Introduction

As part of my cybersecurity internship, this task focused on something many people — including myself — often overlook: browser extensions. At first glance, browser extensions seem harmless. They're small tools meant to enhance functionality and convenience. But through this task, I discovered how easily they can become a major security threat if misused or left unchecked.

This task taught me how to critically assess each extension I've installed, examine the permissions they're granted, and understand how attackers can exploit them to steal data or hijack sessions. It was a great blend of technical insight and awareness-building.

What I Did – Step-by-Step

Step 1: Opened My Browser's Extension Manager

I used Google Chrome for this task and typed chrome://extensions/ into the address bar. This opened a list of all the extensions currently installed in my browser.

Step 2: Reviewed Each Extension

For every extension, I checked:

Its name and purpose

The permissions it requested

When it was last updated

Its Web Store reviews and ratings

Whether I actually used it anymore

I paid special attention to permissions like:

"Read and change all your data on the websites you visit"

"Read your browsing history"

"Access clipboard data"
These kinds of permissions can be risky, especially if the extension doesn't clearly need them.

Step 3: Identified Unnecessary or Suspicious Extensions
Out of the 8 extensions I had installed, I found:

2 that I hadn’t used in a long time

1 that had poor reviews and suspicious permissions

1 that was legit but could be replaced with a safer, lighter alternative

Step 4: Uninstalled Unwanted Extensions
I removed the following:

Price Compare Tool – Requested unnecessary permissions; reviews mentioned data leaks.

Screenshot Pro – Hadn't used it in months; requested permission to read all data.

Emoji Keyboard – Fun, but unnecessary and accessed clipboard.

I only kept essential extensions like:

A trusted ad blocker

Grammarly

Google Docs Offline

Step 5: Restarted My Browser
After cleanup, I restarted Chrome. Not only did it load slightly faster, but I also felt better knowing that I had more control over what had access to my browser activity.

What I Learned
Before this task, I never thought much about browser extensions. I installed them and forgot about them. But now I understand that:

Browser extensions can act like spyware if they're malicious.

Some look innocent but collect browsing data, keystrokes, or passwords in the background.

Not all extensions go through strict vetting, even in official web stores.

It’s important to treat extensions like any software — evaluate, update, or remove regularly.

Best Practices I’ll Follow Moving Forward

Always read the permissions before installing an extension.

Prefer open-source or highly-rated tools with transparent developers.

Avoid installing multiple extensions that serve similar purposes.

Uninstall anything I don’t use — better safe than sorry.

Keep extensions updated, just like apps or antivirus software.

Enable developer mode periodically to review hidden background activity.

Extensions I Removed
Extension Name Reason for Removal
Price Compare Tool Suspicious reviews; overreaching permissions
Screenshot Pro Unused and had "read all site data" permission
Emoji Keyboard No longer needed; accessed clipboard data

Final Thoughts
This task made me realize that even seemingly harmless things like browser extensions can introduce risk into our digital lives. Being in cybersecurity isn't just

about defending against hackers — it's also about making small, conscious choices every day to stay secure.

Cleaning up my extensions was a simple task, but it taught me a valuable lesson: never blindly trust anything that has access to your data.