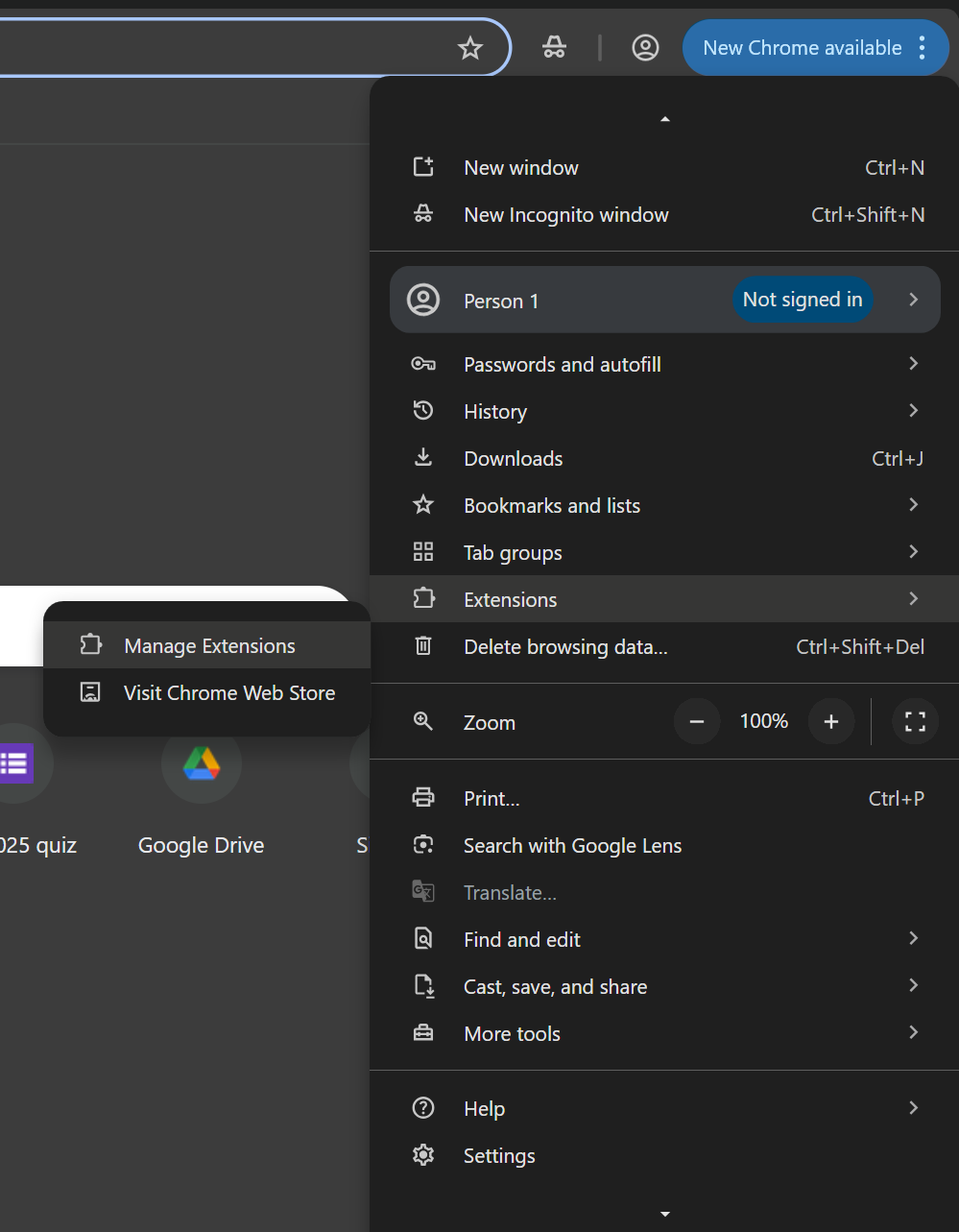
**Step-by-Step Instructions**

**1. Open Extension/Add-ons Manager**

* **Chrome:** Click the three-dot menu > *Extensions* > *Manage Extensions*  
  Or type: chrome://extensions/ in the address bar.

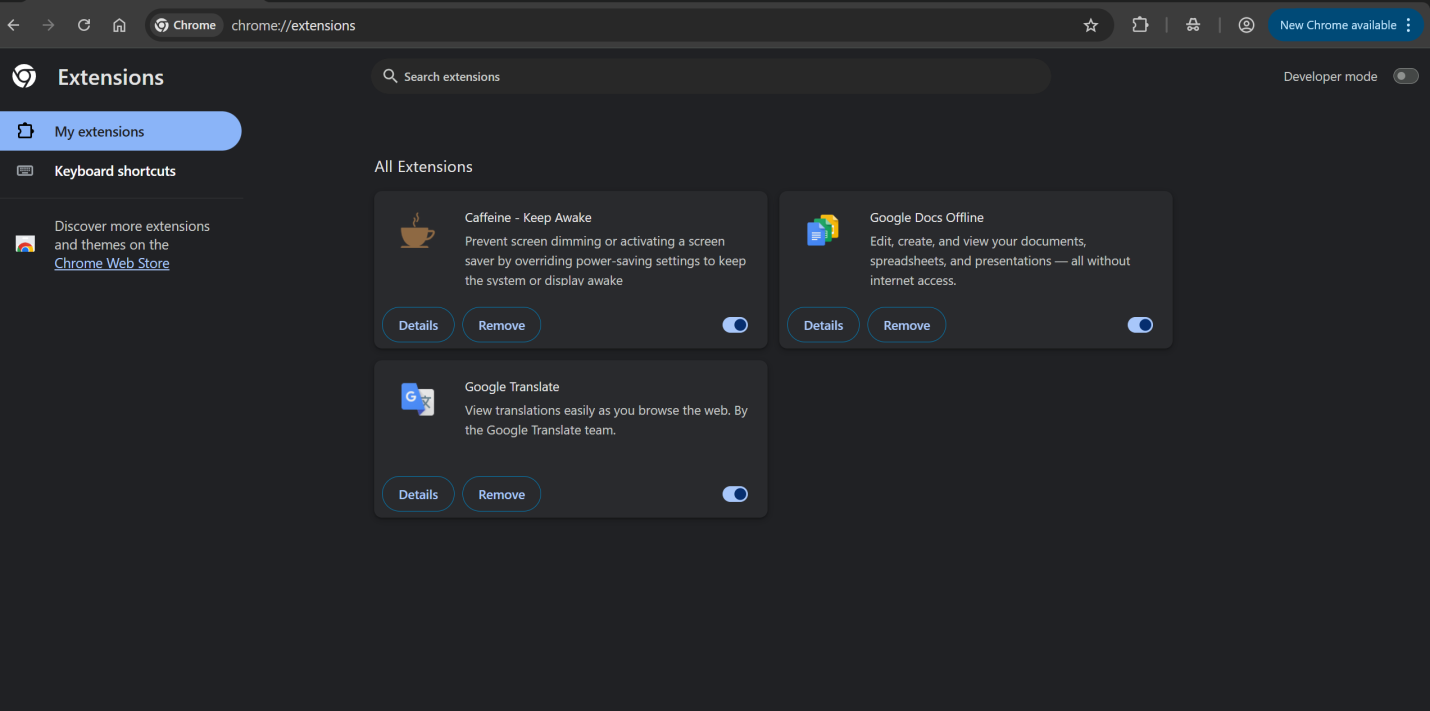


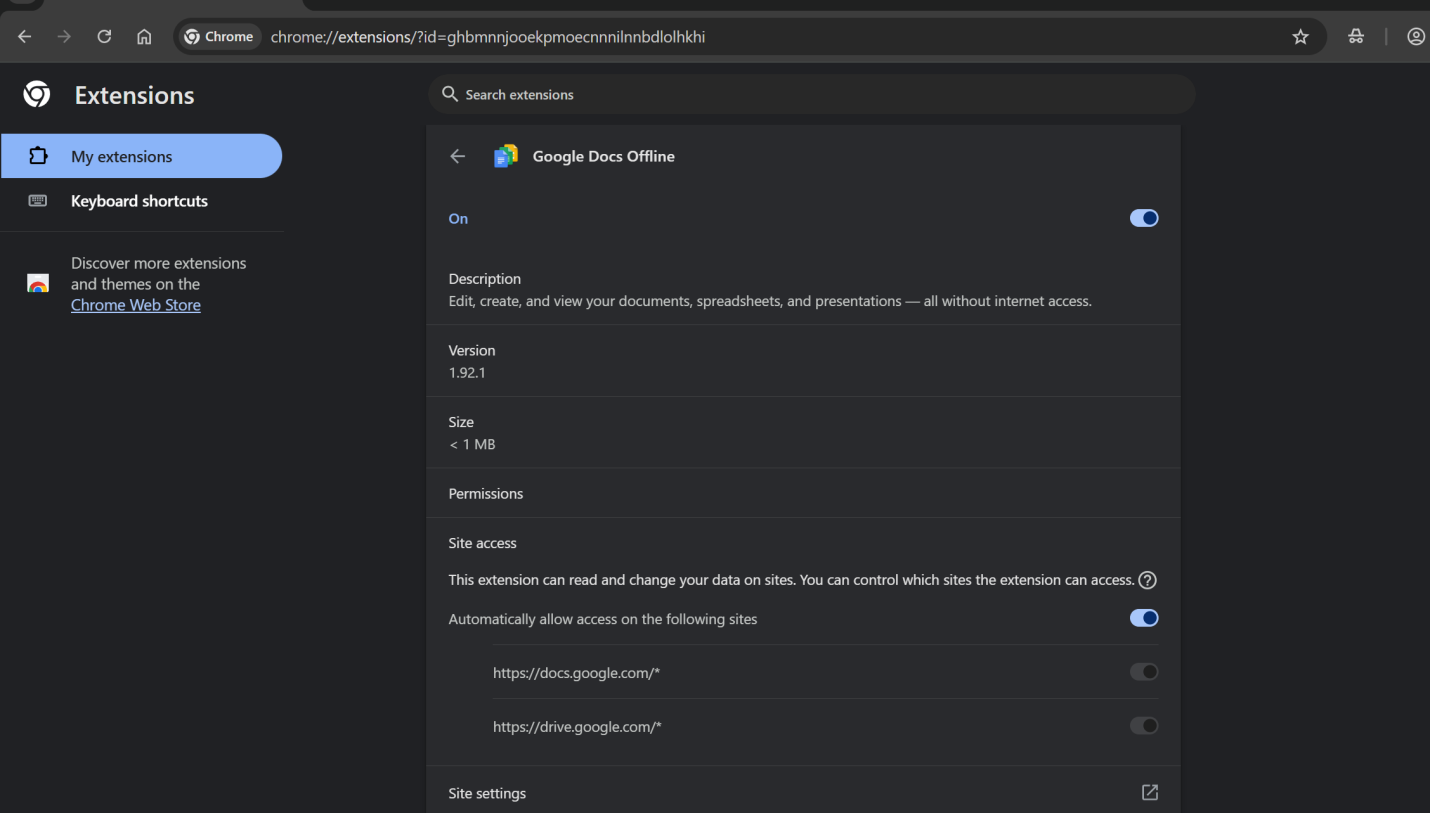
### 2. ****Review Installed Extensions****

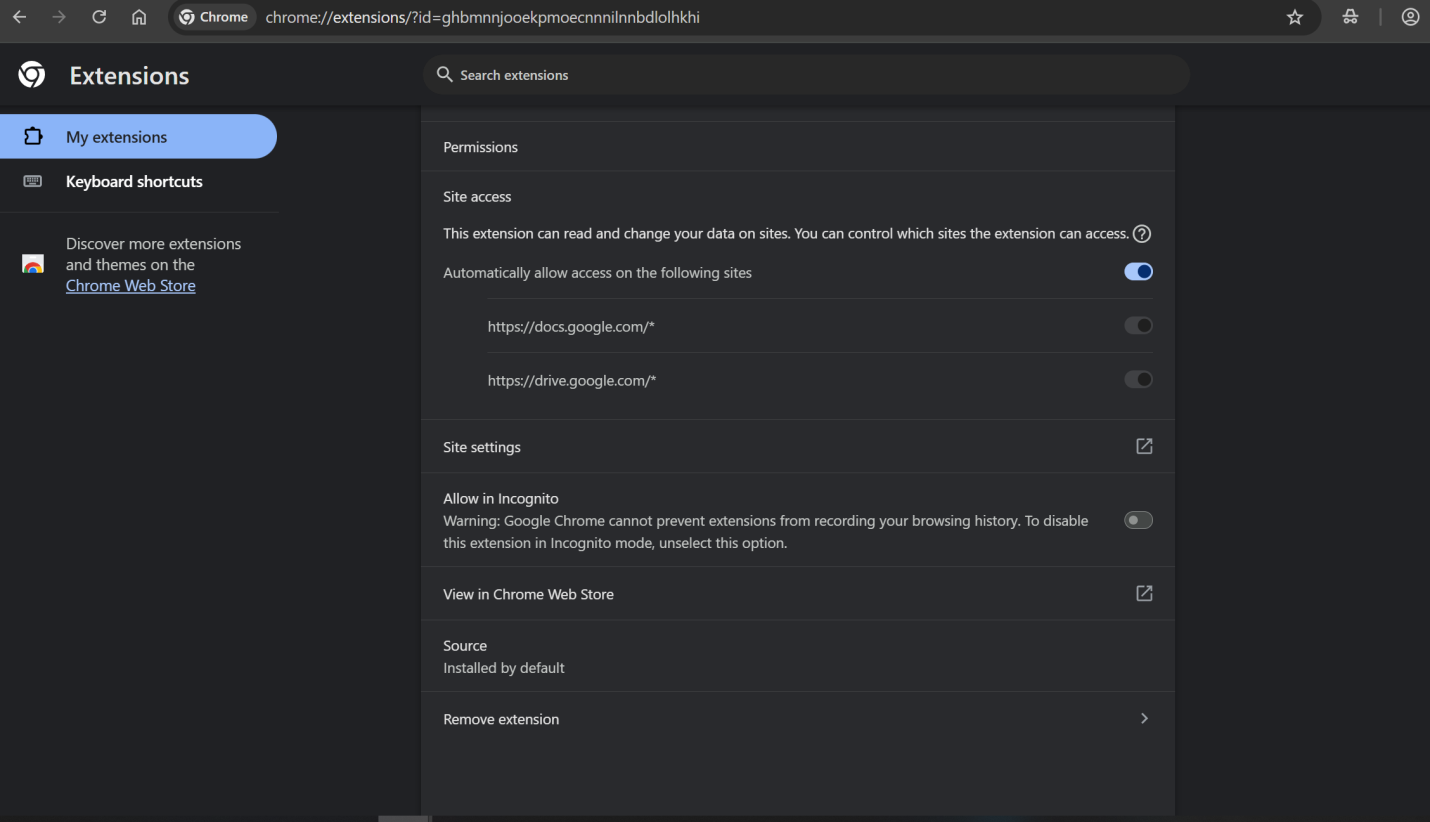
* Go through each extension name and description.

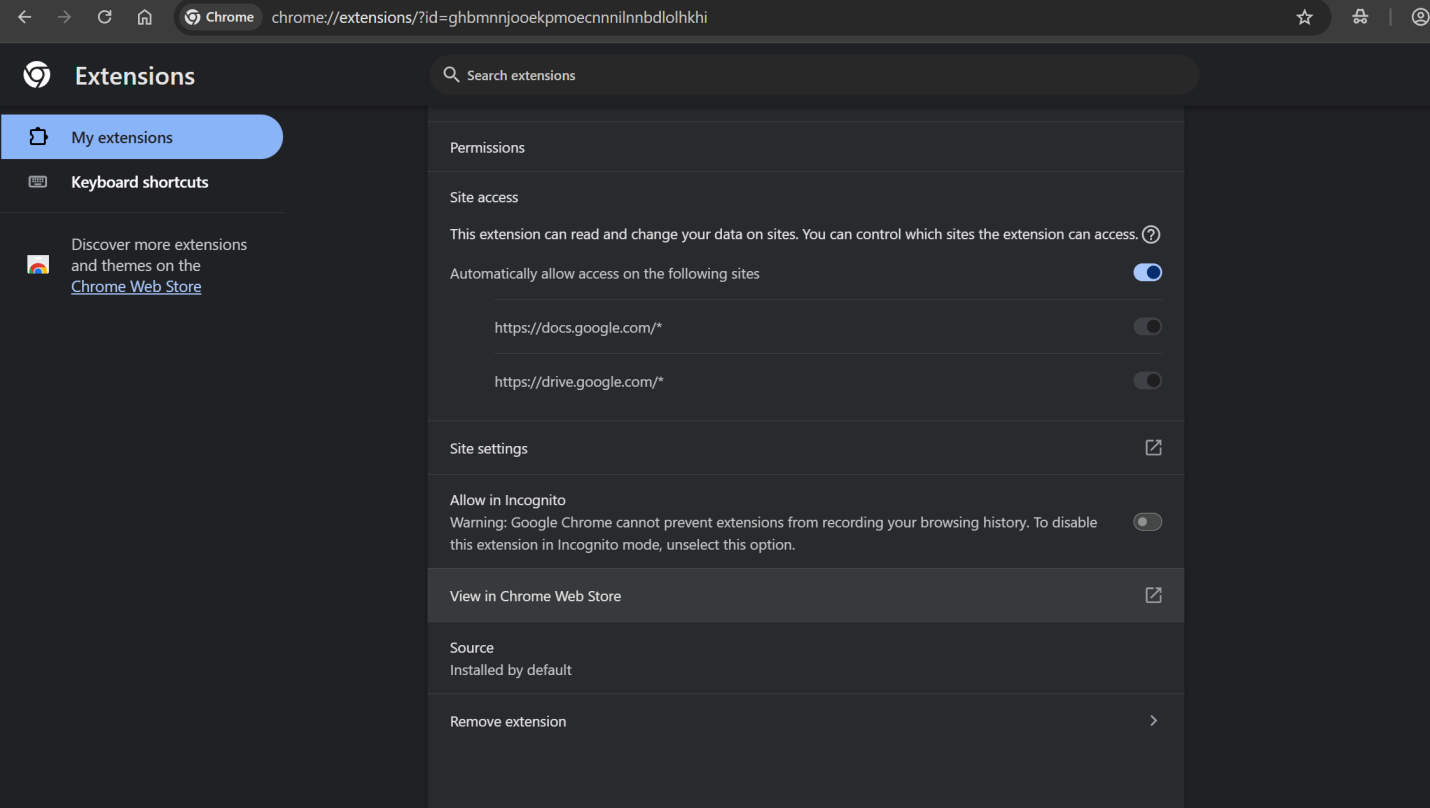
### 3. ****Check Permissions & Reviews****

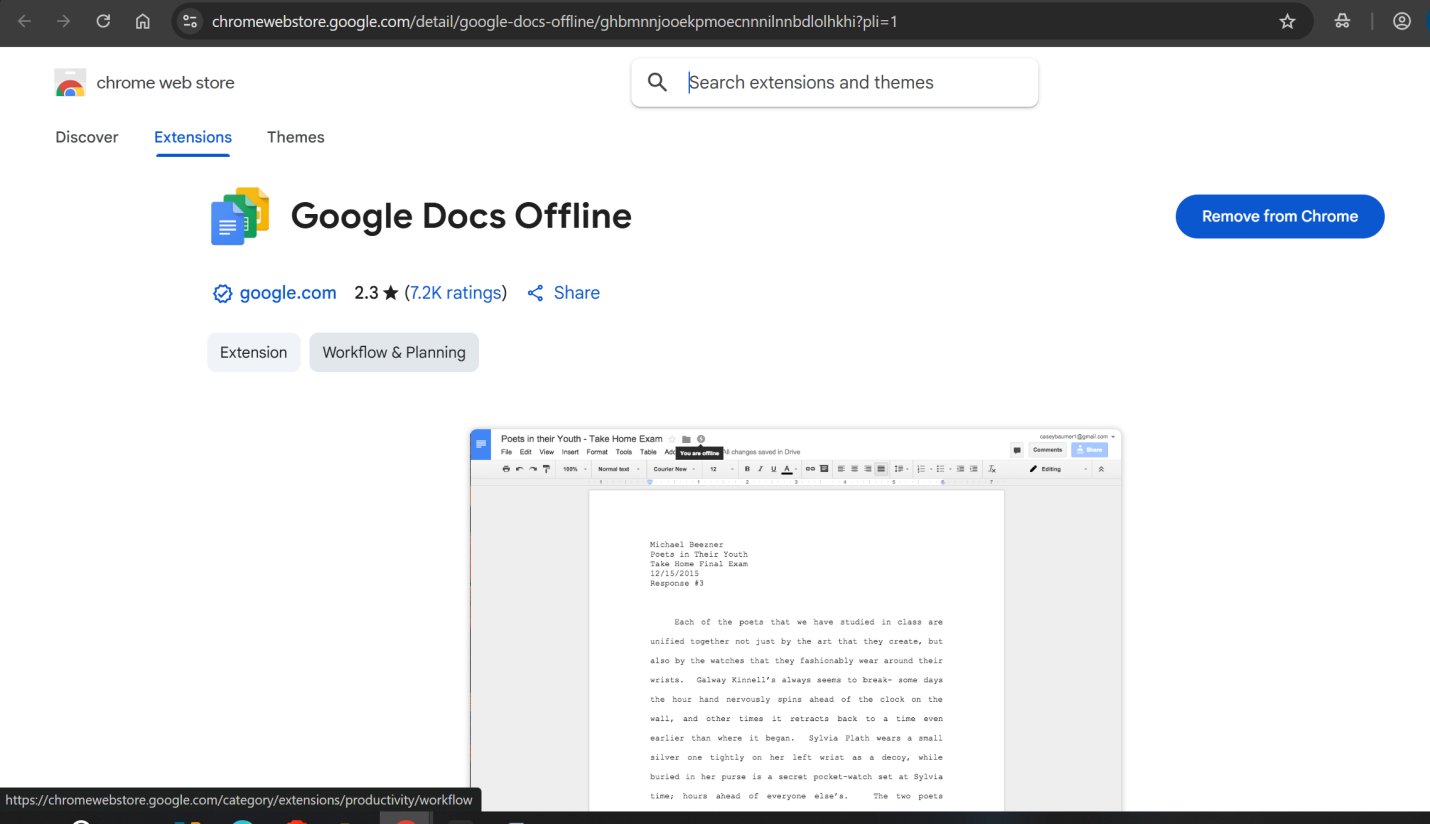
* Click “Details” (Chrome)
  + What permissions does it ask for (e.g., access to all your websites)?
  + Is it asking for more than it needs to function?
* Look it up in the Chrome Web Store:
  + Check user reviews.
  + Look for recent reports of malware or data harvesting.

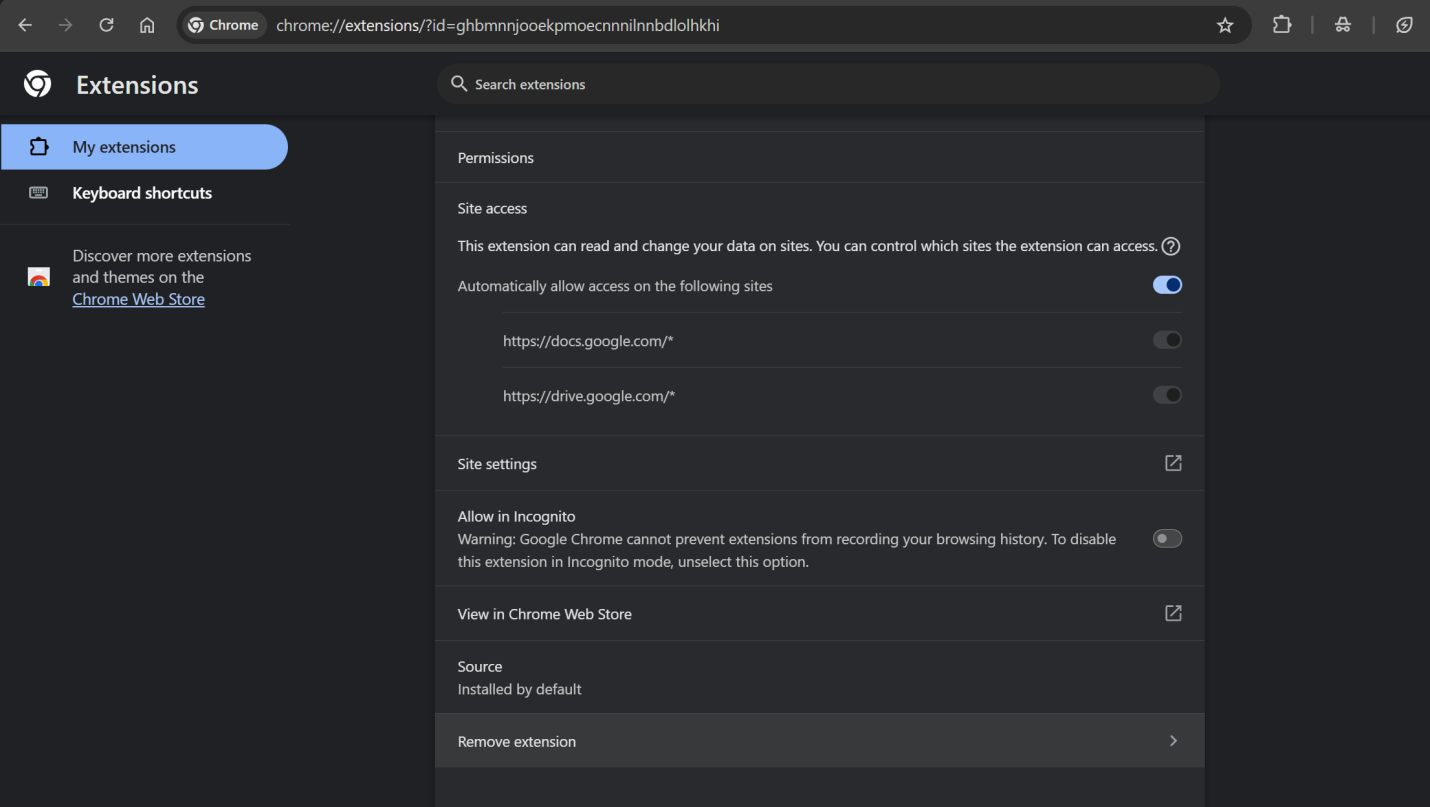


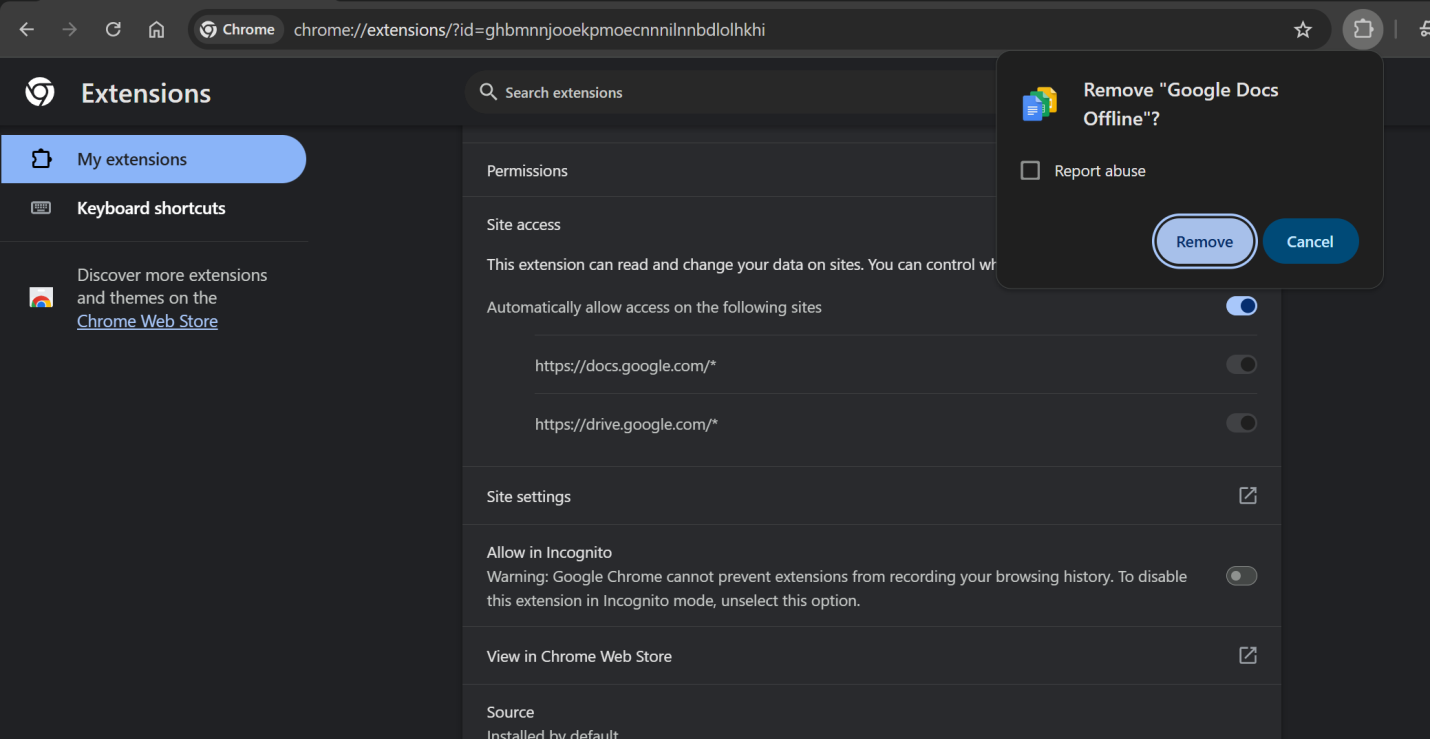


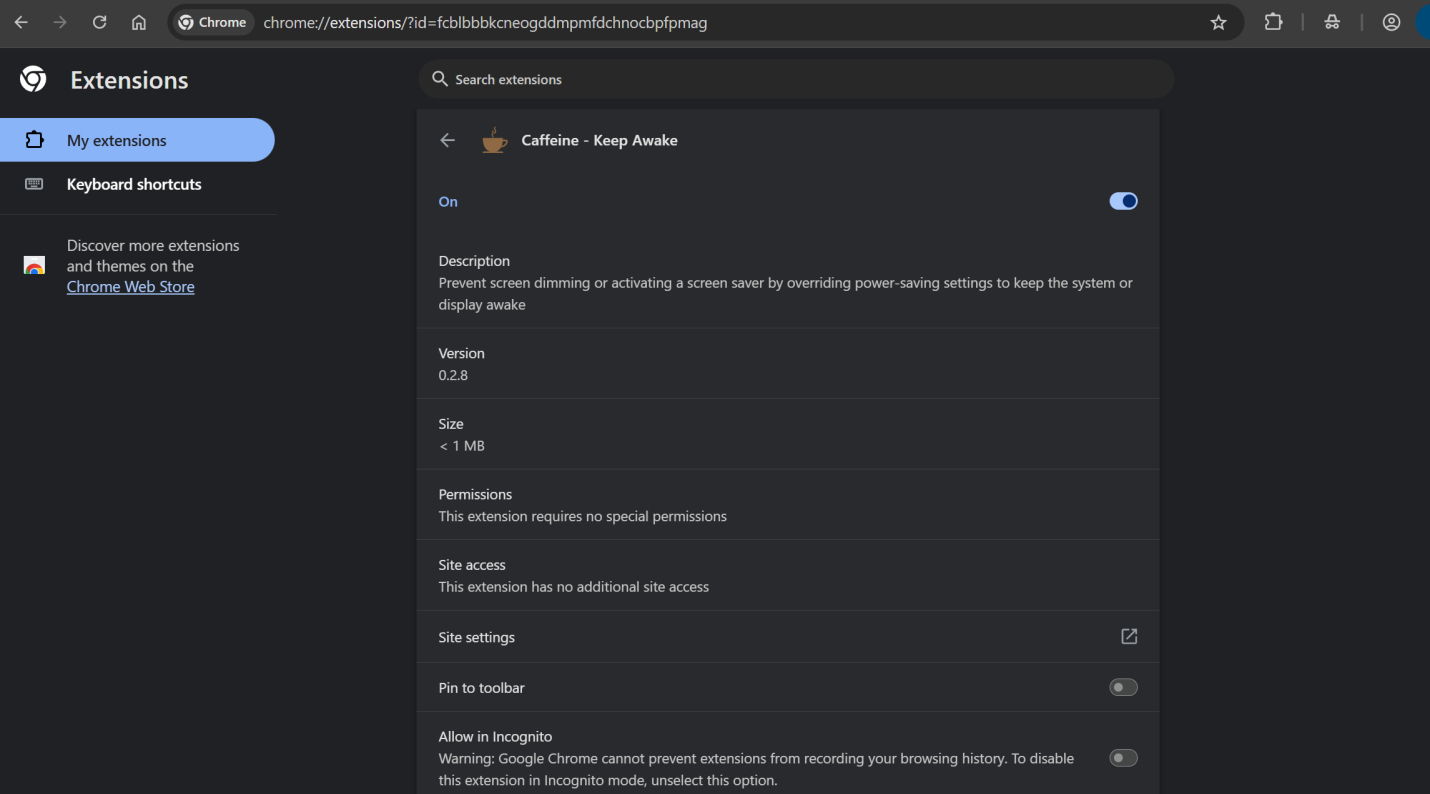


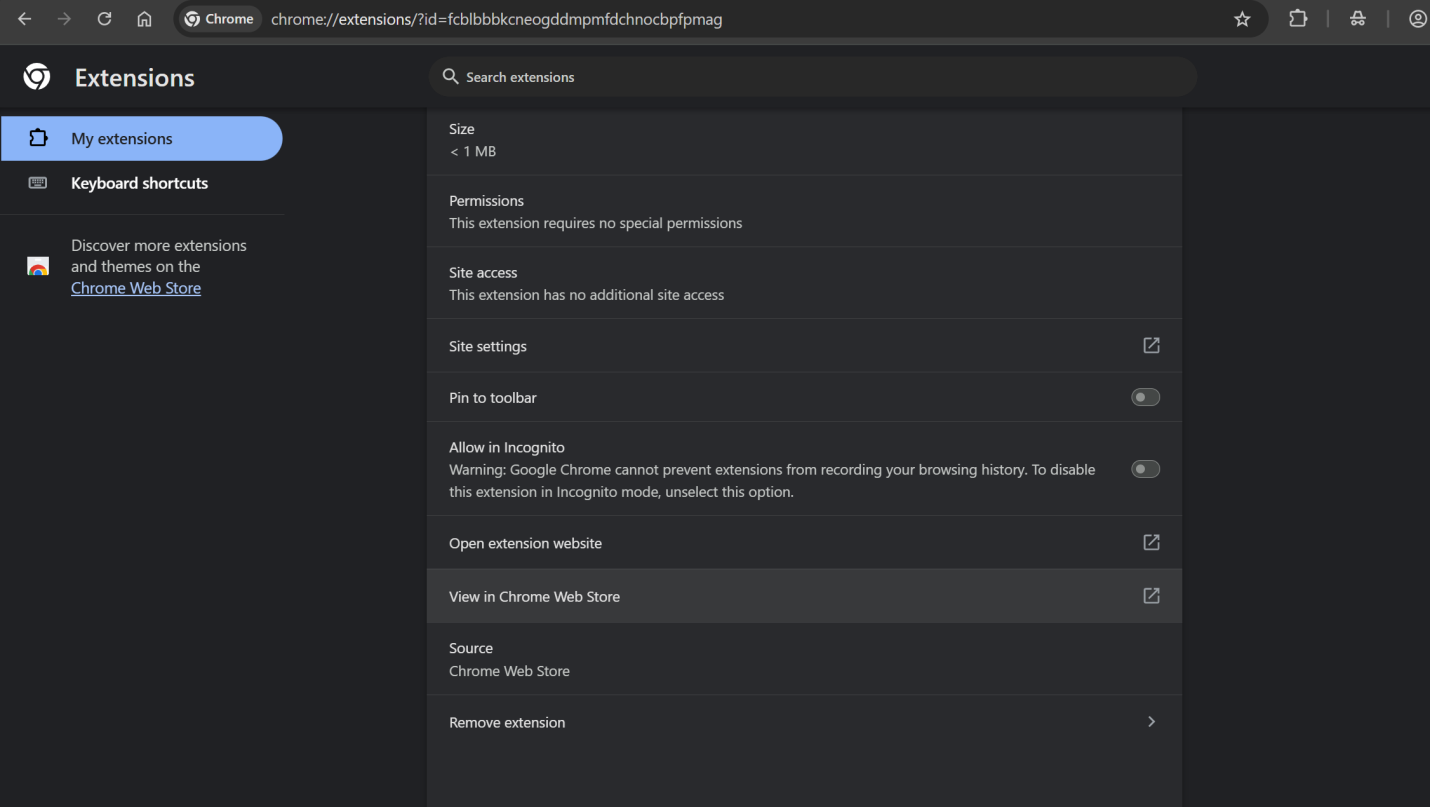


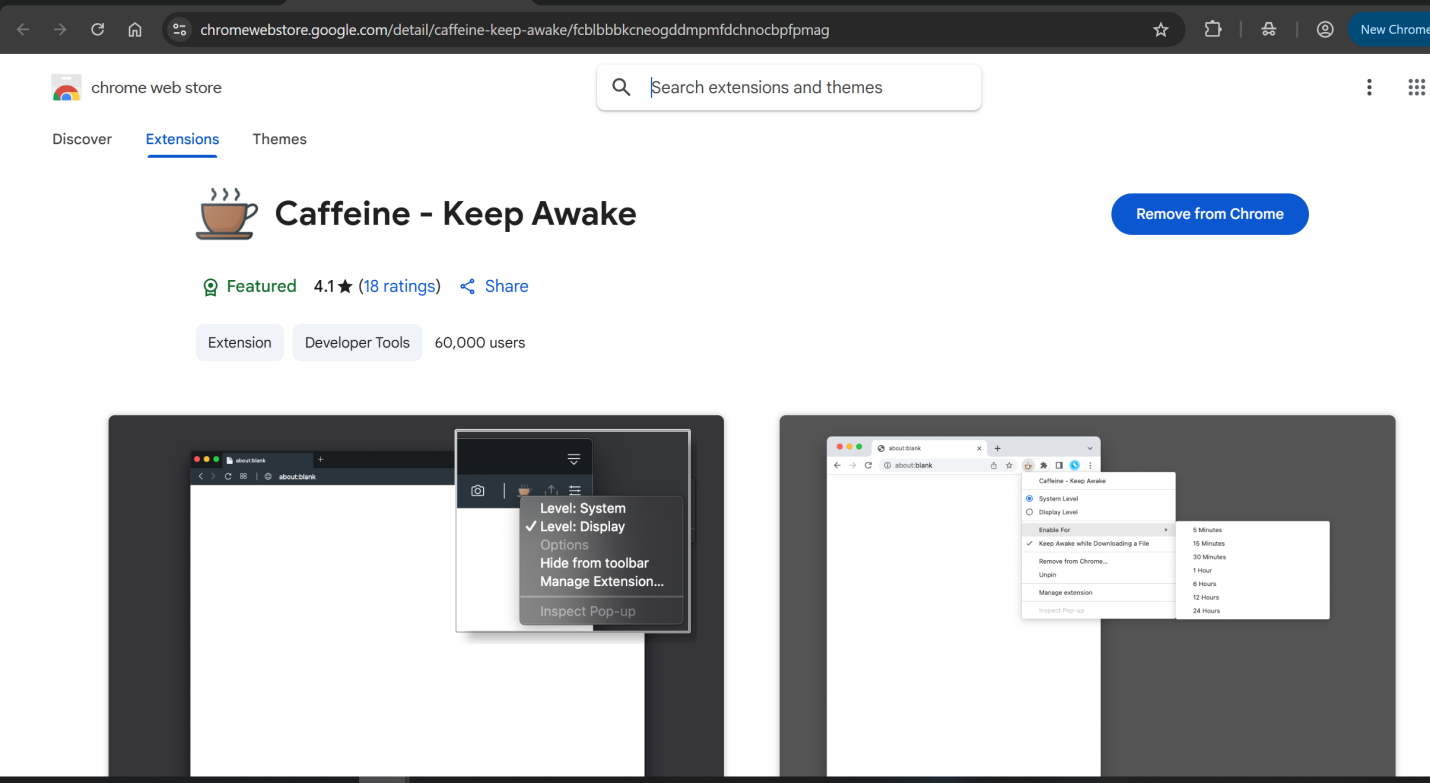












### 4. ****Identify Suspicious/Unused Extensions****

Red flags include:

* Poor ratings or no reviews.
* Unknown developer or vague description.
* Reports of aggressive ads, redirects, or data collection.
* You don’t remember installing it.

### 5. ****Remove Suspicious or Unused Extensions****

* Click “Remove” or trash icon next to the extension.
* Confirm deletion.

### 6. ****Restart Browser****

* Fully close and reopen your browser.
* Check if performance improves (faster loading, fewer pop-ups, less CPU usage).

### 7. ****How Malicious Extensions Harm Users****

* They can:
  + Steal passwords or personal data.
  + Hijack search engines or inject ads.
  + Track browsing history.
  + Act as spyware or install other malware.