# Identify and Remove Suspicious Browser Extensions

## Objective:

To learn how to identify and remove potentially harmful or unnecessary browser extensions.

## Tools Used:

* Google Chrome

## Steps Performed:

1. Opened the Chrome extensions page via “chrome://extensions/”.
2. Reviewed all installed browser extensions.
3. Checked extension permissions and verified them with Chrome Web Store reviews.
4. Identified an unfamiliar and suspicious extension.
5. Removed the suspicious extension.
6. Restarted the browser to apply changes.
7. Observed improved performance and increased awareness of extension-related risks.

## Installed Extensions:

|  |  |  |
| --- | --- | --- |
| **Extension Name** | **Status** | **Comments** |
| BlockSite: Block Websites & Stay Focused | Kept | Productivity tool, trusted extension. |
| Cold Turkey Blocker | Kept | Used for blocking distractions, no red flags. |
| Google Docs Offline | Kept | Google official extension, safe and necessary. |
| Loom – Screen Recorder & Screen Capture | Kept | Useful for screen recordings, good reviews. |
| EasyConvert PDF Tool | Removed | Unknown origin, requested access to all websites, poor reviews. Marked as suspicious. |

## Outcome:

* Removed 1 suspicious extension.
* Verified safety of all remaining extensions.
* Gained awareness of how extensions can pose security or privacy risks.

## Research on Malicious Extensions

Malicious browser extensions pose serious security and privacy threats. During this task, I researched how they can harm users, and here are the key findings:

* **Data Theft:** Some extensions can read and exfiltrate sensitive data such as passwords, credit card numbers, and browsing history.
* **Ad Injection:** They may insert ads or redirect users to malicious websites, compromising browsing experience and security.
* **Cryptojacking:** Some malicious extensions secretly use the user’s device to mine cryptocurrency, slowing down performance.
* **Session Hijacking:** Malicious code can hijack browser sessions, gaining unauthorized access to accounts or impersonating users.
* **Surveillance:** These extensions may track all user activity, even on sites where privacy is expected, such as banking or email platforms.
* **Backdoor Installation:** Some are designed to install further malware or act as a gateway for remote attackers.

**Example Case:** In 2020, Google removed over 100 malicious Chrome extensions that were stealing user data under the guise of utilities like PDF converters and ad blockers.

## ****Prevention Tips:****

* Only install extensions from reputable developers.
* Regularly audit permissions.
* Limit the number of active extensions.
* Avoid extensions with low ratings or suspicious reviews.

## Conclusion:

Regular review and cleanup of browser extensions can significantly reduce security vulnerabilities and improve browser performance. This task highlighted the importance of managing extensions carefully.