# Identifying and Removing Malicious Browser Extensions

**Risks of Malicious Extensions**

- **Data Theft** – Some extensions secretly collect user credentials, browsing history, and personal data.
- **Ad Injection** – Unauthorized ads may appear on webpages, redirecting users to unsafe sites.
- **Security Vulnerabilities** – Malicious extensions may disable browser security, making users vulnerable to cyber threats.
- **Browser Manipulation** – Some extensions hijack search engines, changing default settings to push harmful content.

**Steps Taken to Identify Suspicious Extensions**

1. **Checked Installed Extensions**
    - **Chrome**: Accessed chrome://extensions/.
    - **Firefox**: Checked about:addons.
    - **Brave**: Used the Chrome Extensions page.

2. **Reviewed Permissions**
    - Flagged extensions requesting unnecessary access (e.g., tracking browsing activity).

3. **Verified Extension Source**

- Ensured extensions were downloaded from official stores and had legitimate developer reviews.

**Extensions Removed**

- friGate Light: Designed to bypass site restrictions, but it also encrypted user traffic data in suspicious ways.
- Nimble Capture & KProxy: These extensions stripped security protections from websites, making users vulnerable to attacks.