**TASK – 7**

## IDENTIFY AND REMOVE SUSPICIOUS BROWSER EXTENSIONS.

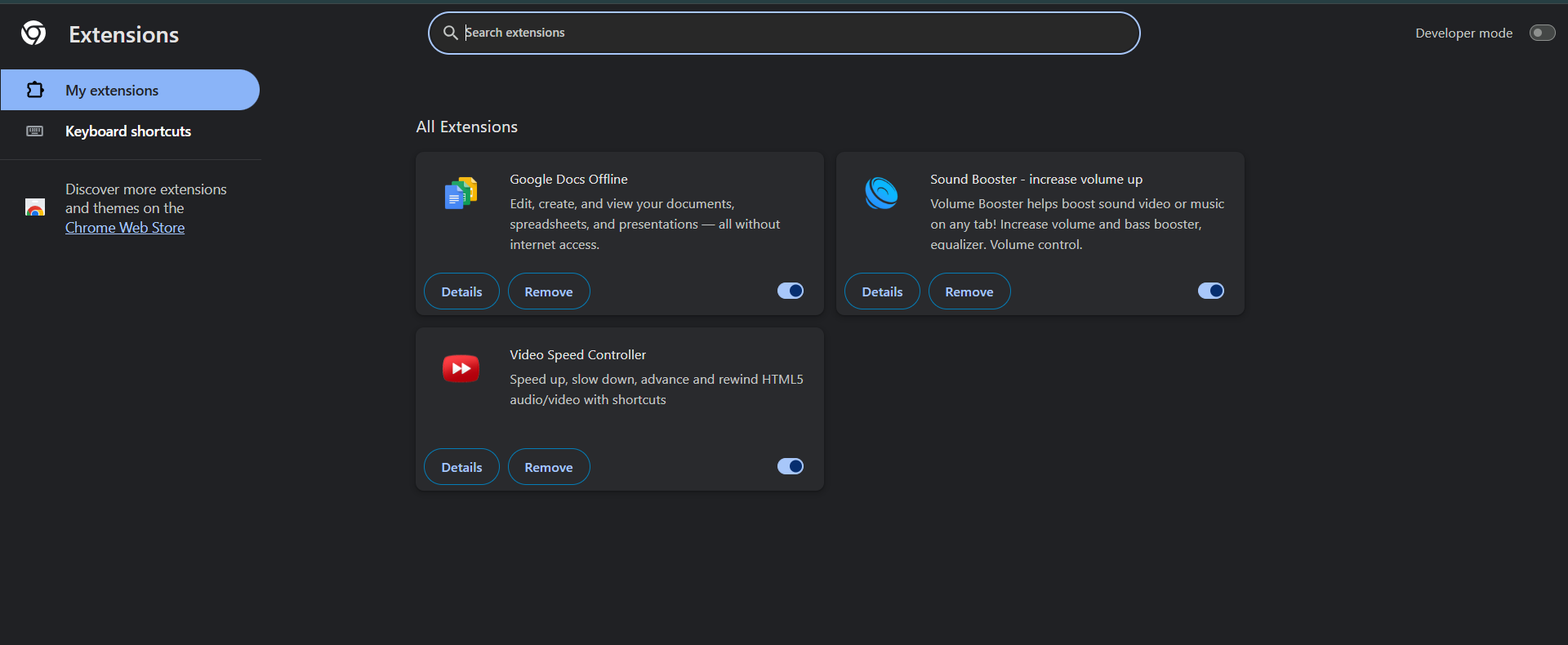
**Taking a Look at My Browser Extensions :**

So I had this cybersecurity assignment where I needed to dig into my Chrome extensions, and honestly? It was way more eye-opening than I expected. The whole point was to see what I had lurking in there, figure out if anything looked sketchy, and get a better sense of what these little add-ons might be doing behind the scenes.

**Here's How I Went About It :**

I started by typing chrome://extensions into my browser—you know, that hidden page most of us never think to check. Then I went through each extension one by one, asking myself: "Do I actually use this? What's it really doing?"

The real detective work happened when I clicked into the details for each one. That's where you see all the permissions they're asking for, and let me tell you, some of them are pretty bold about what they want access to.



**Google Docs Offline** seemed totally fine—it's Google's own thing and only touches their services. Makes sense.

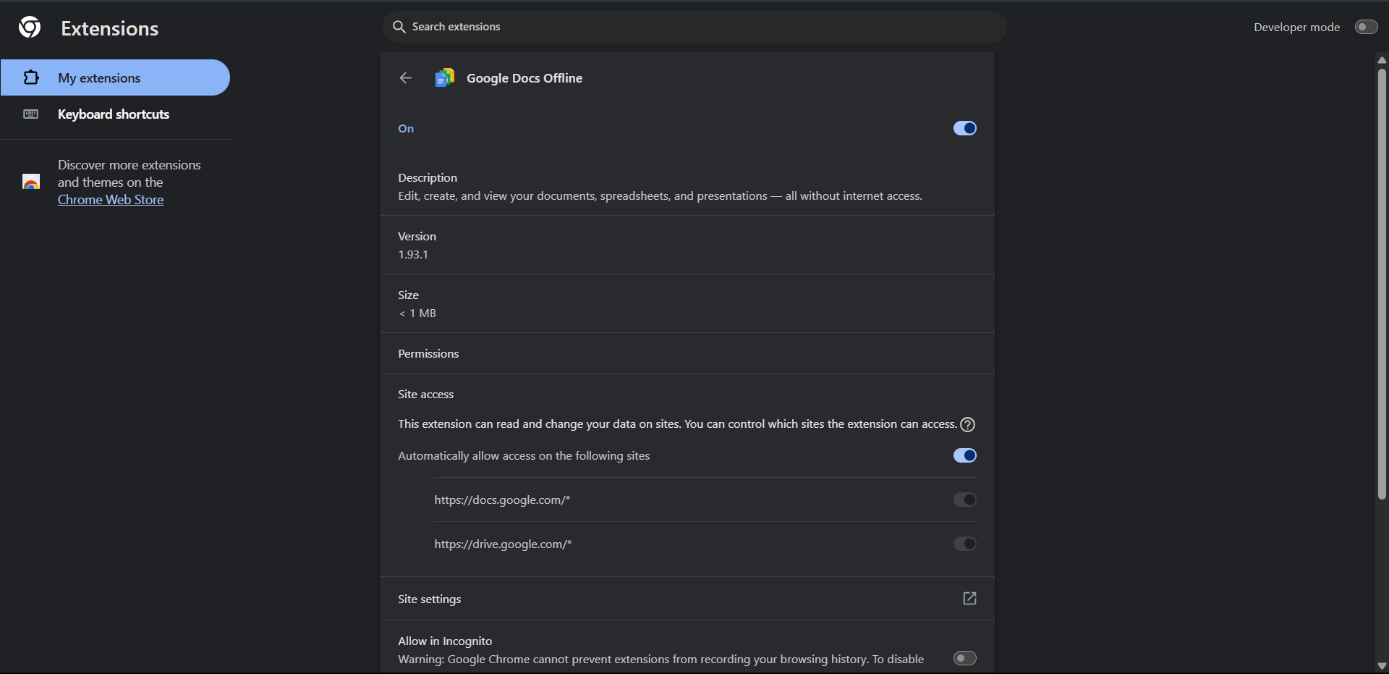
But then there's **Sound Booster**. This little guy wants permission to read and change data on *every single website* I visit. For a volume booster? That raised some red flags for me.

**Video Speed Controller** was in the same boat—asking for way more access than it seems to need just to speed up YouTube videos.

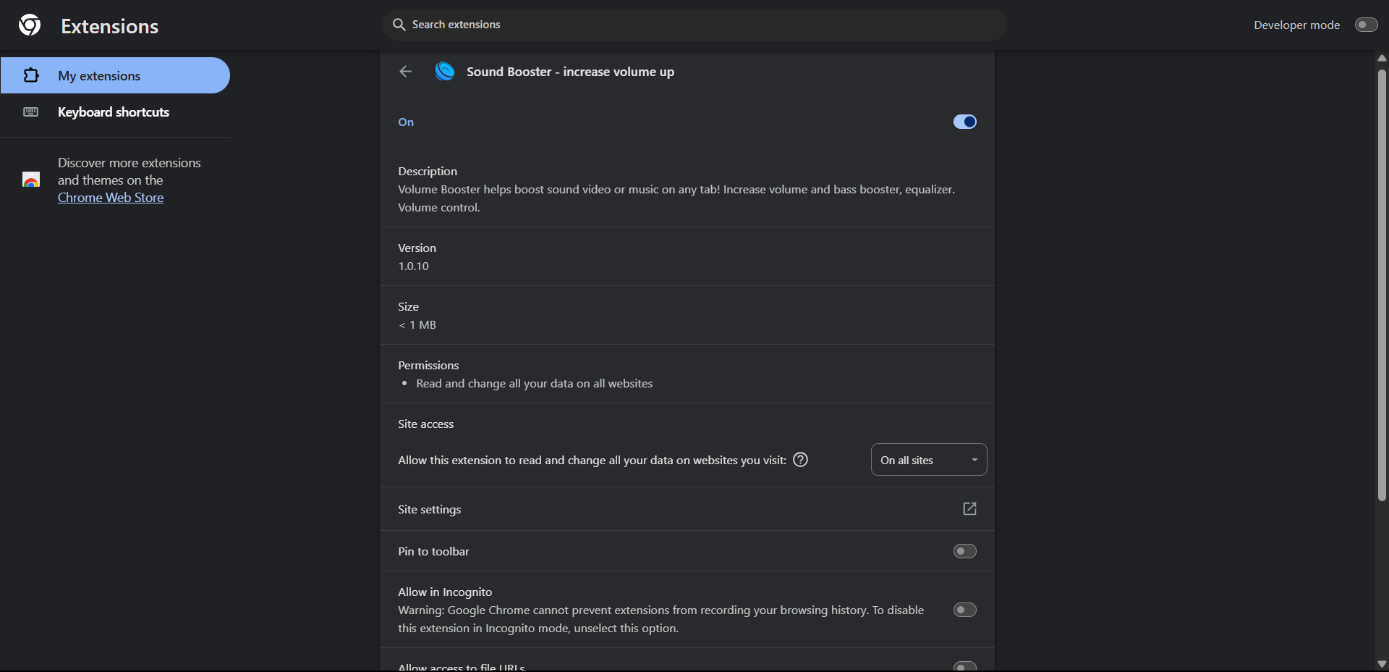
I didn't go on a deletion spree right away, but I definitely made some mental notes. After poking around, I restarted my browser and called it a day.

**What I Found :**

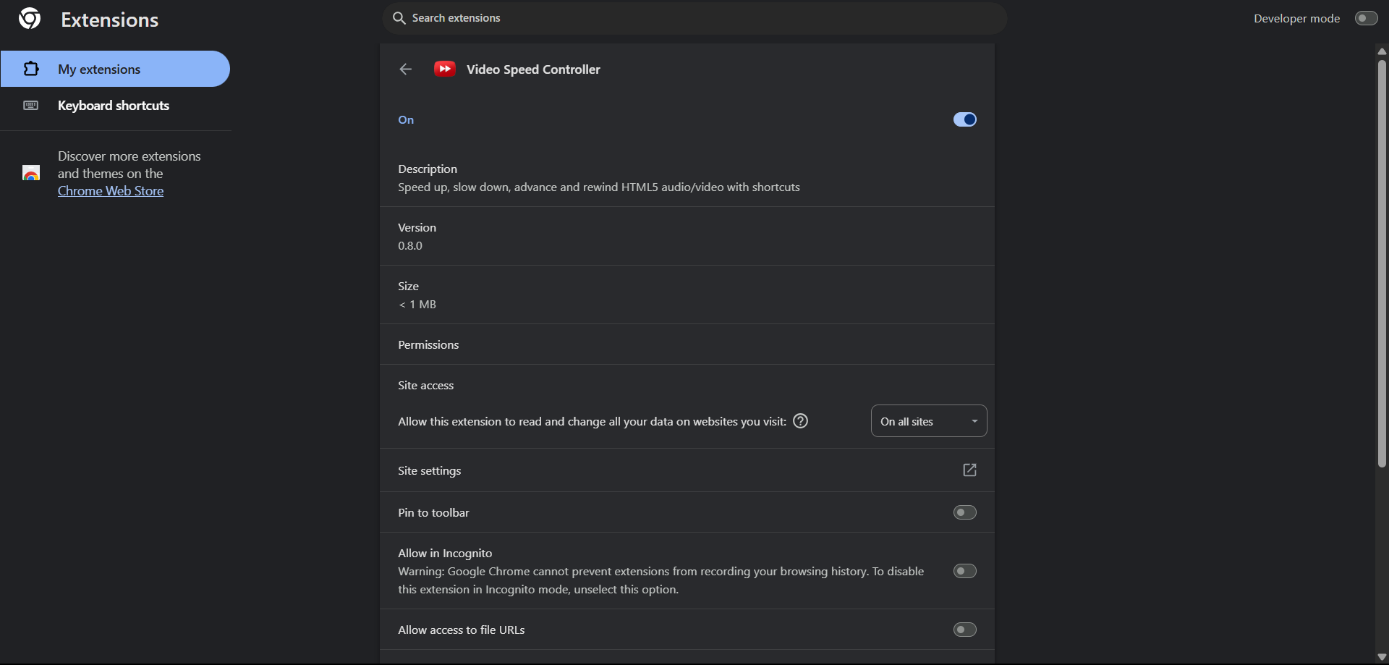
**Google Docs Offline** This one's straightforward—it lets me work on Google Docs when my internet decides to take a break. Since it's made by Google and only works with their stuff, I'm not worried about it.



**Sound Booster** Look, I get it—sometimes you need that extra volume boost when you're watching something with terrible audio. But asking for access to read and change data on every website? That feels like overkill. It's probably fine, but it's the kind of thing that could go sideways if it wasn't legitimate.



**Video Speed Controller** I actually use this one all the time (who has time to watch everything at normal speed?), and it's pretty popular, so I'm keeping it. Still, those broad permissions make me a little uneasy.



**⚠️ Harmful/Suspicious Browser Extensions & Their Risks ( AI info).**

* **Hola VPN**  
  ▸ Misused user bandwidth and turned users into nodes in a peer-to-peer network.  
  ▸ Could be exploited for illegal traffic or botnet activity.
* **Superfish**  
  ▸ Injected advertisements into webpages and weakened HTTPS encryption.  
  ▸ Created serious security vulnerabilities.
* **SpeakIt!**  
  ▸ Originally a text-to-speech tool, but was later found injecting ads and tracking user behavior.  
  ▸ Violated user privacy.
* **Hover Zoom**  
  ▸ Collected private browsing data and injected affiliate tracking codes.  
  ▸ Used user data for profit without consent.
* **User-Agent Switcher and Manager**  
  ▸ Installed malicious scripts that committed click fraud in the background.  
  ▸ Drained system resources and violated ad policies.
* **Fake Flash Player Extensions** (e.g., “Flash Player+”)  
  ▸ Pretended to be legitimate Flash support tools.  
  ▸ Often contained crypto miners or spyware.
* **DataSpii Extensions** (e.g., Hover Zoom, SuperZoom, SpeakIt!)  
  ▸ A group of 8+ extensions revealed in 2019 to collect browsing history, usernames, and more.  
  ▸ Caused a major privacy scandal.
* **AutoplayStopper (Fake versions)**  
  ▸ Some fake versions mimicked the real one but included ad injectors and trackers.  
  ▸ Installed malware in disguise.