Task 7: Identify and Remove Suspicious Browser Extensions

Author: Anshikaa Pahilajani

Cyber Security Internship — Elevate Labs

Date: 2 October 2025

Objective

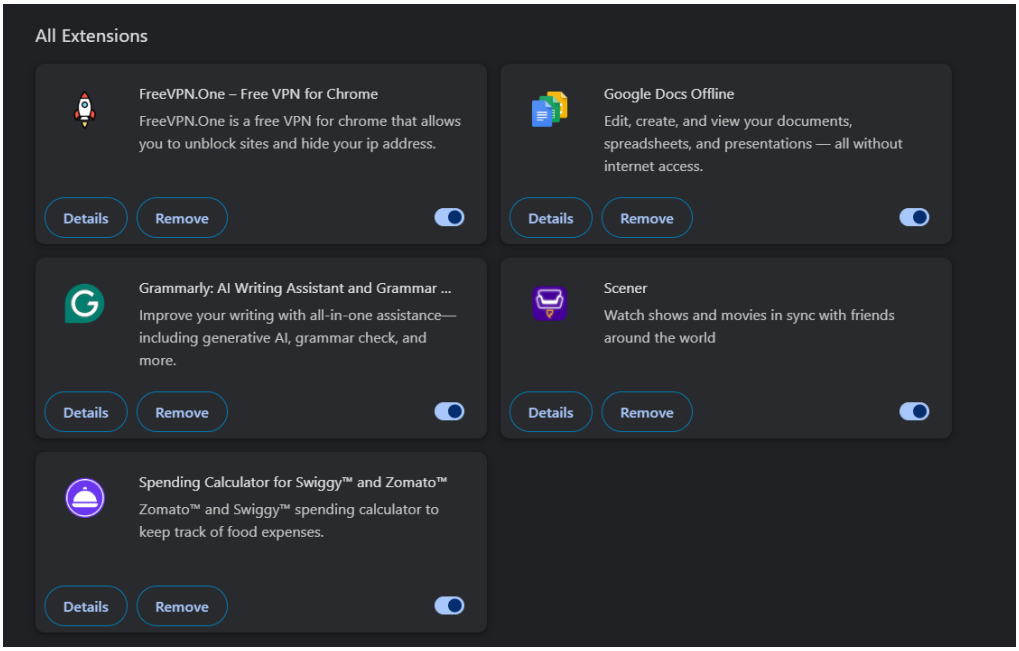
To identify, analyze, and remove potentially harmful browser extensions in Chrome, understand their permissions, and raise awareness of browser security risks.
Note: A demo extension (**FreeVPN.One**) was installed temporarily to demonstrate detection and removal of suspicious extensions. It was **removed immediately** after analysis.

Tools Used

- Chrome Browser (chrome://extensions/)
- Chrome Web Store
- Word / PDF for documentation

Steps Performed

1. Opened Chrome → chrome://extensions/.

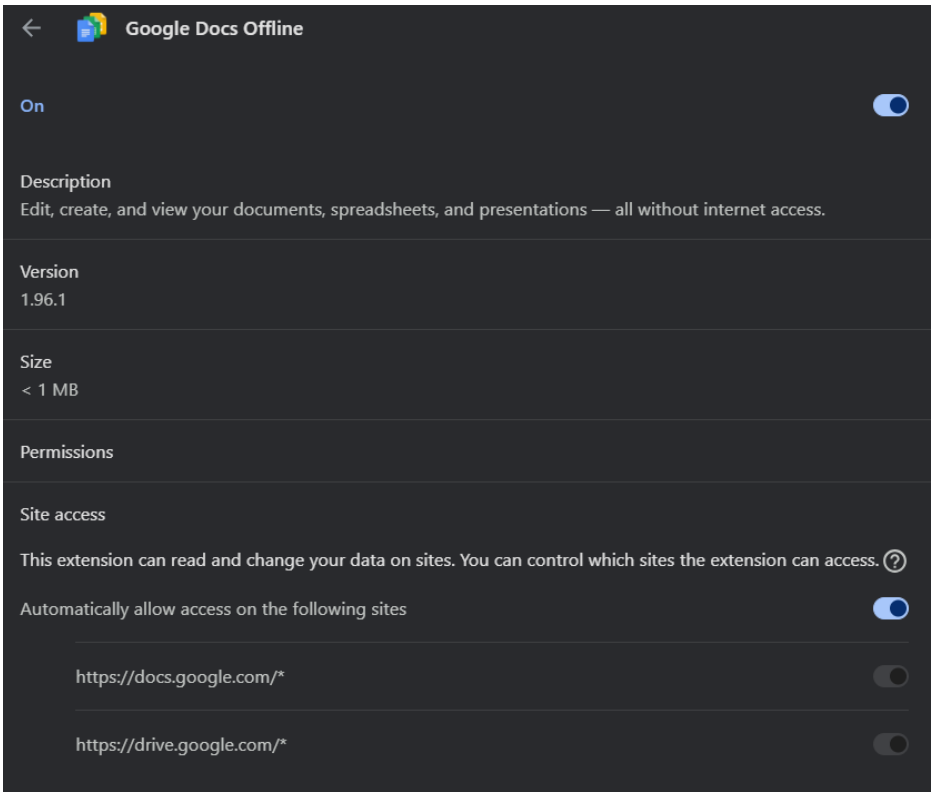


2. Reviewed each extension individually:
    - Checked **permissions**
    - Checked **site access**
    - Verified legitimacy (official store, developer, reviews)

3. Identified unused or suspicious extensions.
4. Removed unnecessary/suspicious extensions.
5. Restarted Chrome to verify changes and performance.
6. Documented all steps, findings, and lessons learned.

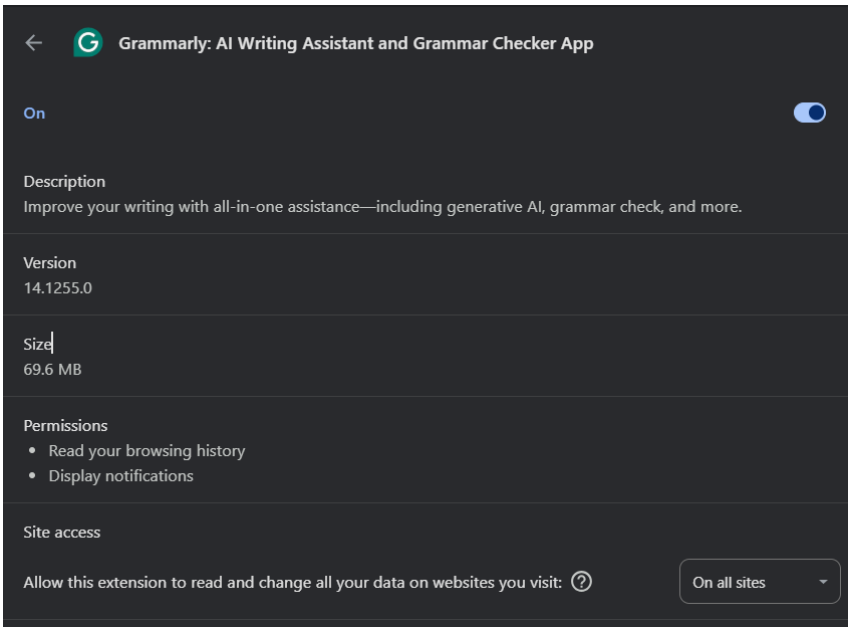
Findings / Analysis

1. **Google Docs Offline**



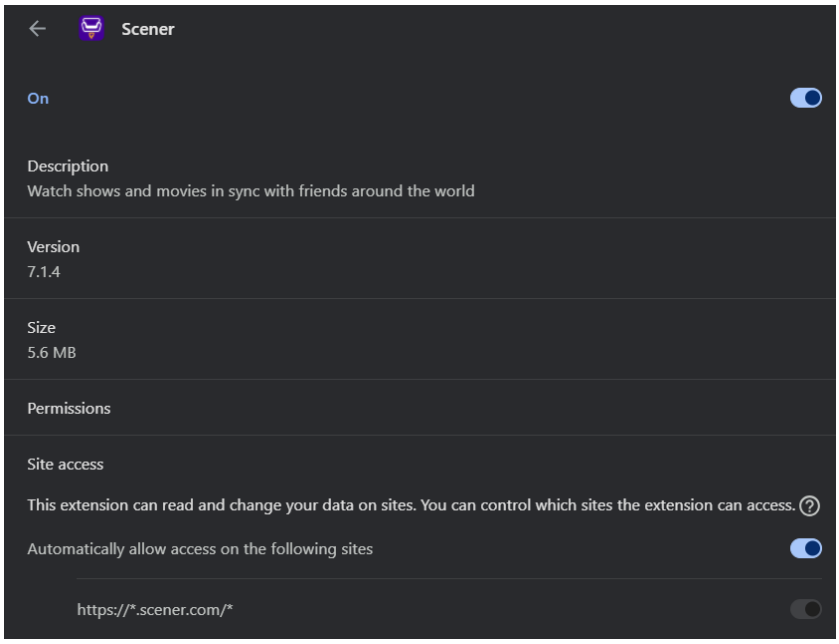
- **Permissions:** Read and change data only on docs.google.com and drive.google.com
- **Site Access:** Limited to Google Docs & Drive
- **Good Points:** Official Google extension, only needed permissions, safe
- **Potential Risks:** Minimal, no suspicious activity
- **Conclusion:** Legitimate and safe.

2. Grammarly: AI Writing Assistant



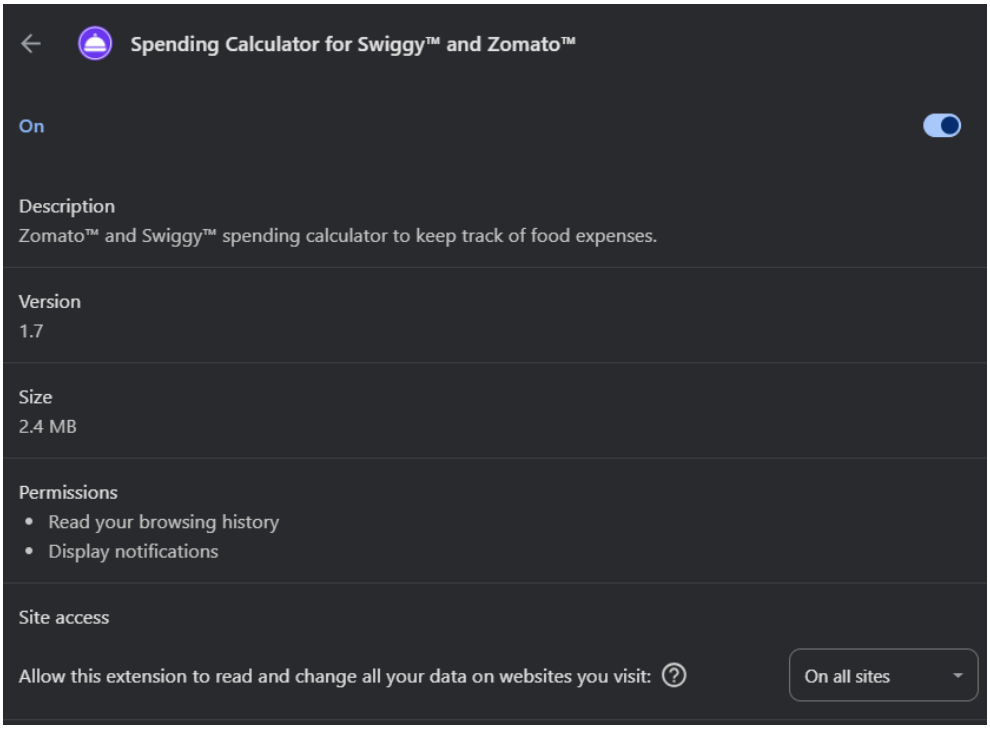
- **Permissions:** Read browsing history, display notifications
- **Site Access:** All websites visited
- **Good Points:** Trusted brand, helps with writing & grammar
- **Potential Risks:** Broad access can theoretically read all text input, privacy-conscious users should monitor usage
- **Conclusion:** Safe, but high-scope permissions require awareness

3. Scener



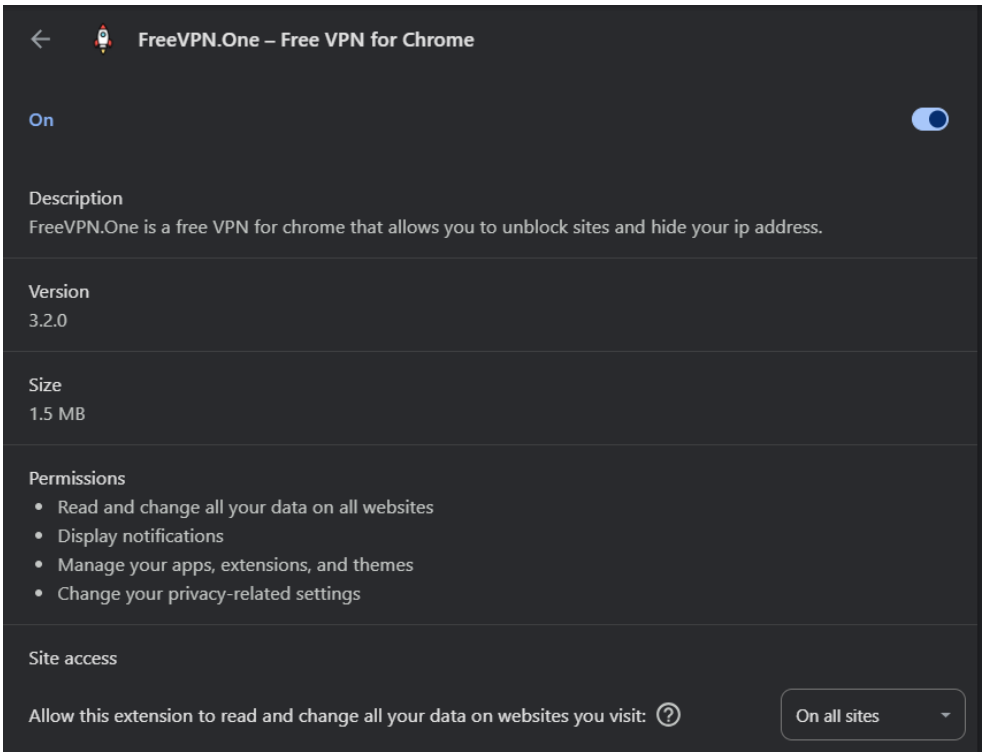
- **Permissions:** Read/change data on scener.com domain only
- **Site Access:** Restricted to scener.com and subdomains
- **Good Points:** Narrow permissions, limited scope, functional for intended purpose
- **Potential Risks:** Minimal, nothing suspicious
- **Conclusion:** Safe extension

4. **Spending Calculator (Swiggy & Zomato)**

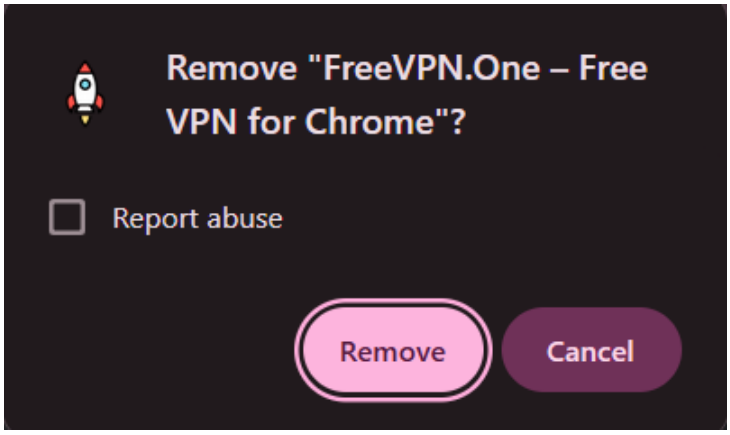


- **Permissions:** Read browsing history, display notifications
- **Site Access:** All sites
- **Good Points:** Useful for tracking online spending
- **Potential Risks:** Permissions broader than needed, could access unrelated sites
- **Conclusion:** Legitimate but less trustworthy, removed if unused for safety

5. **FreeVPN.One (Demo for Report Purposes)**



- **Permissions:** Read/change all site data, manage apps/extensions/themes, change privacy settings, display notifications
- **Site Access:** All sites
- **Good Points:** VPN functionality
- **Potential Risks:** Extremely broad permissions, can read/change all sites, manage other extensions, modify privacy settings, documented as malicious in security research
- **Conclusion:** Suspicious extension installed temporarily for demonstration, **removed immediately**. Shows importance of auditing extension permissions.



Summary Table

Extension	Permissions	Site Access	Good Points	Potential Risks	Action Taken
Google Docs Offline	Read/change Docs/Drive	Google Docs & Drive	Official, safe	Minimal	Kept
Grammarly	Read history, notifications	All sites	Trusted brand	High access scope	Kept
Scener	Read/change Scener	Scener only	Narrow permissions	Minimal	Kept
Spending Calculator	Read history, notifications	All sites	Useful	Broad access	Optional removal
FreeVPN.One	Read/change all, manage extensions, privacy settings	All sites	VPN function	Highly risky, malicious	Removed

Key Learnings

- Always review **permissions and site access** for each extension.
- Trusted extensions are generally safe but check for **broad permissions**.
- Niche or free extensions may request unnecessary access → **potential risk**.
- Installing a demo suspicious extension illustrates proactive security practices.
- Removing unused/suspicious extensions reduces attack surface.

Conclusion

The review of Chrome extensions showed that:

- Most installed extensions were safe and legitimate.
- One demo extension (**FreeVPN.One**) demonstrated how broad permissions can signal potential malicious behavior.
- Proactive auditing and removal of unused or suspicious extensions is essential to maintain browser security.