

Report: Analysis of My Browser Extensions

Date: June 5, 2025 **Intern:** Muhammad Ali Khan **Organization:** ELEVATE LABS

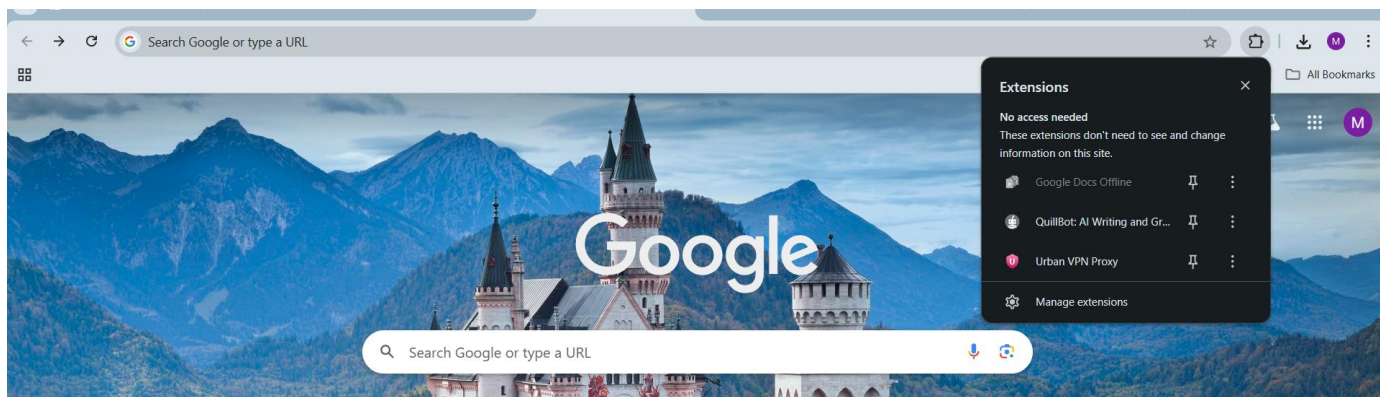
1. Introduction

This report documents all the steps executed to perform Task 7 of the internship. This task focuses on identifying and removing potentially harmful browser extensions to enhance cybersecurity hygiene and to critically evaluate installed extensions by examining their permissions and reviews.

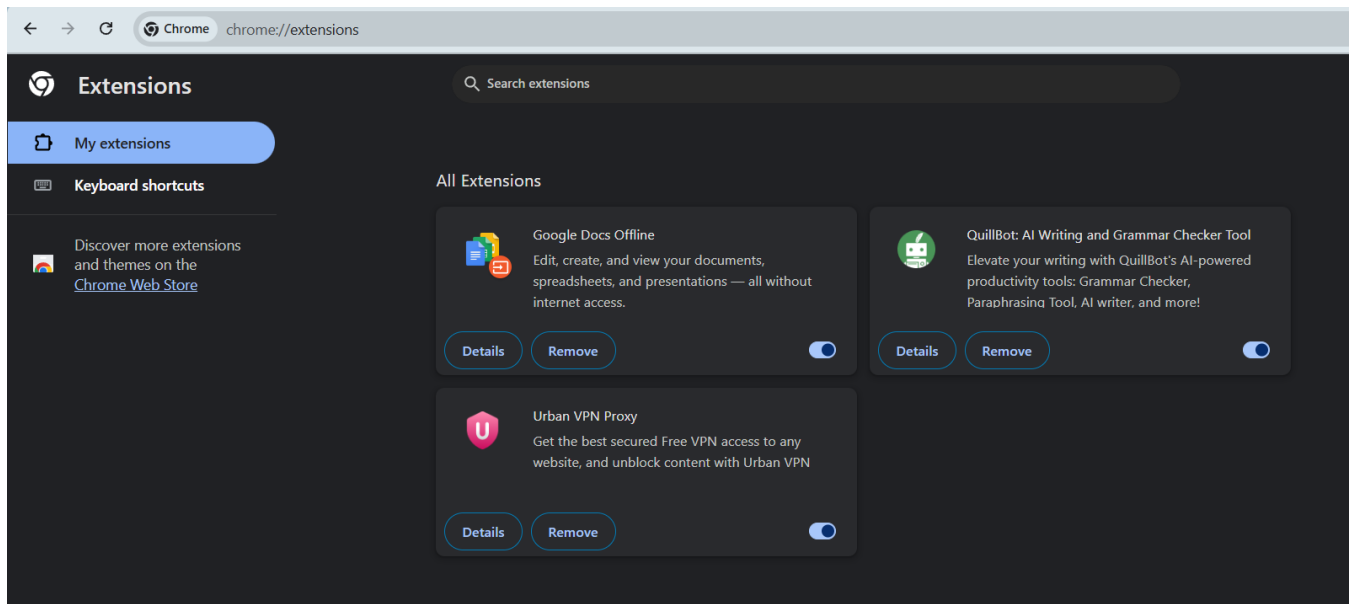
Objective: Eliminate unnecessary or suspicious add-ons, which can improve browser performance and protect against threats like data theft or malware injection.

2. Opened my browser – Google Chrome.

Then, selected the extensions icon beside the search bar and clicked on the Manage extensions icon to open the extension manager of google chrome.



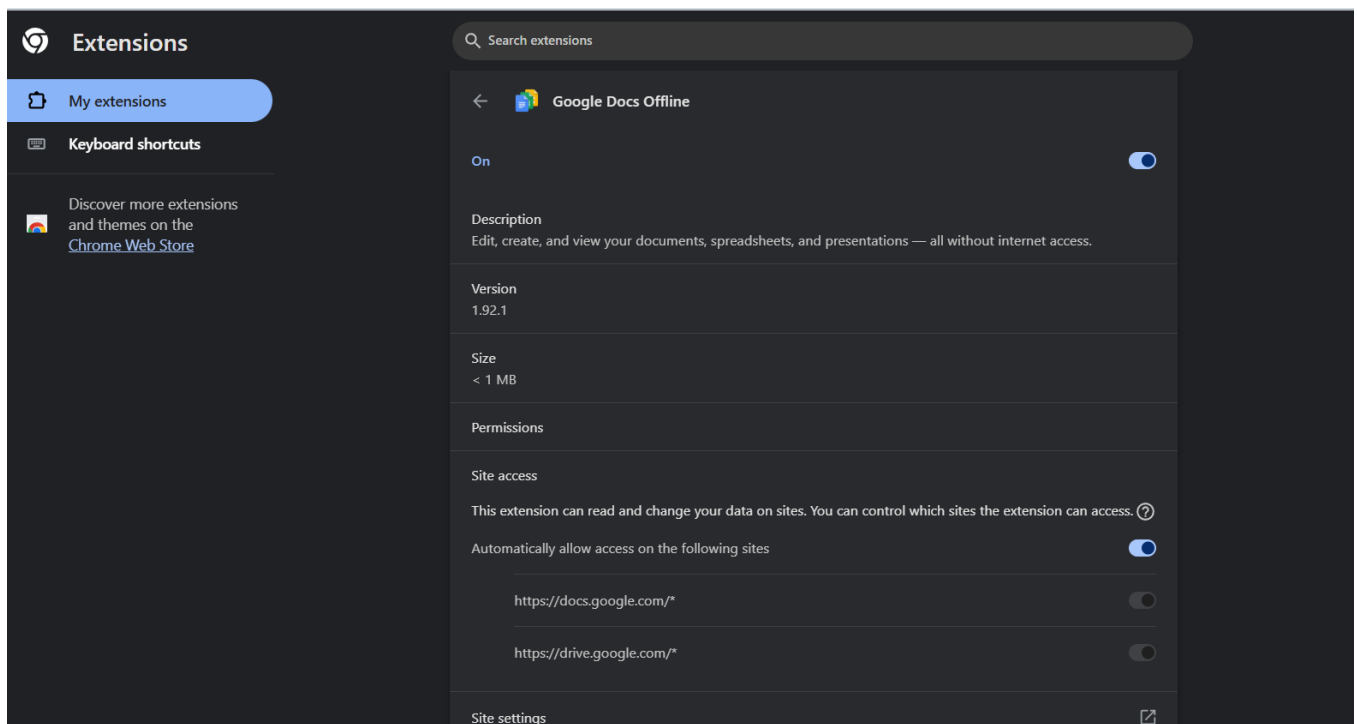
Now, the extensions tab is open and it shows the following 3 extensions added to my chrome browser: **1. Google Docs Offline** **2. QuillBot** **3. Urban VPN Proxy**

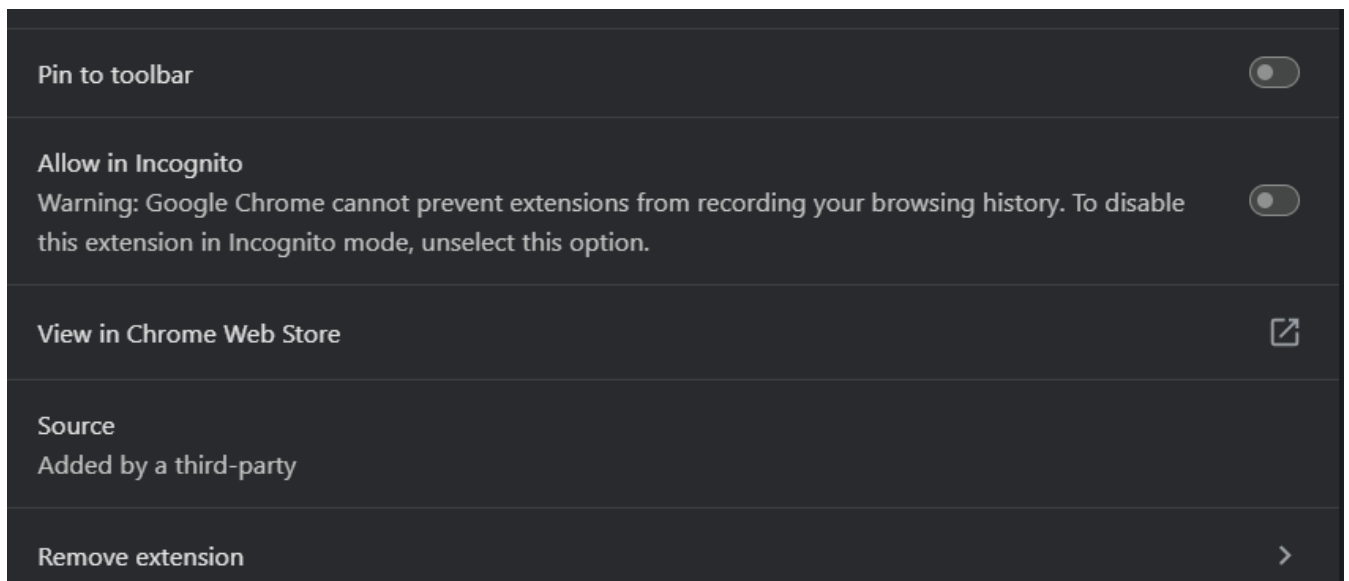


3. Reviewing all of the extensions one by one for careful examination.

The following steps include clicking on the Details option for each of the extensions.

Opened the Google Docs Offline extension – which enables me to continue my work on google docs in case of internet disconnection.





The permissions required by this extension are **none**, as can be seen above in the screenshot under the Permissions bar. Next, to check the reviews I opened the extension in Chrome Web Store by clicking on the link provided: ‘*View in Chrome Web Store*’. Then clicked on reviews which displayed the following page:

2.3 out of 5 ★★☆☆☆

7.2K ratings • Google doesn't verify reviews. [Learn more about results and reviews.](#)

Filter by All reviews Sort by Recent Language English Write a review

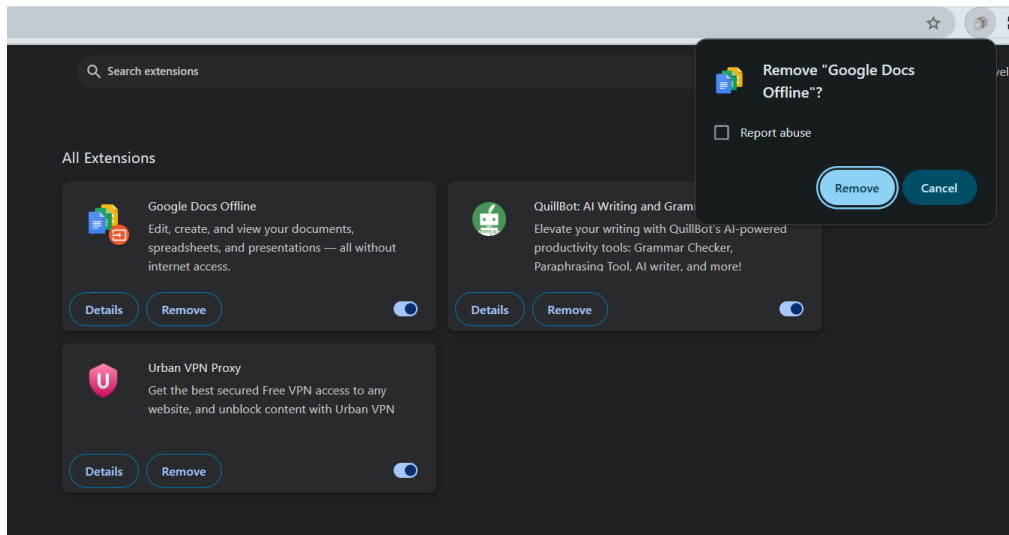
Jonathan Scheiderer ★☆☆☆☆ 5 Jun 2025
When, in all of the operation of work sheets, spreadsheet, doc history, has the basic original operating functions of a computer needed to be an extension?
Was this helpful? 👍 👎

teve bah ★☆☆☆☆ 4 Jun 2025
The enshittification continues, and we have to install an extension to preserve a basic function of the program.
We had a nice few years when tech more or less worked the way we needed it to. We, us, the people who do the overwhelming majority of the work.
Need all the billionaires to take a long trip in a short submarine. Have a nice trip, fellas.
1 person found this review to be helpful 👍 👎

The reviews of this extension – Google Docs Offline aren’t good. It only scores **2.3 out of 5**. Moreover, the reviews provided by the users, **do not appreciate the functionality of this extension**. Therefore, through careful examination and thoughtful observation, I hereby decide **to remove this extension due to the following reasons**:

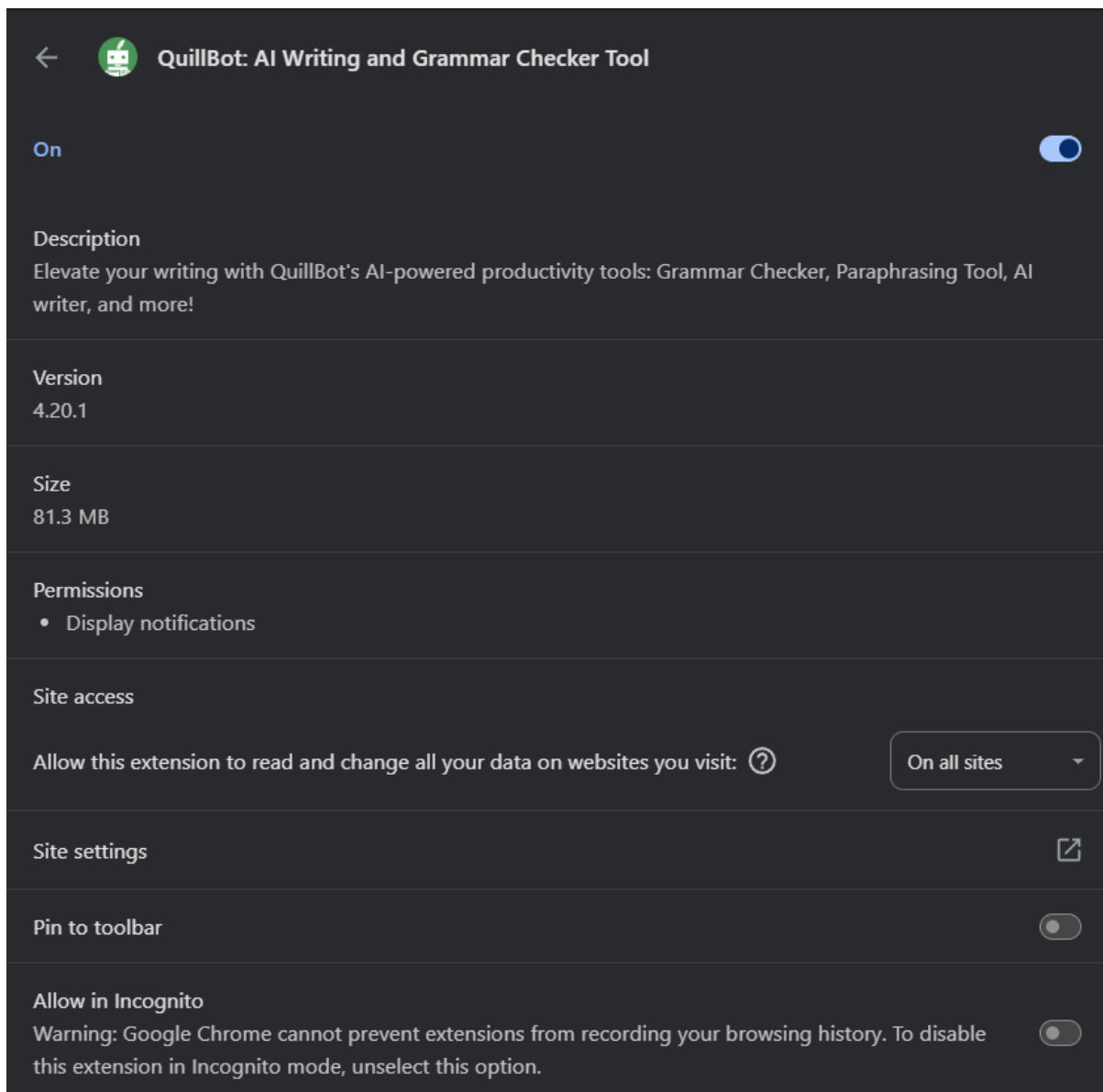
- **Unused:** I haven't had the opportunity to use this extension even once.
- **Lack of Functionality:** I remember once I got disconnected from the internet, and was using google docs, but it still didn't enable me to continue my work offline.
- **Bad Reviews:** 2.3-star rating and bad reviews by the user
- **Security Implications:** This extension seems to be suspicious, and I do not even remember installing it unlike the other 2 extensions.

I then clicked on **the Remove tab** and removed it. The following screenshot displays this:



4. Opened the QuillBot extension

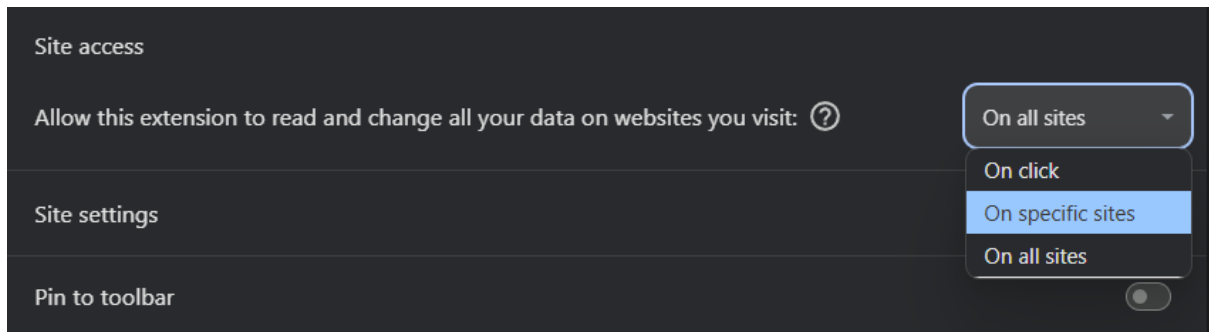
QuillBot enables me to check for any grammatical mistakes I make while typing something online. A very helpful tool for me.



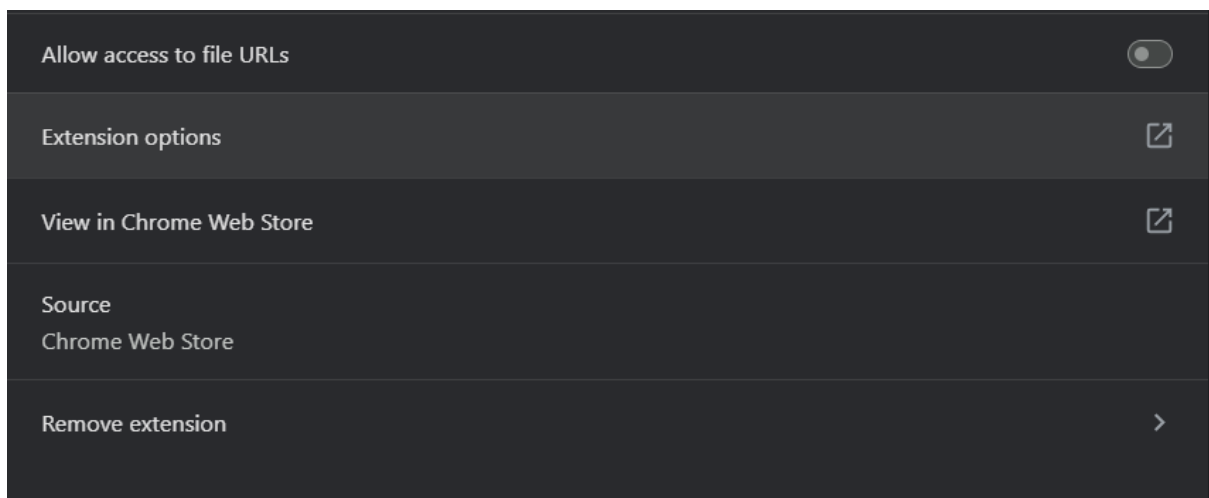
The permission required by this extension is only to **display notifications**. Within the Site access tab it can be found that this extension **has the access to read and change all my data on all the websites I visit**.

I find this tool very effective, yet it **shouldn't be authorized** to read and change my data on all websites like the financial web applications. I shouldn't allow QuillBot to read my financial transactions and the data I enter into the inputs available on the financial web-app like debit/credit card credentials, CVV or OTPs as they do not require any grammar check.

Therefore, **to limit the access** given to QuillBot I clicked on the drop-down menu currently showing 'On all sites'. Now I have the other two following options:



I chose **'On click'**, because it will grant me granular control over what data QuillBot can access and retrieve. This specific action is implemented on the grounds of a key security principle which is **"Least Privilege"**.



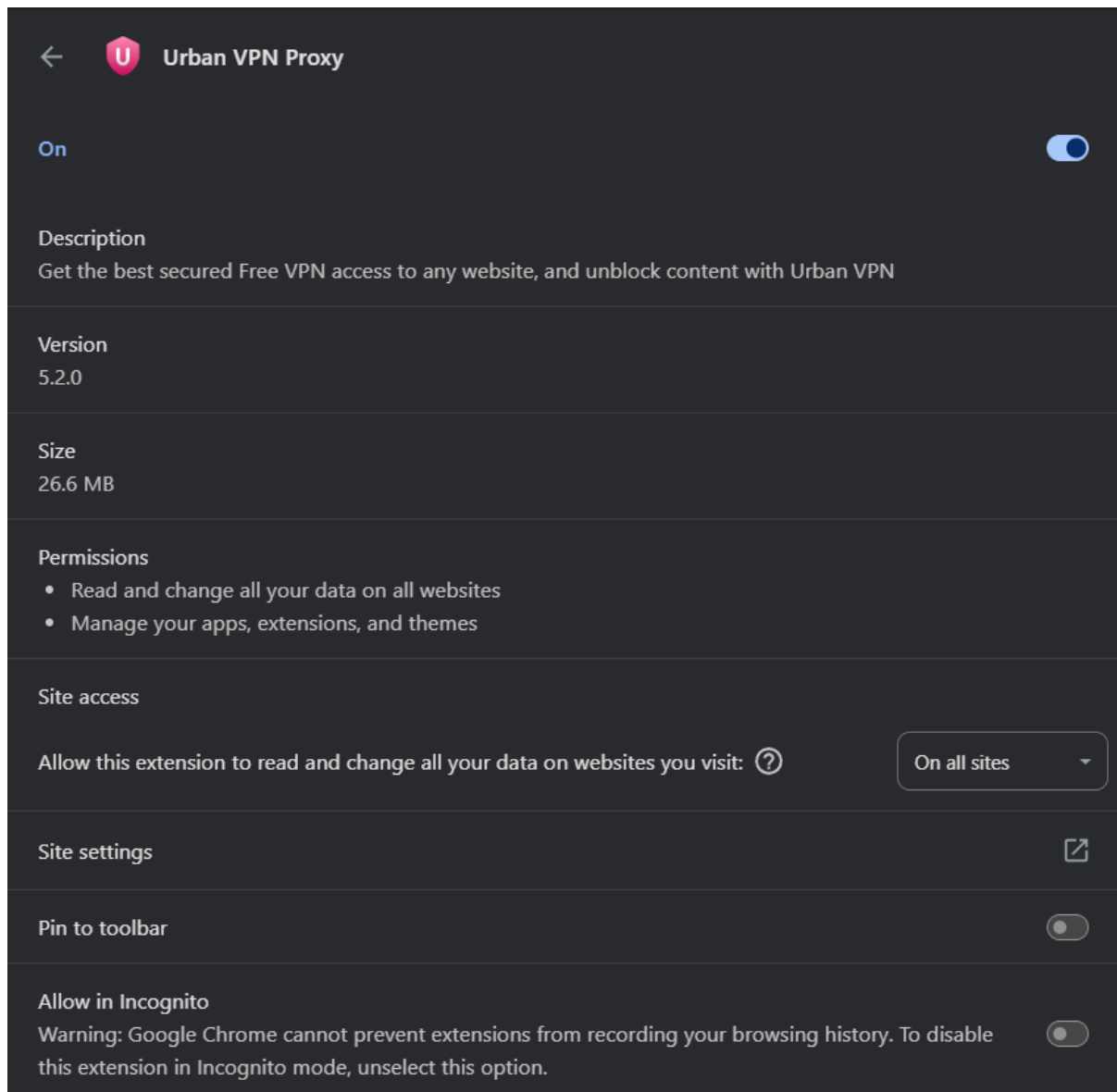
Then, I visited the chrome web store to **examine the reviews** of this extension. As shown in the screenshot below:



QuillBot has a star rating of **4.6 out of 5**, which is excellent and the user reviews regarding this extension are appreciative. So, after a little change in Site access I do not find any other security risks related to QuillBot therefore, **I decided to keep it.**

5. Opened the Urban VPN Proxy extension

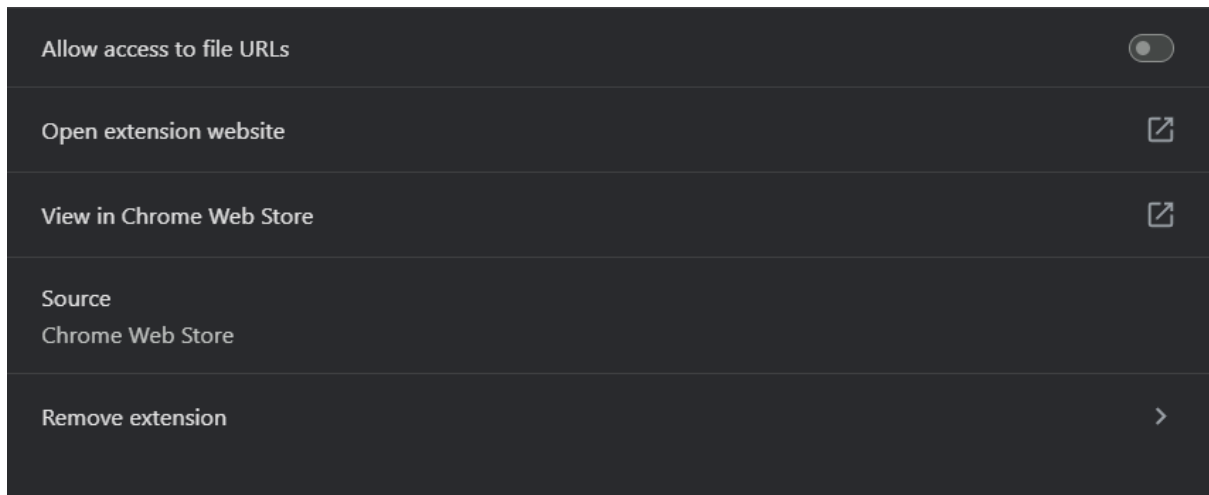
This extension provides VPN solution for free, and enables anonymity over the Internet. I do not use this tool quite often. Being the case, I only remember it using once.




The Urban VPN Proxy has **the following permissions:**

- Read and change all your data on all websites
- Manage your apps, extensions, and themes

Additionally, this extension also has the same Site access permissions as QuillBot had. Further I examined its reviews on the chrome web store.



 **Urban VPN Proxy** Remove from Chrome

Featured 4.7 ★ (48K ratings) Share

Extension Privacy & Security 5,000,000 users




4.7 out of 5 ★★★★★
48K ratings • Google doesn't verify reviews. [Learn more about results and reviews.](#)




Filter by
All reviews

Sort by
Recent

Language
English

Write a review

 carbon phyu ★★★★★ 5 Jun 2025
use full vpn
Was this helpful?  

 Ninh Nguyễn ★★★★★ 5 Jun 2025
NICE!!!
Was this helpful?  

The Urban VPN Proxy has a good star rating of **4.7 out of 5**. Moreover, the user reviews of this extension are remarkable. Anyways, I decided to remove this extension because of the following reasons:

- **Unused:** I haven't used this extension since a long time, neither do I have the need of having or using it.
- **Excessive Permissions:** This extension has been given a lot of permissions and site access, which I am not comfortable with.

6. Restarted the browser

However, I was unable to notice any changes after restarting the browser except for feeling a little improvement in the speed that's all.

7. The Hidden Dangers of Malicious Extensions

Browser extensions, while often useful, can be a gateway for malicious actors. These seemingly harmless add-ons can be weaponized to compromise your digital life in various ways.

Theft of Sensitive Information

Malicious extensions pose a significant threat by stealing your sensitive personal and financial information. By tricking you into granting extensive permissions, they can:

- Monitor all your Browse activity.
- Steal login credentials for *banking websites*, *credit card numbers*, and *private messages*.
- Log your keystrokes to capture everything you type.
- Capture screenshots without your knowledge.

This surreptitiously gathered data is then often sold on the dark web or used for ***identity theft*** and ***financial fraud***.

Active Harm to Your System and Accounts

Beyond just data theft, these extensions can actively harm your computer and online accounts. Their capabilities include:

- **Injecting Malware:** They can install harmful software like *ransomware*, which encrypts your files and demands a payment, or *spyware* that continuously monitors your activities.
- **Hijacking Resources:** Some extensions hijack your system's resources for activities like ***cryptocurrency mining***. This can drastically slow down your computer and increase electricity consumption.
- **Content Manipulation:** They can manipulate the content you see, redirecting you to *phishing websites* that mimic legitimate sites to trick you into revealing more personal information.

Deceptive Nature and Distribution

The deceptive nature of these extensions makes them particularly dangerous.

- They can be disguised as legitimate tools, such as *ad blockers* or *document converters*.
- They may be distributed through official browser web stores after bypassing initial security checks.
- In some cases, a legitimate extension can be sold to a new developer who then pushes a ***malicious update*** to its entire user base.

This evolving threat landscape highlights the importance of being cautious, carefully reviewing requested permissions, and regularly auditing your installed extensions to stay safe.