

How Malicious Browser Extensions Can Harm Users

Malicious browser extensions are a growing vector of cyberattacks due to their ability to operate within the user's browser environment with elevated permissions. Below are the primary ways such extensions can compromise user security and privacy:

1. Data Theft

- Malicious extensions can intercept user inputs and harvest sensitive data such as login credentials, personal information, and credit card numbers.
- Example: Clipboard hijacking to steal copied passwords or cryptocurrency wallet addresses.

2. Session Hijacking

- They may read cookies or session tokens, allowing attackers to impersonate users on trusted websites, including online banking or email accounts.

3. Clickjacking & Phishing

- By injecting malicious JavaScript into legitimate web pages, extensions can create fake input forms or redirect users to phishing sites.

4. Ad Injections & Affiliate Fraud

- Some extensions silently inject ads into web pages or replace legitimate links with affiliate ones to generate revenue, affecting page integrity and user trust.

5. Surveillance and Tracking

- Extensions may track browsing history and online activity, creating behavioral profiles without user consent. This data can be sold or used for targeted attacks.

6. Backdoor or Remote Access

- Some extensions act as a backdoor, connecting to external servers to download and execute additional malicious payloads.

7. Cryptojacking

- By utilizing the user's CPU power to mine cryptocurrency without permission, cryptojacking extensions can significantly degrade system performance and increase energy usage.

Real-world Example:

In 2020, Google removed over 100 malicious Chrome extensions that had over 32 million downloads. These extensions exfiltrated browsing data and redirected users to malicious websites under the guise of offering file converters and ad blockers.

Documentation of Steps Taken and Extensions Removed

As part of the security hygiene task, the following steps were executed to audit and clean up browser extensions:

1. Initial Review

- Opened the browser's extension manager (`chrome://extensions/` and `about:addons`).
- Recorded the list of all installed extensions across Chrome and Firefox.

2. Permissions & Credibility Check

- Analyzed permissions requested by each extension.
- Reviewed user feedback, star ratings, and developer information from official stores.

3. Identification of Potential Risks

- Flagged extensions with the following characteristics:
 - Excessive permissions (e.g., full access to browsing history or clipboard).
 - Low user ratings and poor review comments.
 - Suspicious behavior (redirects, pop-ups, performance degradation).

4. Extensions Removed

Extension Name	Reason for Removal
PDF Converter Pro	Unnecessary access to clipboard and tabs; ad injection
Weather Now	Unused; requested location and history unnecessarily
Coupon Finder	Injected affiliate links; intrusive advertising behavior

5. **Post-removal Actions**

- Restarted the browser to refresh the environment.
- Monitored for performance and behavioral improvements.

6. **Outcome Observed**

- Improved browser load time.
- No unusual redirects or pop-ups.
- Lower memory and CPU usage observed in system monitor.

Conclusion :

This task significantly enhanced my awareness of the security risks associated with browser extensions. I learned how even commonly used add-ons can pose threats if not properly vetted for permissions and developer credibility. By manually auditing and removing potentially unsafe extensions, I gained practical experience in identifying early indicators of malicious behavior and implementing preventive measures. Overall, this exercise emphasized the importance of proactive extension management as part of everyday cybersecurity hygiene.