# Browser Extension Security Audit

## Research: How Malicious Extensions Can Harm Users

* Data Theft:

Extensions with broad permissions can read personal data such as saved passwords, email content, or online forms.

* Tracking & Privacy Invasion:

They may secretly track browsing habits, visited websites, or keystrokes and sell this data to advertisers or attackers.

* Browser Hijacking:

Some extensions change your default search engine or homepage to redirect traffic for profit or phishing.

* Ad Injections:

Attackers insert unwanted ads or pop-ups into legitimate websites to generate revenue or spread malware.

* Credential Harvesting:

Fake login pages may appear to trick users into entering sensitive information like usernames and passwords.

* Crypto Mining:

Extensions can secretly use your computer’s resources to mine cryptocurrency, slowing down system performance.

* System Compromise:

In rare cases, extensions exploit browser vulnerabilities to install malware or gain control over parts of your device.

## Documentation: Steps Taken & Extensions Removed

|  |  |  |
| --- | --- | --- |
| **Step** | **Action** | **Details/Findings** |
| 1 | Opened browser extension manager | Checked Chrome Extensions via chrome://extensions/ |
| 2 | Reviewed installed extensions | Total of 8 extensions found |
| 3 | Checked permissions | Two extensions requested excessive permissions |
| 4 | Identified suspicious extensions | Found “Video Downloader Pro” and “Free Coupons Finder” |
| 5 | Removed unnecessary extensions | Both suspicious extensions uninstalled |
| 6 | Restarted browser | Noticed faster startup and smoother browsing |
| 7 | Verified performance | No pop-ups or redirects observed |
| 8 | Saved documentation | Recorded details for future reference |