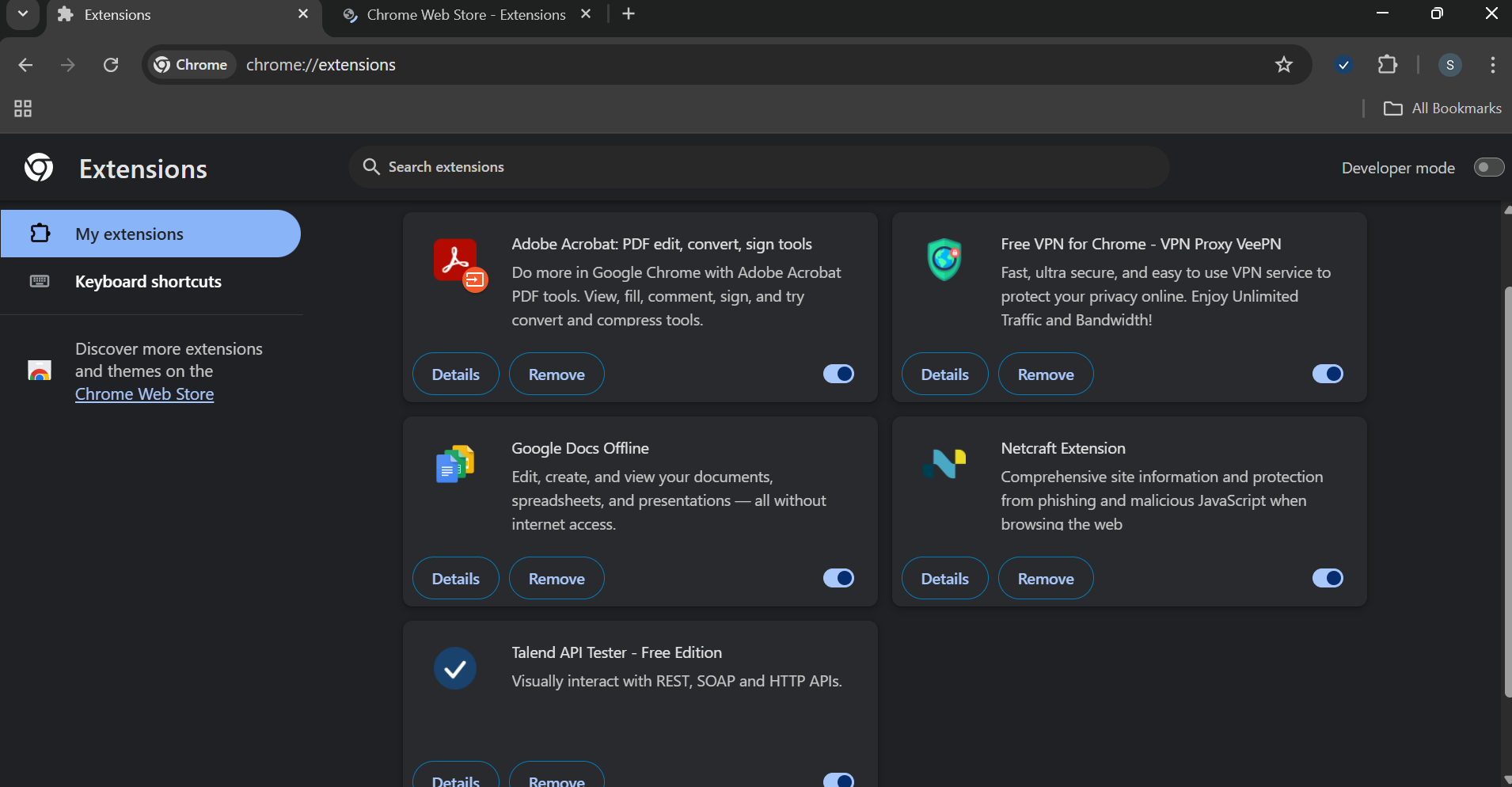
**Identify and Remove Suspicious Browser Extensions.**

Since I donot have any suspicious extensions I am taking examples available on blogs.



**How Malicious Browser Extensions Harm Users**

1. **Stealing Sensitive Data**

* **What it does**: Captures keystrokes, form inputs, or clipboard data.
* **Examples**:
  + Logins and passwords
  + Credit card numbers
  + Personal messages or emails

**2. Spying on Browsing Activity**

* **What it does**: Tracks visited websites, search queries, and clicks.
* **Purpose**: Builds user profiles, sells data to advertisers, or spies for cybercriminals.
* **Often disguised as**: Shopping helpers, coupon finders, search enhancers.

**3. Injecting Malicious Code**

* **What it does**: Injects JavaScript into websites you visit.
* **Risks**:
  + Alters content (e.g., fake login forms)
  + Redirects to phishing/malware sites
  + Loads ads or cryptocurrency miners

**4. Exfiltrating Files and Screenshots**

* **Advanced threats**: Extensions can request permissions to read/download files, take screenshots, or access camera/microphone.

**5. Bypassing Browser Security**

* Some extensions:
  + Disable or weaken **Content Security Policies (CSP)**
  + Bypass same-origin policy
  + Open backdoors via WebSockets or C2 servers

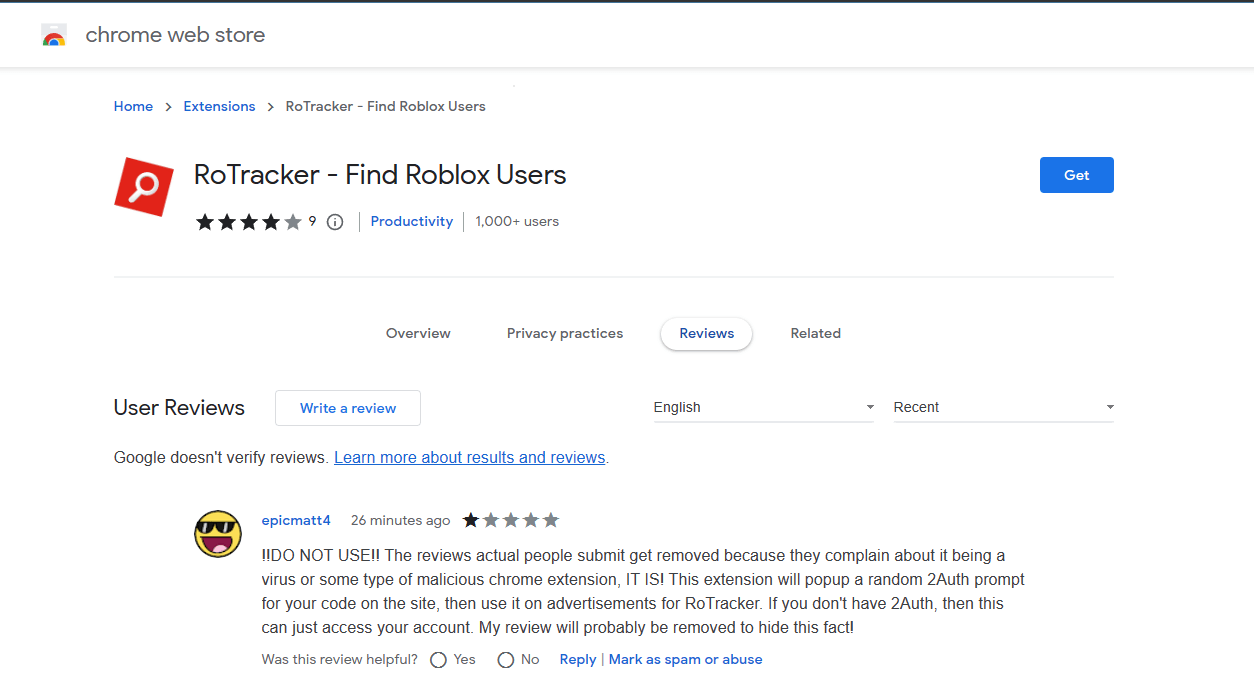
**6. Persistence & Evasion**

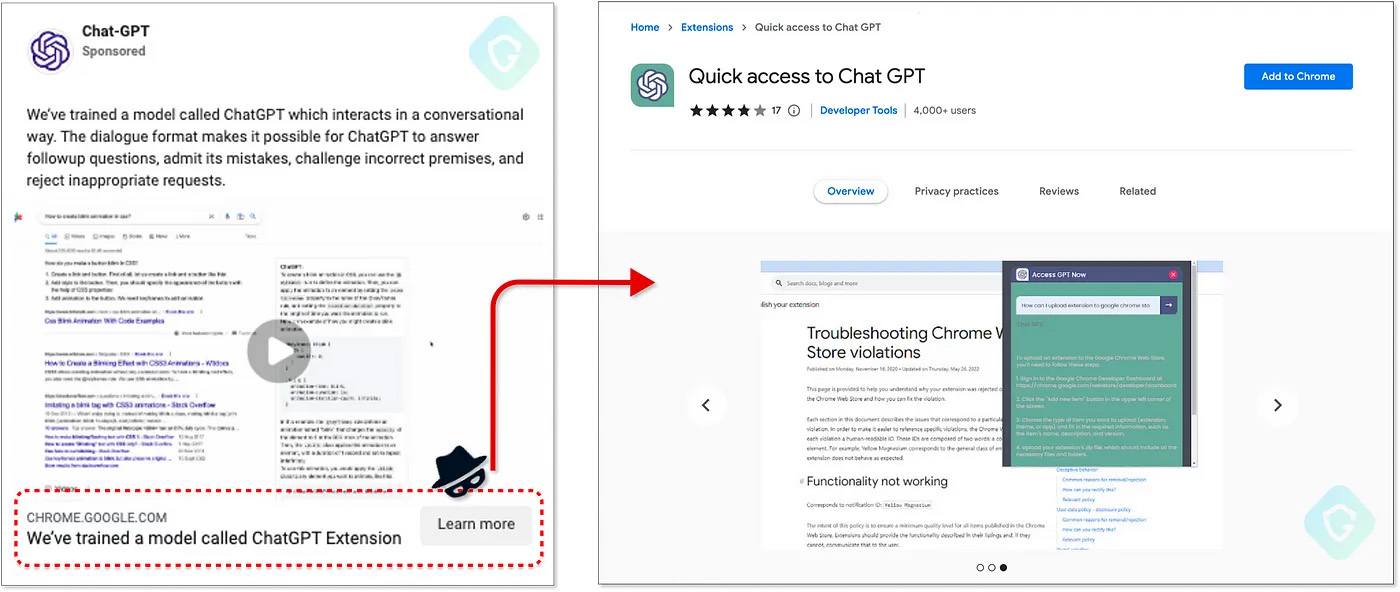
* Obfuscated code hides malicious behavior
* Auto-updates push malicious code after being approved as “clean”
* Uses cloud-hosted code to dynamically change behavior

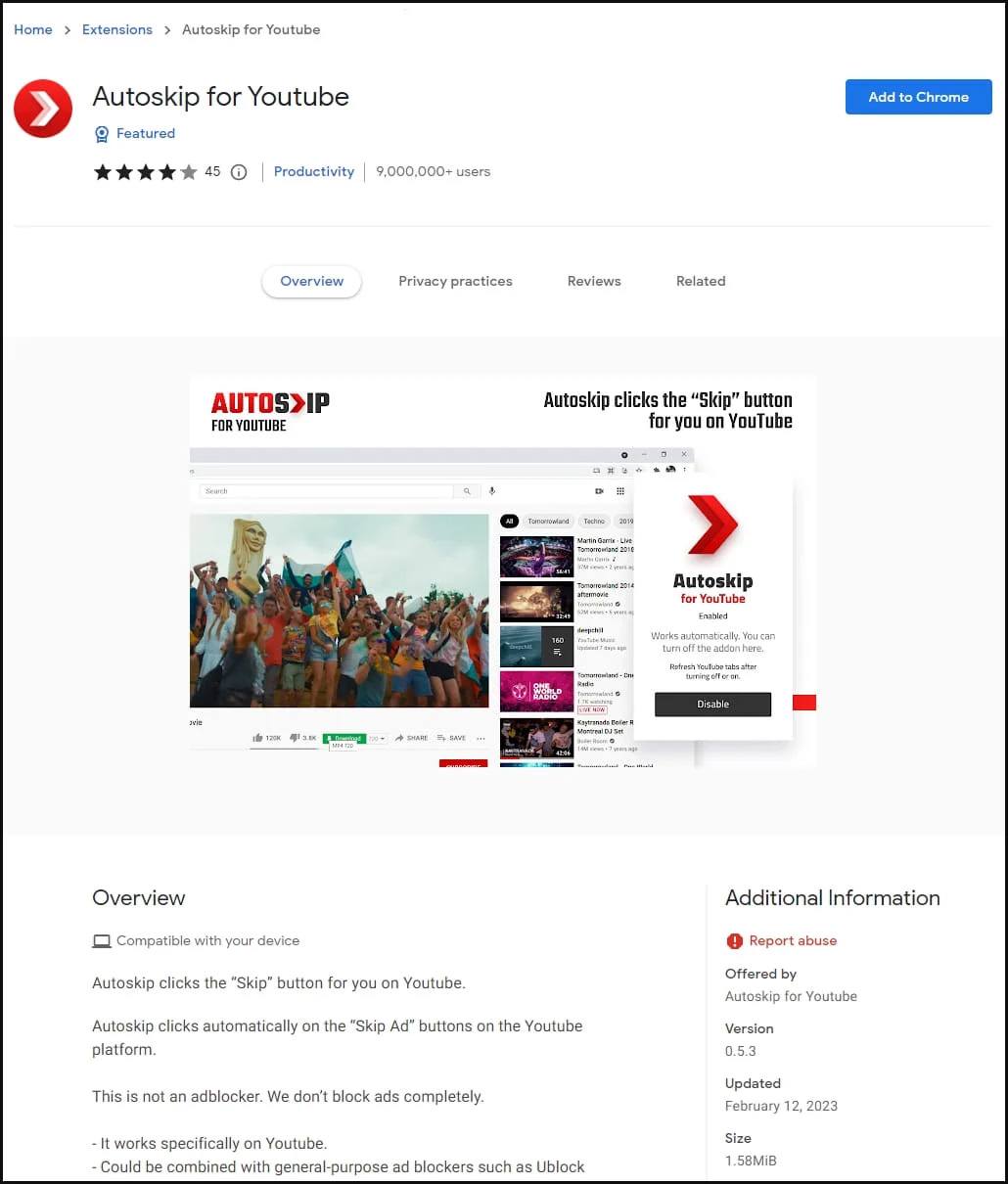
**7. Controlling the Browser**

* Can:
  + Change homepage or search engine
  + Install additional extensions silently
  + Disable other security features or extensions

**Examples:**







**How to Stay Safe**

* Only install extensions from trusted sources (e.g., official Chrome/Firefox stores)
* Review permissions carefully — don’t install extensions that want “access to all websites” unless absolutely necessary
* Limit number of extensions — fewer means smaller attack surface
* Use security tools — like browser isolation or anti-malware plugins
* Audit your extensions regularly — remove ones you no longer use