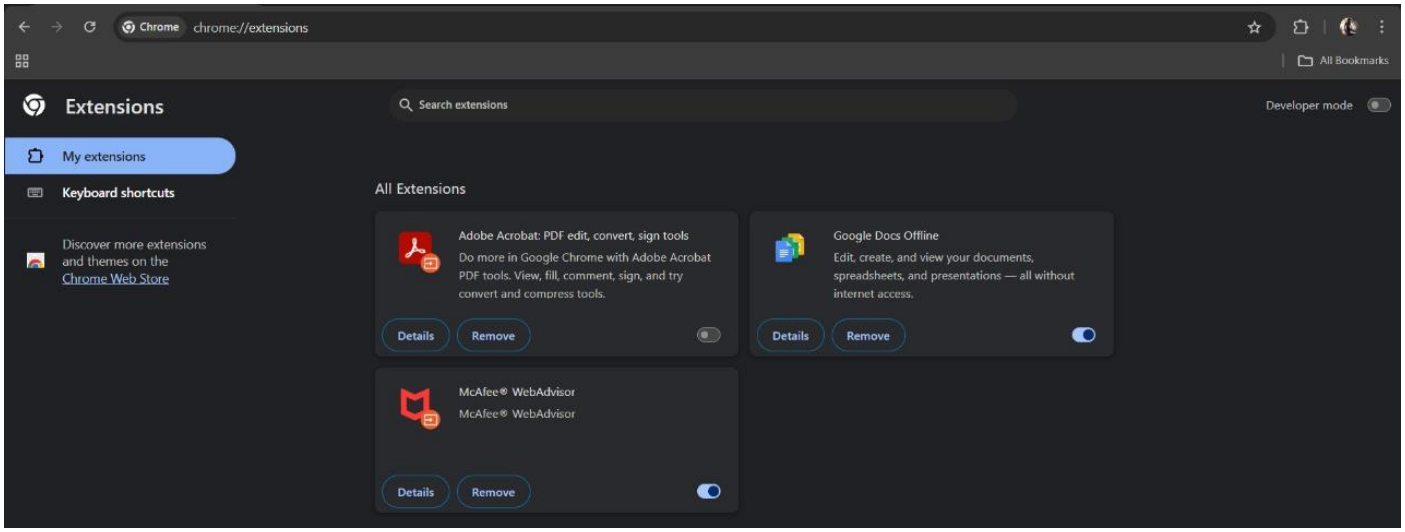
Step 1: Accessing the Browser's Extension Manager

The browser's extensions manager was accessed using the Chrome internal URL:

chrome://extensions/

This interface displays all currently installed browser extensions along with their respective configuration and control options.

Screenshot 1: Installed Extensions Overview



Step 2: Extension Inspection and Permissions Review

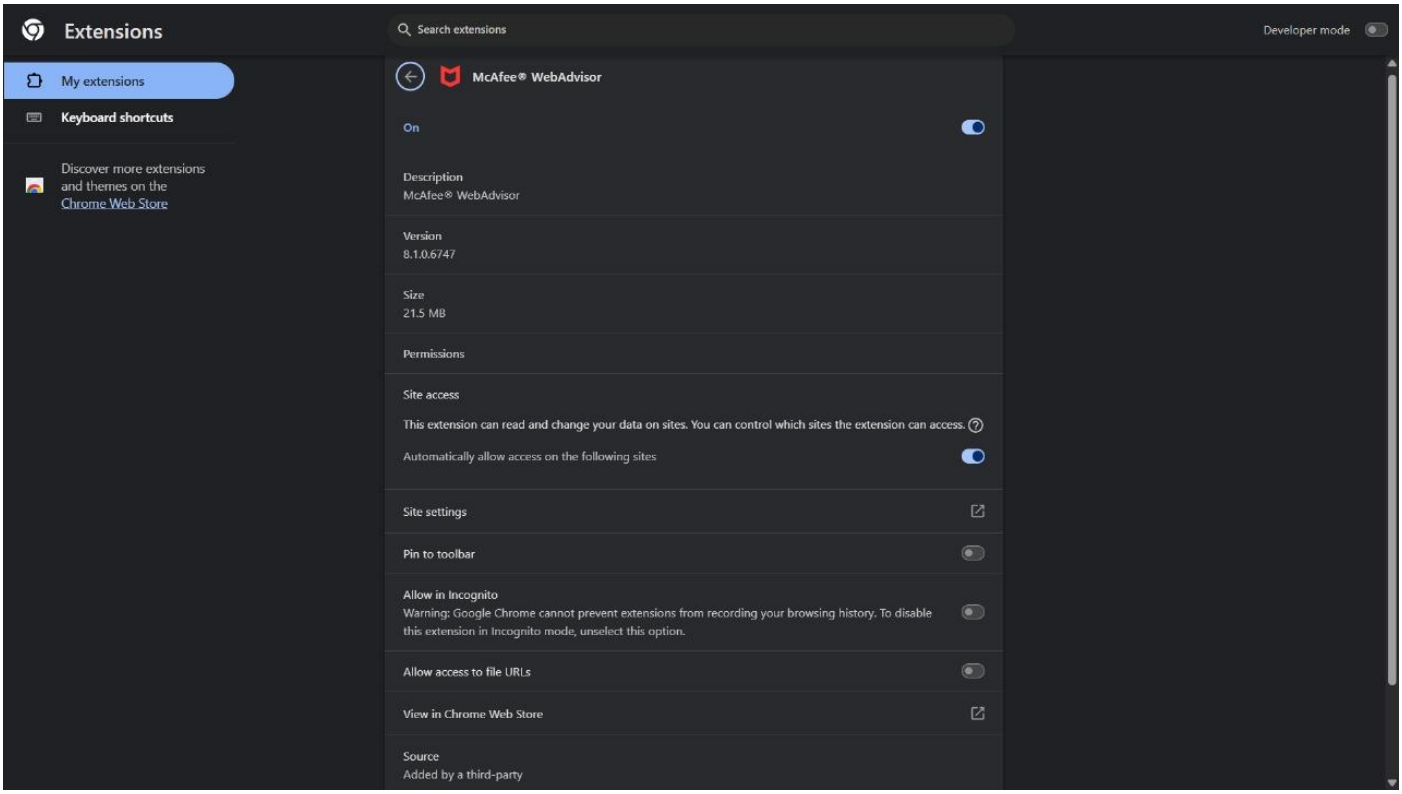
Each installed extension was individually reviewed using the "Details" option. Important aspects like:

- Extension size
- Permissions requested
- Site access capabilities
- Incognito behavior
- Source (whether added by the user or a third party)

were critically analyzed.

Example: The McAfee WebAdvisor extension was found to request permission to read and change all website data.

Screenshot 2: Extension Permissions and Metadata Review



Step 3: Web Store Review and Credibility Check

To assess the trustworthiness of the installed extensions, the Chrome Web Store listings were cross-referenced for each one. This included:

- User reviews
- Developer credibility
- Number of installs
- Last updated date
- Extension category (e.g., productivity, utility, security)

This step helps in identifying abandoned, poorly-rated, or impersonated plugins.

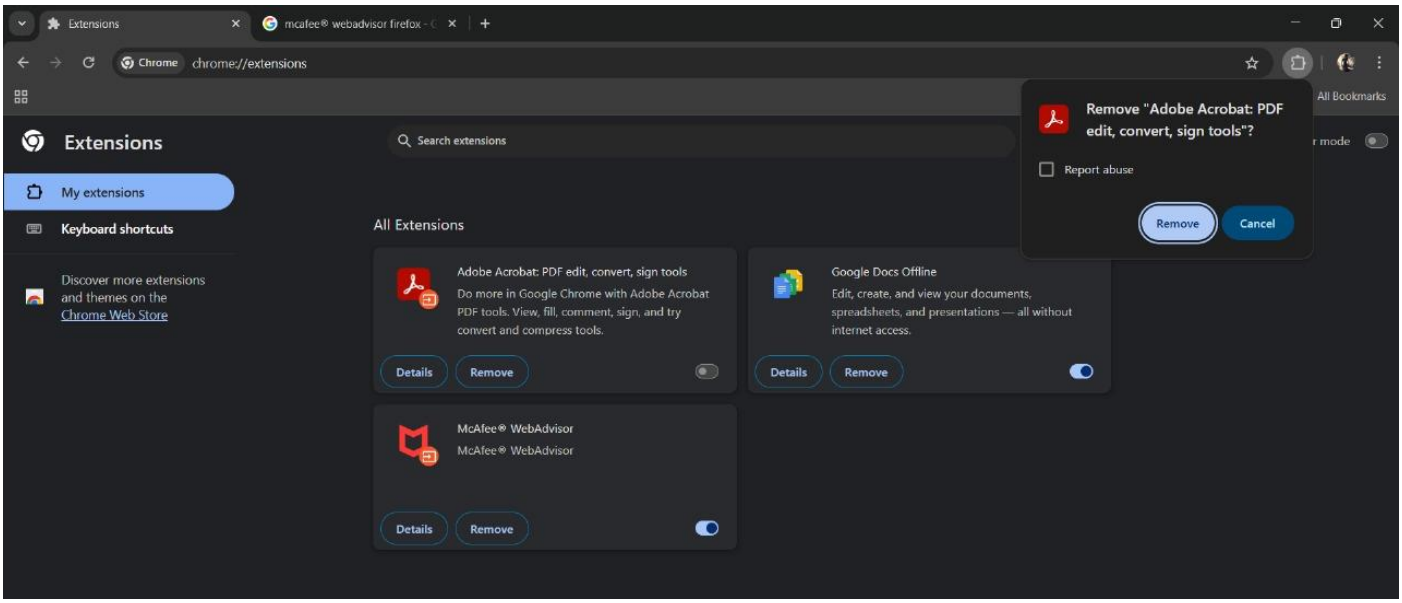
Step 4: Identification of Potentially Unwanted or Suspicious Extensions

During the assessment, the Adobe Acrobat extension was found to be unnecessary based on usage patterns. Although not malicious, unused extensions increase the browser's attack surface and potentially introduce vulnerabilities.

Step 5: Extension Removal

Using the “Remove” option, Adobe Acrobat was uninstalled from the browser. This action eliminates potential risk and improves browser startup performance.

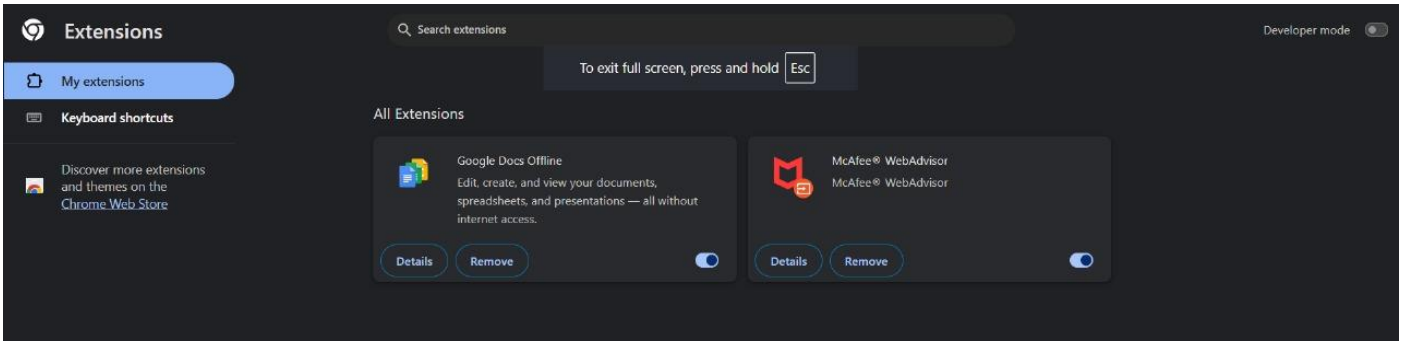
Screenshot 3: Extension Removal Prompt



Step 6: Post-Cleanup Verification and Performance Check

The browser was restarted and the extensions manager was reloaded to ensure the removal was successful. The extension list now reflected only necessary and secure plugins.

Screenshot 4: Verified Clean Extension List

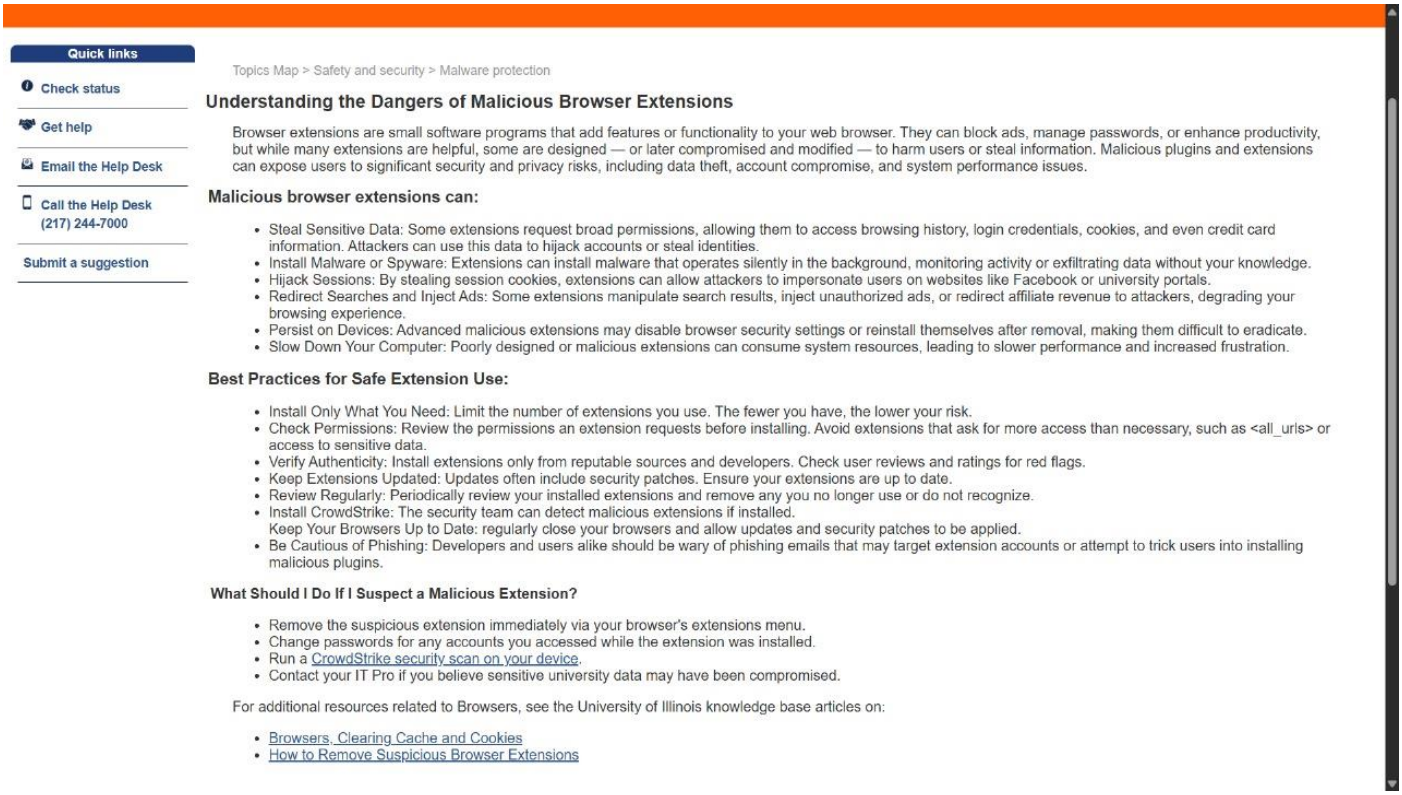


Step 7: Research – How Malicious Extensions Impact Security

Further research was conducted on the implications of malicious browser extensions. According to the University of Illinois' IT Knowledge Base, browser extensions can:

- Steal browsing data, credentials, and cookies
- Inject malicious advertisements
- Hijack user sessions
- Install spyware or malware
- Slow down system performance
- Persist even after attempted removal

Screenshot 5: Security Advisory on Malicious Extensions



Quick links

Check status

Get help

Email the Help Desk

Call the Help Desk (217) 244-7000

Submit a suggestion

Topics Map > Safety and security > Malware protection

Understanding the Dangers of Malicious Browser Extensions

Browser extensions are small software programs that add features or functionality to your web browser. They can block ads, manage passwords, or enhance productivity, but while many extensions are helpful, some are designed — or later compromised and modified — to harm users or steal information. Malicious plugins and extensions can expose users to significant security and privacy risks, including data theft, account compromise, and system performance issues.

Malicious browser extensions can:

- Steal Sensitive Data: Some extensions request broad permissions, allowing them to access browsing history, login credentials, cookies, and even credit card information. Attackers can use this data to hijack accounts or steal identities.
- Install Malware or Spyware: Extensions can install malware that operates silently in the background, monitoring activity or exfiltrating data without your knowledge.
- Hijack Sessions: By stealing session cookies, extensions can allow attackers to impersonate users on websites like Facebook or university portals.
- Redirect Searches and Inject Ads: Some extensions manipulate search results, inject unauthorized ads, or redirect affiliate revenue to attackers, degrading your browsing experience.
- Persist on Devices: Advanced malicious extensions may disable browser security settings or reinstall themselves after removal, making them difficult to eradicate.
- Slow Down Your Computer: Poorly designed or malicious extensions can consume system resources, leading to slower performance and increased frustration.

Best Practices for Safe Extension Use:

- Install Only What You Need: Limit the number of extensions you use. The fewer you have, the lower your risk.
- Check Permissions: Review the permissions an extension requests before installing. Avoid extensions that ask for more access than necessary, such as <all_urls> or access to sensitive data.
- Verify Authenticity: Install extensions only from reputable sources and developers. Check user reviews and ratings for red flags.
- Keep Extensions Updated: Updates often include security patches. Ensure your extensions are up to date.
- Review Regularly: Periodically review your installed extensions and remove any you no longer use or do not recognize.
- Install CrowdStrike: The security team can detect malicious extensions if installed.
  Keep Your Browsers Up to Date: regularly close your browsers and allow updates and security patches to be applied.
- Be Cautious of Phishing: Developers and users alike should be wary of phishing emails that may target extension accounts or attempt to trick users into installing malicious plugins.

What Should I Do If I Suspect a Malicious Extension?

- Remove the suspicious extension immediately via your browser's extensions menu.
- Change passwords for any accounts you accessed while the extension was installed.
- Run a CrowdStrike security scan on your device.
- Contact your IT Pro if you believe sensitive university data may have been compromised.

For additional resources related to Browsers, see the University of Illinois knowledge base articles on:

- Browsers, Clearing Cache and Cookies
- How to Remove Suspicious Browser Extensions

Step 8: Final Status and Trusted Extensions

After completion of the task, the following extensions were retained:

Extension Name	Purpose	Reason for Retention
Google Docs Offline	Access to offline Google Docs	Trusted and used
McAfee® WebAdvisor	Web security and protection	Security layer

All other non-essential extensions were removed for minimal risk exposure and better performance.

Extensions Removed

Extension Name	Justification
Adobe Acrobat: PDF Tools	Rarely used; elevated permissions; non-critical

---

Conclusion

This exercise reinforced the importance of regularly auditing browser extensions as part of routine cybersecurity hygiene. Even legitimate extensions can become security liabilities if not maintained or if compromised. Regular inspection ensures minimal exposure to:

- Data leakage
- Unauthorized access
- Browser exploitation

Key Learnings

- Always review extension permissions before installation.
- Retain only essential, trusted, and well-maintained extensions.
- Remove third-party extensions added without user knowledge.
- Research before installing new extensions, especially free or promotional ones.

Outcome

- Reduced attack surface
- Improved browser load time
- Better control over data and site access
- Awareness of malicious extension behaviors
