# Research how malicious extensions can harm users.

Malicious browser extensions can pose significant security and privacy threats to users. These harmful extensions often appear as legitimate tools (e.g., ad blockers, shopping assistants), but once installed, they can exploit browser permissions to carry out various malicious actions.

---

**How Malicious Extensions Can Harm Users:**

**1. Data Theft**

- **What they do:** Steal sensitive information such as:
  - Passwords
  - Credit card details
  - Browsing history
  - Cookies and session tokens
- **How:** By injecting malicious JavaScript that reads data from web pages or form fields.

**2. Credential Harvesting**

- Some extensions log keystrokes or auto-filled login credentials and send them to remote servers.

**3. Session Hijacking**

- **By accessing session cookies**, extensions can impersonate users on websites (e.g., Gmail, banking sites).

**4. Ad Injection and Click Fraud**

- Inject unwanted ads into websites, earning revenue through ad impressions or clicks.
- Redirect users to affiliate or malicious websites.

**5. Man-in-the-Browser (MitB) Attacks**

- Modify web pages in real-time to change content, insert phishing forms, or alter transaction details (e.g., in online banking).

**6. Downloading and Executing Malware**

- Can download additional malware or backdoors to the user's system.
- Some exploit APIs to interact with the file system (especially in Chromium-based browsers).

**7. Browser Hijacking**

- Change default search engines, home pages, and new tab pages to malicious sites without user consent.

**8. Tracking and Surveillance**

- Track user behavior across websites, often selling data to third parties or using it for profiling.

**9. Privilege Escalation**

- Exploit security flaws in browser extension APIs to gain higher privileges or escape the browser sandbox.

---

**Real-World Examples**

1. **DataSpii (2019):**
   - Browser extensions leaked sensitive data from over 4 million users, including corporate information and private documents.
2. **Great Suspender (2021):**
   - A popular Chrome extension was found to contain malware after it was sold to a new developer.
3. **Fake Ad Blockers (2018):**
   - Several malicious ad blocker clones tricked users and injected harmful scripts.

---

**How to Stay Safe**

- **Install from official stores only (Chrome Web Store, Firefox Add-ons)**
- **Check reviews, permissions, and developer information**
- **Use browser security features to review and restrict extension permissions**
- **Keep browsers and extensions updated**
- **Avoid installing unnecessary extensions**
- **Regularly audit installed extensions for suspicious behavior**

There are no malicious/unwanted extensions that are installed in the browser and everything looks clean.