**ELEVATE LAB TASK 7** – Browser Extensions,

A brief report on how to Install, identify, use and remove Browser Extensions.

**Objective** – Learn to install and use of extension spot harmful and useful extensions remove harmful extensions.

Key concept Learn – Browser security, Extension, Permission, malware.

**Introduction**

What is Browser extension?

**A browser extension is a small piece of software that adds features and functionality to your web browser, enhancing your browsing experience.**

**Definition and Functionality**

A browser extension is essentially a software module that allows users to customize their web browsers. These extensions can add new features, modify existing functionalities, or enhance the user interface.

**How They Work**

Browser extensions interact with the browser's core functionality using technologies like HTML, CSS, and JavaScript. They can access specific APIs provided by the browser, allowing them to modify web pages, automate tasks, and interact with the browser's user interface. For example, an extension might add a button to the toolbar that performs a specific action when clicked.

**Tools and Requirements**

In this analysis I am using chrome browser version -

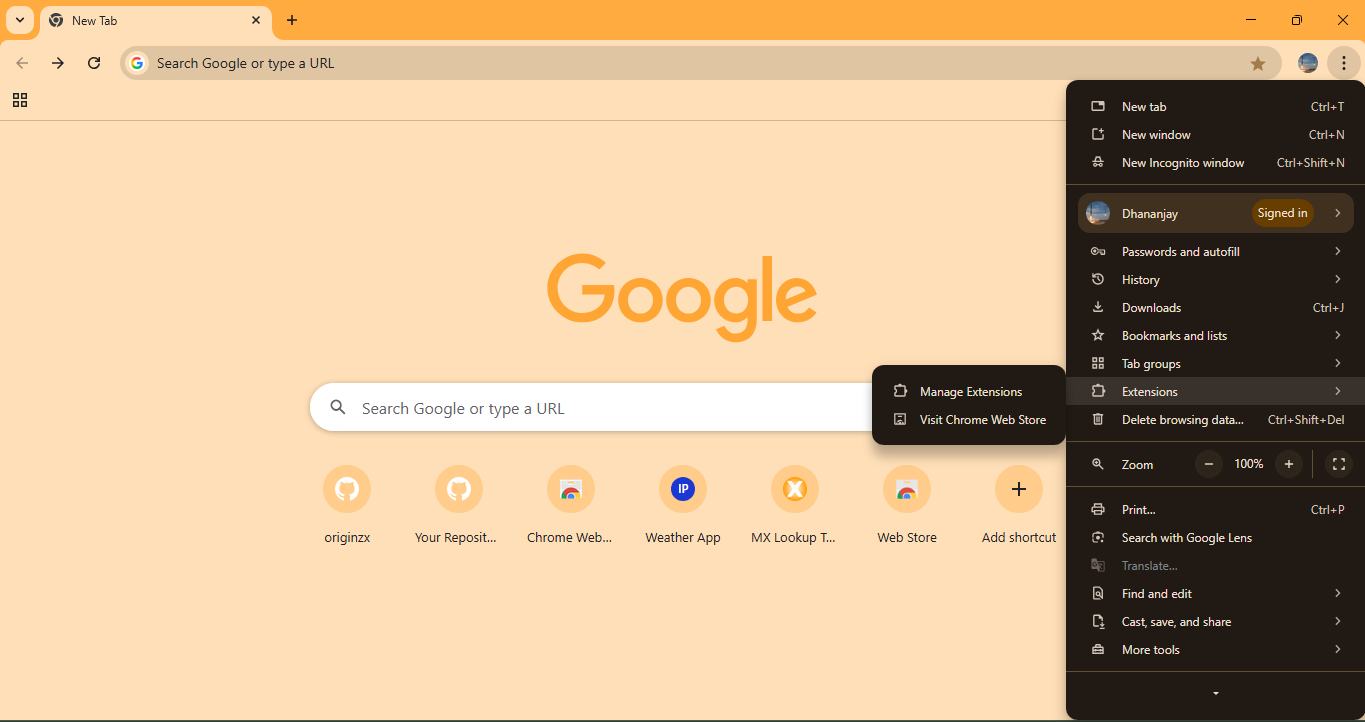
To work with extension analysis we need a web browser like MS edge or Chrome browser, Safari or Fire Fox any one of them.

Procedure

Installing a Browser extension

For Chrome Browser –

Simply open chrome click on Customize and control commonly known as three dot at right side corner above,



This will show many option you simply go to Extensions click on it

After clicking you will see two new option

Manage Extensions

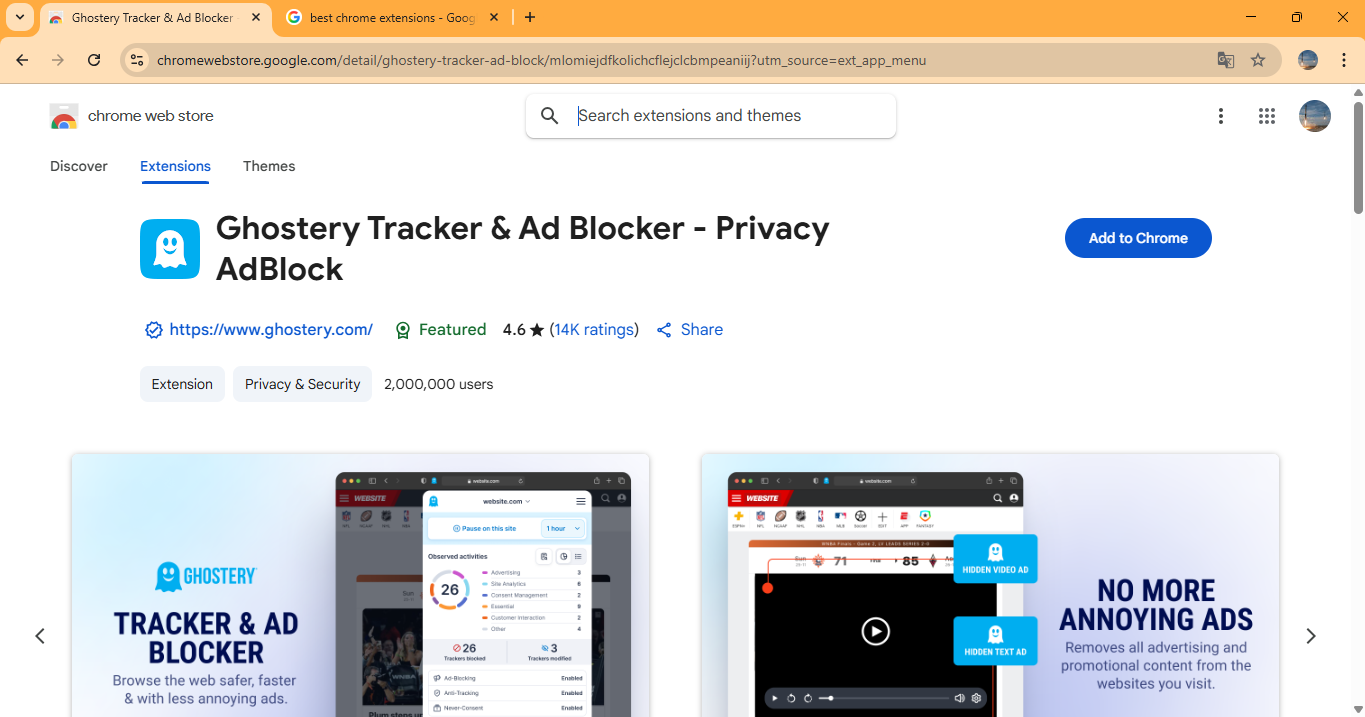
Visit chrome web store

For installation we click in visit chrome web store after click on it you will redirected to welcome page of chrome web browser there you can search for your useful or favourite extension

I recommend some useful extension to improve productivity, security and privacy

1. Task management
2. Password management
3. Grammarly
4. uBlock origin
5. Zapier
6. Ghostery
7. Lastpass

Here we will search and try to download an extension name Ghostery.

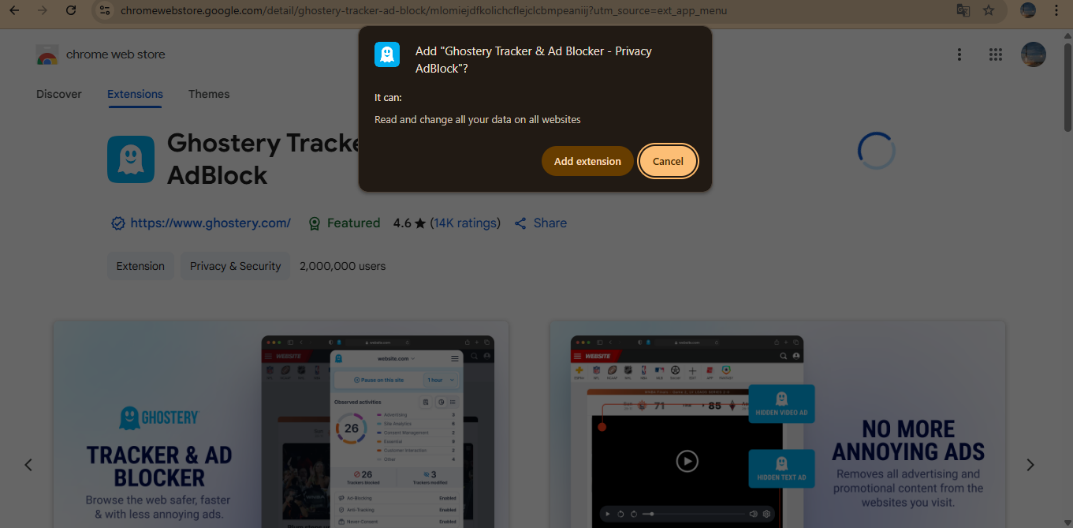


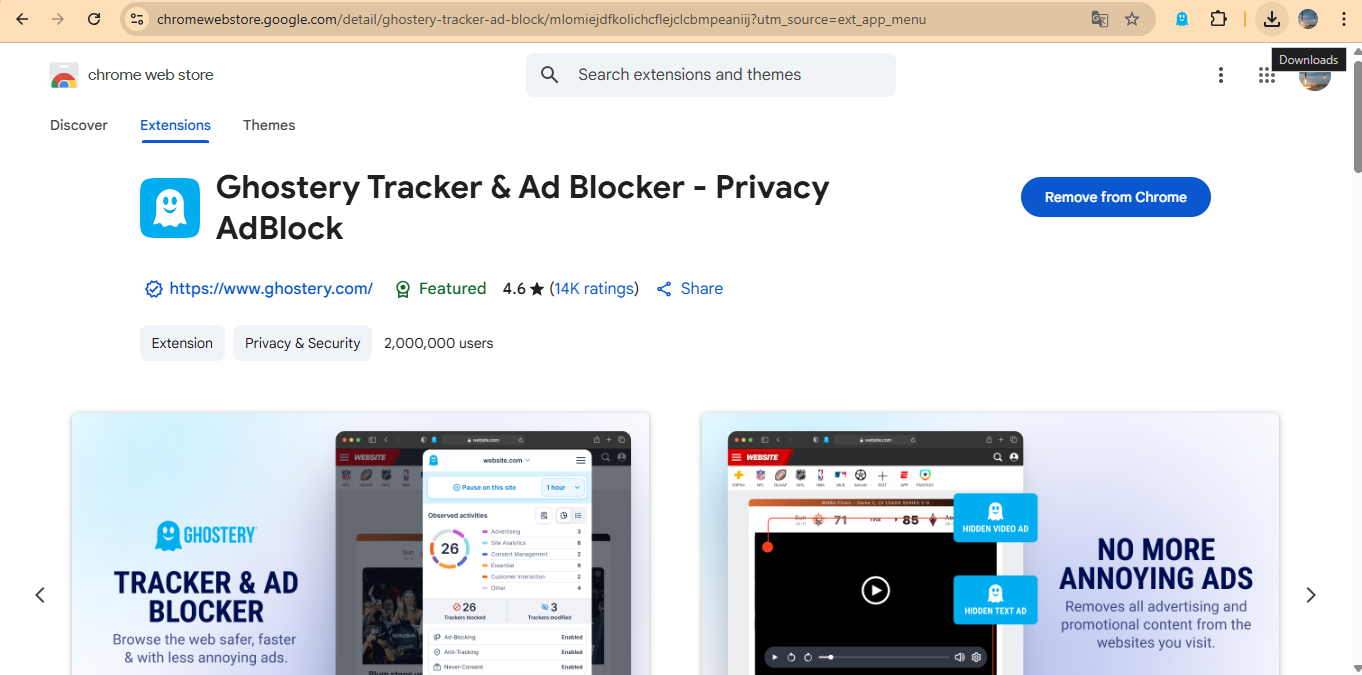
It’s a powerful and easy-to-use privacy extension. Block ads, trackers & speed up your web.

Ghostery is a powerful Tracker & Adblocker extension for Chrome with over 100 million downloads. Block ads, stop trackers, and speed up websites. Privacy at its best. FEATURES \* Block all ads on websites, including YouTube and Facebook, to focus on the information that matters. \* Stop trackers from collecting your personal data. \* Automatically remove intrusive cookie pop-ups and express dissent to online tracking. \* Get detailed tracker information on any website you visit, including the number of trackers, their type, and the company operating them. \* Preview tracker information on search engine result pages to make informed choices. \* Inspect the largest database of trackers, updated fast and reliably for all users.

To install click on Add to Chrome after click it will download a file and show a option now click on “Enable Ghostery” and it will automatically setup to chrome

It will pass a message to simply click allow or add extension



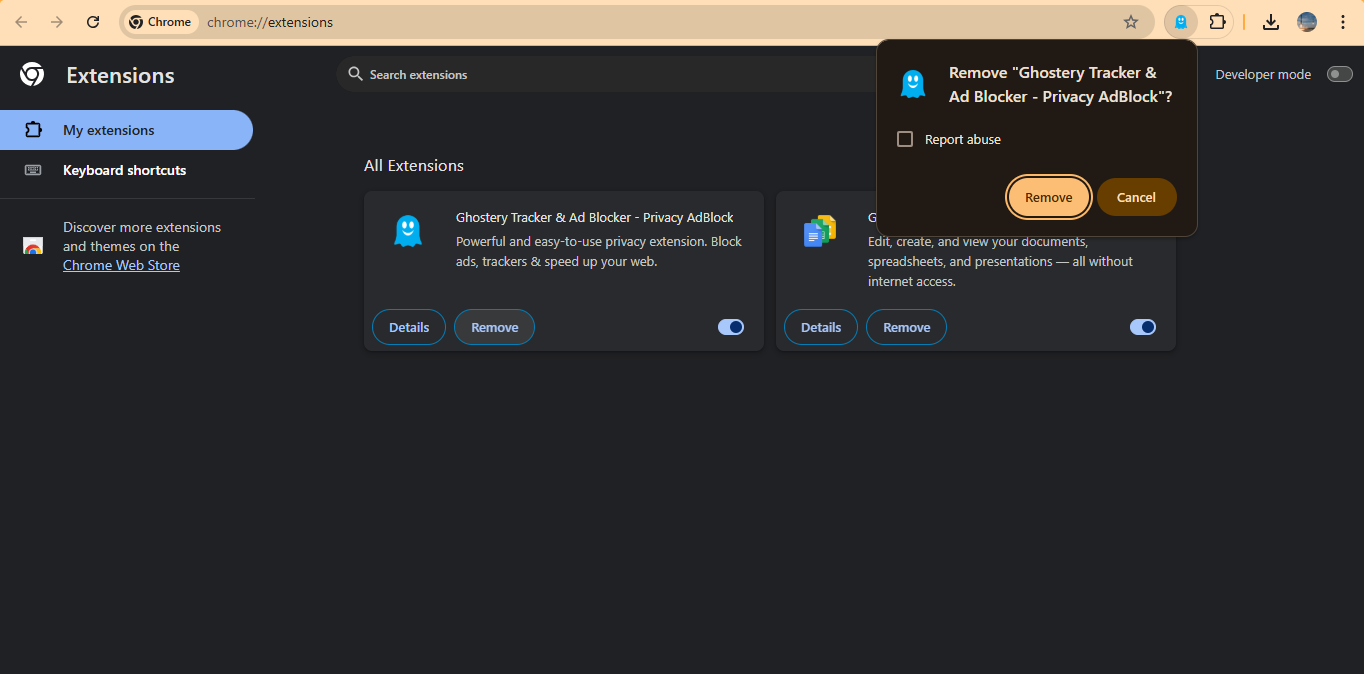


Finally its done and ready to use

Steps to remove an extension

To remove an extension simply search that extension and you will see a option “remove from chrome” or

Click on control and customization go to Extension > then Manage Extension this option all the extension installed in chrome browser here you can manage all extensions there you will see remove option click on it and Bingo extension will be removed or you can disable if no longer I use.



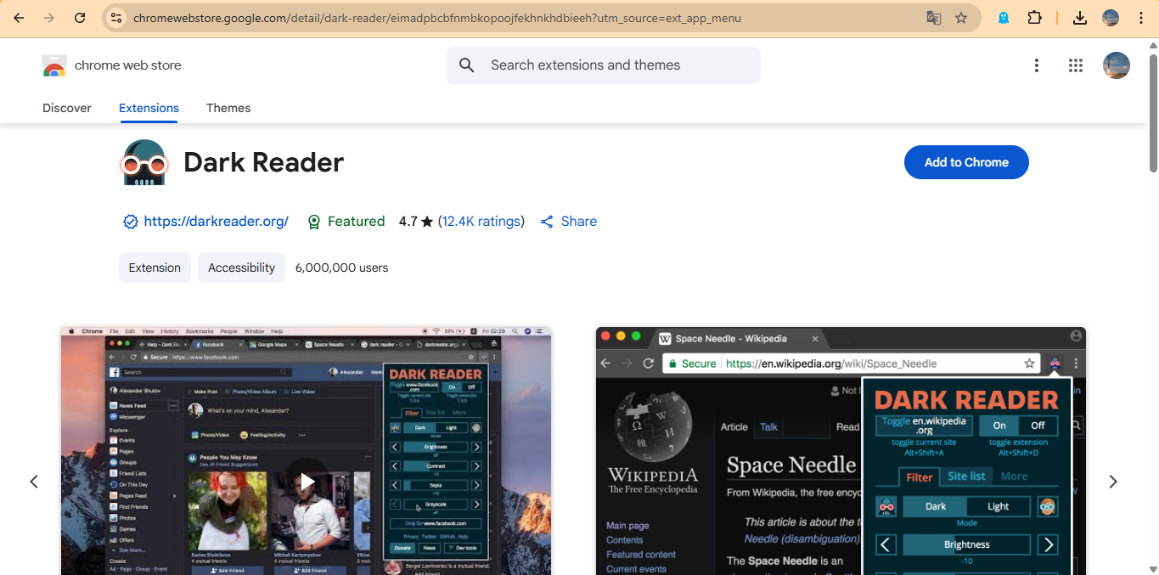
**Security Considerations**

While browser extensions can significantly enhance functionality, they also pose security and privacy risks. Many extensions require broad permissions to access data on the websites you visit, which can lead to potential misuse. Users should be cautious when installing extensions, especially from unknown sources, as malicious extensions can compromise personal information or introduce malware.

Risk of using a Browser Extension

Here are some risks associated with browser extensions:

* **Malware and Malicious Code**: Extensions can contain malicious code that injects scripts into webpages, monitors user activity, or steals data.
* **Overly Permissive Access**: Many extensions request extensive permissions that can lead to unauthorized access to sensitive information.
* **Redirecting Search Queries**: Some extensions can manipulate search queries and redirect users to unwanted sites.
* **Keyloggers**: Malicious extensions may include keyloggers that record and steal sensitive data, such as login credentials and financial information.
* **Exploits and Vulnerabilities**: Extensions can serve as gateways for exploits, potentially compromising the security of the browser and the user's data.
* **Slow down the speed of browser –** some of malicious or heavy extension affect browser by slowing their speed

Here we discuss about a extension which slown down the speed of a browser have a look on it

While Dark Reader is a popular and useful browser extension for enabling dark mode, it does have some potential drawbacks. These include performance issues like slowdowns on certain websites, especially those with a lot of JavaScript, and occasional rendering issues where websites don't display correctly.

**Ways to be safe from malicious of harmful extensions**

1. **Install extensions from browser app store or trusted sites.**
2. **Always Check the permission and suspicious activity of extension**
3. **And if you are highly concerned about security then before installing a extension read review and description for the extension.**

**Conclusion**

Browser extensions are powerful tools that can greatly enhance your web browsing experience by adding functionality and customization options. However, it's essential to choose extensions wisely and be aware of the permissions they request to ensure a safe browsing environment. You can find and install extensions from your browser's official web store, which is the safest method to add new features.