Suspicious Browser Extensions Removal Report

Name: Kirana P

Date: 14-Aug-2025

Browser Used: Google Chrome

1. List of Installed Extensions

Extension Name	Developer	Permissions	Recognized	Notes
Google Docs	Google Docs Inc	Access all sites	Yes	Trusted, widely used
McAfee	McAfee Inc	Access all sites	Yes	Trusted, widely used
EasyScreenshot	unknown	Access all Browsing data	No	Unfamiliar, investigate

2. Research & Evaluation

Extension: EasyScreenshot

Web Store Link: Found, but little detail.

Ratings & Reviews: Rated 2.3/5; complaints about pop-ups, data misuse.

Developer: No credible website or contact info.

Permissions: Requests access to all browsing data—excessive for a screenshot tool.

External Reports: Listed as potentially harmful on some forums/blogs.

Decision: Removed

Reason: Negative reputation, excessive permissions, and suspicious developer.

3. Actions Taken

Extension Name	**Action**	**Date**	**Reason for Removal**
EasyScreenshot	Removed	14-Aug-2025	Excessive permissions, Security risks found

4. Key Takeaways / Reflection

What I Learned: Extensions can request dangerous permissions and pose real privacy/security threats, even if on official stores.

Surprise Findings: Some trusted-seeming tools had poor reviews and unexplained permissions.

Future Actions: I will only install verified extensions, always check permissions, and periodically review installed add-ons.

5. Steps Taken to Remove Extension

1. Opened the Extensions page in Chrome.

2. Reviewed all installed extensions and found “EasyScreenshot.”

3. Researched “EasyScreenshot” online.

4. Found reports of suspicious activity and negative user reviews.

5. Clicked “Remove” next to the extension.

6. Confirmed removal when prompted.

7. Verified that the extension was gone from the list.

.**Research how malicious extensions can harm users.**

Malicious browser extensions can cause significant harm to users through a wide variety of attacks and privacy violations:

Theft of Sensitive Data: Malicious extensions may request broad permissions that allow them to access and steal your browsing history, login credentials, session cookies, credit card numbers, and even confidential business information. This data can be exfiltrated to attackers, leading to identity theft or financial loss.

Account Compromise and Session Hijacking: By stealing session cookies or authentication tokens, attackers can impersonate users and gain access to sensitive websites, potentially taking over personal or corporate accounts without needing the actual username and password.

Surveillance and User Tracking: These extensions can act as spyware, silently tracking your browsing behavior, recording keystrokes (keylogging), capturing screenshots, or even accessing your camera, microphone, or physical location. This enables targeted phishing campaigns or privacy invasion.

Malware Installation: Some extensions deploy additional malicious software to your system, such as ransomware, spyware, or remote access trojans, compromising your device’s security even further.

Browser Hijacking and Content Manipulation: Attackers can alter your search results, redirect your traffic to phishing sites or malware downloads, inject unauthorized ads on pages you visit, and manipulate the content you see. For example, you might be redirected to a fake login page or a site prompting you to install fake software, resulting in further compromise.

Fraud and Click Hijacking: By injecting or modifying affiliate links, malicious extensions can commit advertising fraud, generate revenue for attackers at your expense, or redirect legitimate payments to unauthorized recipients.

Persistence and Stealth: Many malicious extensions are programmed to disable browser security controls, evade removal, or reinstall themselves automatically. Because they integrate directly with the browser, their activities can remain hidden for a long time.

Corporate Espionage and System Compromise: In enterprise environments, malicious browser extensions have been used to carry out industrial espionage and attacks that compromise entire IT infrastructures by stealing sensitive company data or spreading malware across organizational networks.

Performance Issues: Even outside of intentional harm, malicious or poorly designed extensions can severely slow down your browser and overall computer performance, leading to loss of productivity or system crashes.

Real-World Case Examples:

- Sometimes trusted extensions are bought out by malicious actors or compromised through developer credential theft. Attackers then update the extensions with harmful code, affecting millions of users without their knowledge.

- Recently, over 2 million users were affected when seemingly legitimate extensions began tracking user activity, hijacking browsers, and redirecting users to phishing or malware site.