

TASK - 7

Objective: Learn to spot and remove potentially harmful browser extensions.

Step 1. Open your browser's extension/add-ons manager.

The method varies slightly by browser.

Google Chrome:

Click the three vertical dots in the top-right corner → More tools → Extensions.

Or, type chrome://extensions/ into the address bar and press Enter.

Mozilla Firefox:

Click the three horizontal lines in the top-right corner → Add-ons and themes.

Or, type about:addons into the address bar and press Enter.

Microsoft Edge:

Click the three horizontal dots in the top-right corner → Extensions.

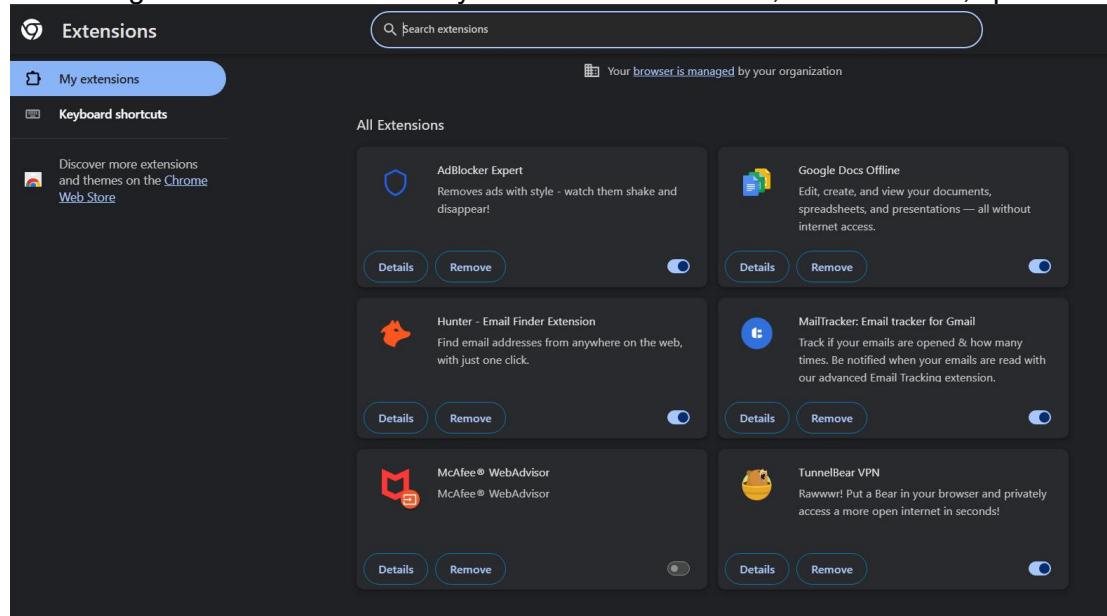
Or, type edge://extensions/ into the address bar and press Enter.

Apple Safari:

Safari → Settings (or Preferences) → Extensions.

Step 2 : Review the Extensions or Add-ons

I am using different extension in my browser like adblocker,email trackers, vpn etc.

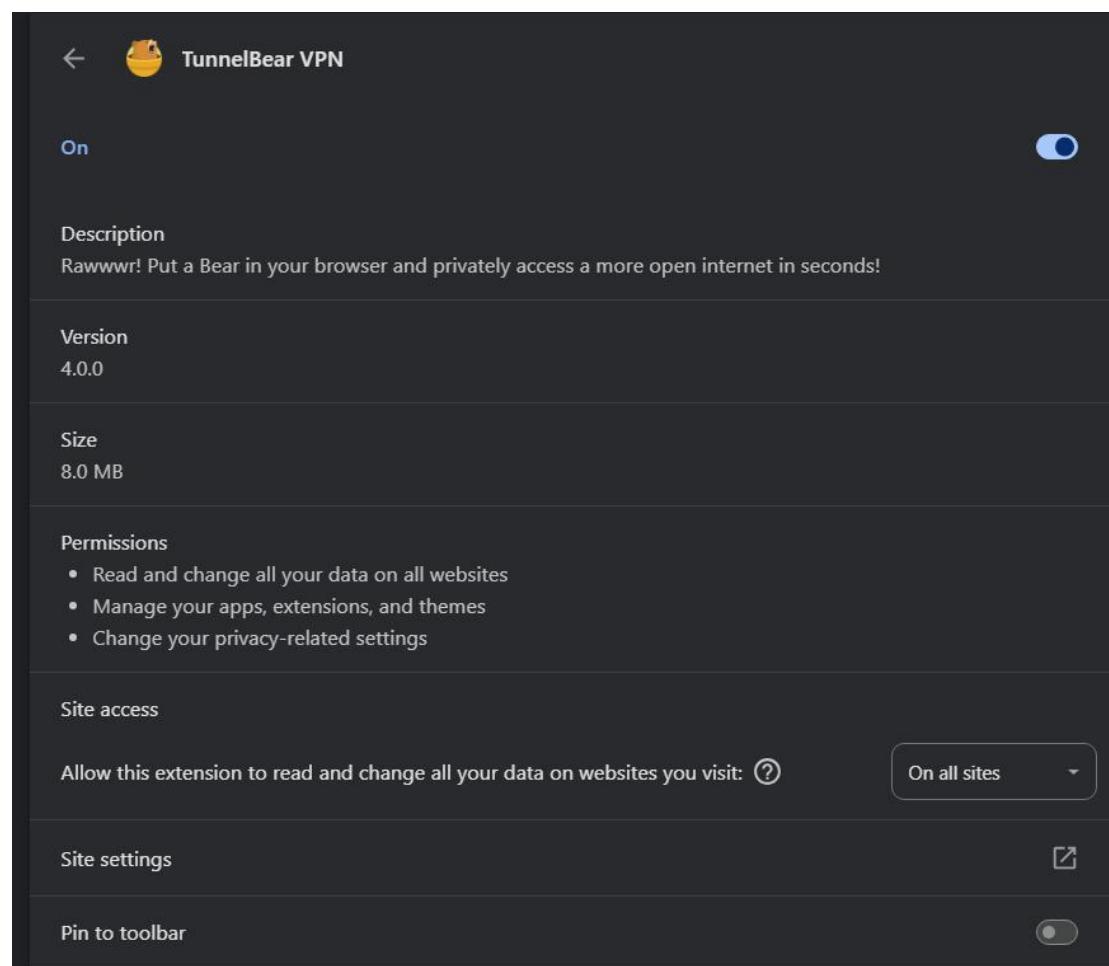


Step 3: Check Permissions and Reviews for Each Extension

This is the most critical step for identifying potential threats.

Click on each extension in the list to see its details.

Review Permissions: Look for a section called "Permissions," "Details,".



This extension is used by 10 million users .

It has the rating of 4.6 out of 5 .

Benefits:

Reduce the ability for websites, advertisers and ISPs to track your browsing Secure your browser on public WiFi

Get around blocked websites

Connect to a lightning fast private network with connections to 20 countries

 Hunter - Email Finder Extension

On

Description
Find email addresses from anywhere on the web, with just one click.

Version
3.1.4

Size
3.3 MB

Permissions

- Read your browsing history

Site access

Allow this extension to read and change all your data on websites you visit: [?](#)

Site settings 

Pin to toolbar

This extension is used by 700k users.

It has rating of 4.7 out of 5.

Benefits :

Find email addresses from anywhere on the web, with just one click.

Hunter for Chrome lets you find immediately who to contact when you visit a website.

The screenshot shows the settings page for the AdBlocker Expert extension. At the top, there's a back arrow and the extension's logo. The status is set to "On" with a blue toggle switch. Below that is a "Description" section stating "Removes ads with style - watch them shake and disappear!". The "Version" is listed as 1.0.0. The "Size" is 8.2 MB. Under "Permissions", it says "Block content on any page". The "Site access" section allows reading and changing data on all sites, with a dropdown menu set to "On all sites". The "Site settings" and "Pin to toolbar" options are present with their respective toggle switches. A note about "Allow in Incognito" mentions that Google Chrome cannot prevent extensions from recording browsing history, with a toggle switch currently off.

This extension is used by 100k+ users .

It has 4.5 rating out of 5.

Benefits:

- Timed ad viewing with automatic hiding
- Blocks intrusive pop-ups and overlays after the fair view period
- Stops tracking scripts and malicious ads completely
- Works across all websites and platforms
- Lightweight with minimal impact on performance

Step 3 : Remove Suspicious or Unnecessary Extensions

Identify any unused or suspicious extension form your chrome because a lot of extensions are malicious , this can extract and steal our data without noticing .

Step 4 : Research How Malicious Extensions Can Harm Users

Malicious browser extensions can cause a variety of problems:

Data Theft: They can steal sensitive information you type into websites, including passwords, credit card numbers, and personal details (keylogging).

Ad Injection: They can inject unwanted, malicious, or fraudulent ads into the web pages you visit.

Browser Hijacking: They can change your default search engine, homepage, or new tab page without your consent, often to a phishing site or one filled with ads.

Tracking & Profiling: They can track your entire browsing history, building a detailed profile of your interests, habits, and online behavior to sell to data brokers.

Cryptojacking: They can use your computer's resources to mine cryptocurrencies without your knowledge, slowing down your system.

Malware Distribution: They can be used as a gateway to download and install more severe malware onto your computer.

Summary :

I have removed adblocker expert because there is no need of and it looks some suspicious for me .

And I also removed tunnelbear vpn . it may have lot of features but there may chance of data theft because it will read all the data when browsing , so it may be malicious extension but instead of this I am using protonvpn which a most trusted free vpn service provider.