

## # Research: Risks of Malicious Browser Extensions

Browser extensions often enhance usability and provide additional features, but if they are malicious or compromised, they can create serious threats to both **security** and **privacy**. Below are some of the major risks:

### ### 1. Theft of Personal Data

- \* Can capture confidential details such as login credentials, credit card numbers, cookies, and browsing records.

- \* Example: A fake password manager secretly recording everything typed.

### ### 2. Unwanted Ads & Redirections

- \* Inject extra pop-ups, banners, or ads into web pages.

- \* May also redirect users to phishing pages or other harmful sites.

### ### 3. User Tracking & Privacy Breach

- \* Some extensions monitor browsing activity using powerful permissions like **“Read and change all your data on the websites you visit.”**

- \* Collected information might be sold to advertisers or misused by attackers.

### ### 4. Abusing Excessive Permissions

- \* With overly broad permissions, extensions can tamper with web content, alter search results, or run hidden scripts in the background.

### ### 5. Delivery of Malware

- \* Can act as a channel to download and install malware, including spyware, ransomware, or keyloggers, without the user realizing it.

### ### 6. Exploiting System Resources

- \* Some malicious add-ons hijack CPU/GPU resources for hidden tasks such as **cryptocurrency mining**, which slows down the system.

## ## Key Points to Remember

- \* Malicious extensions are dangerous because they appear to be useful tools.

- \* Only install from reliable marketplaces (e.g., Chrome Web Store, Firefox Add-ons).

- \* Always verify the developer’s credibility, check reviews, and examine requested permissions.

- \* Regularly audit installed extensions and remove any that seem unnecessary or suspicious.