PROJECT REPORT TASK 7

IDENTIFY AND REMOVE SUSPICIOUS BROWSER EXTENSIONS

Objective

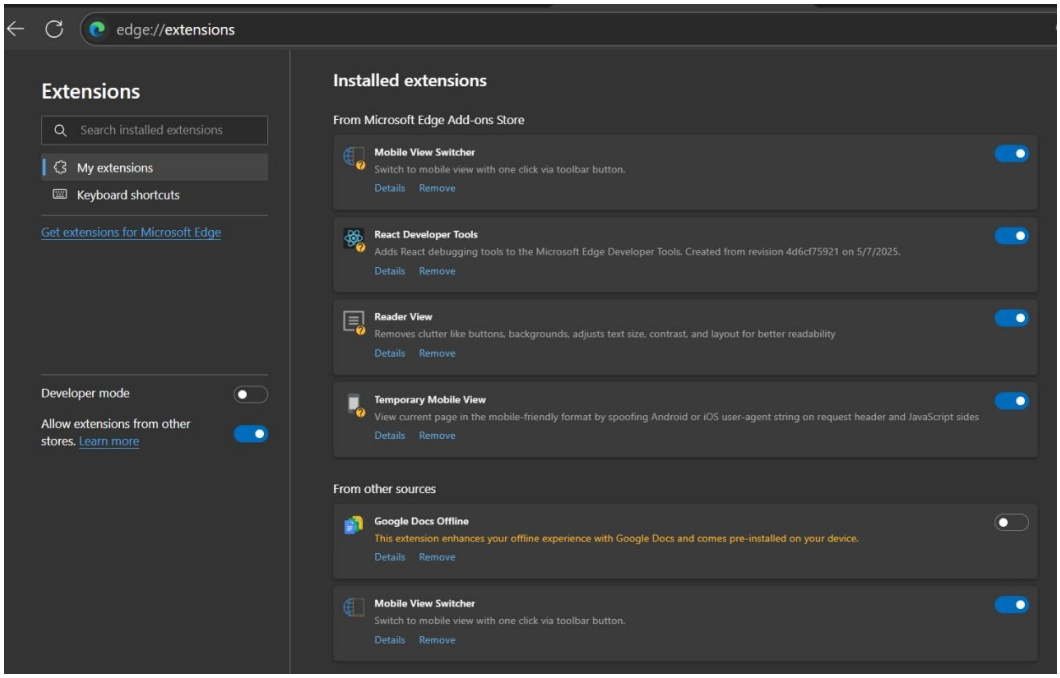
The objective of this task is to understand how to recognize potentially harmful or unnecessary browser extensions, review their permissions and sources, safely remove any suspicious or unused extensions from the web browser (Microsoft Edge), and document the process. This will help improve browser security, privacy, and performance.

Step 1: Open Extensions in Edge

1. Open **Microsoft Edge**.
2. Click the **three dots menu (⋯)** at the top right.
3. Select **Extensions**.
    - Or directly type edge://extensions in the address bar and press **Enter**.

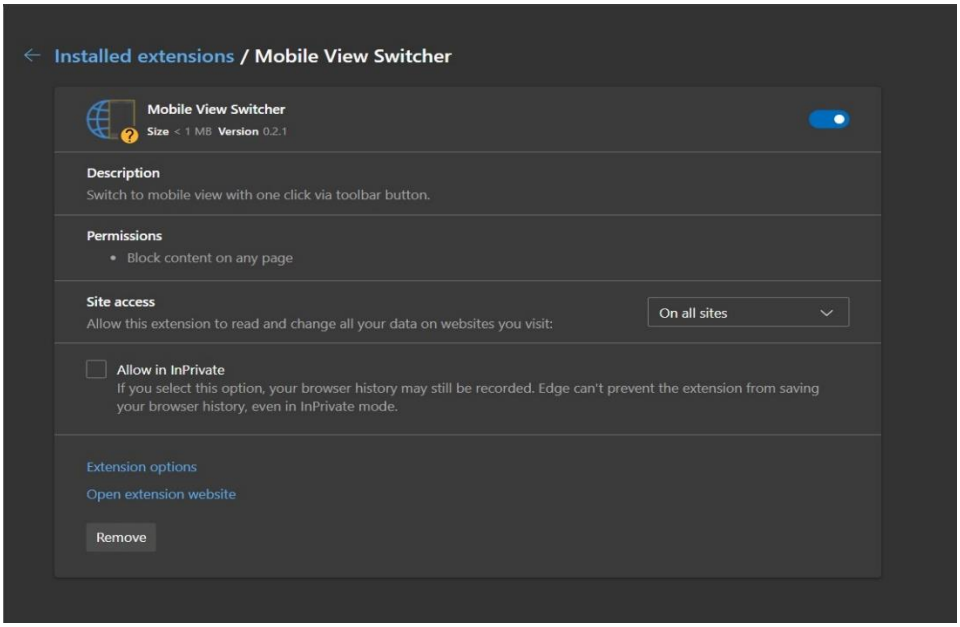
Step 2: Review Installed Extensions

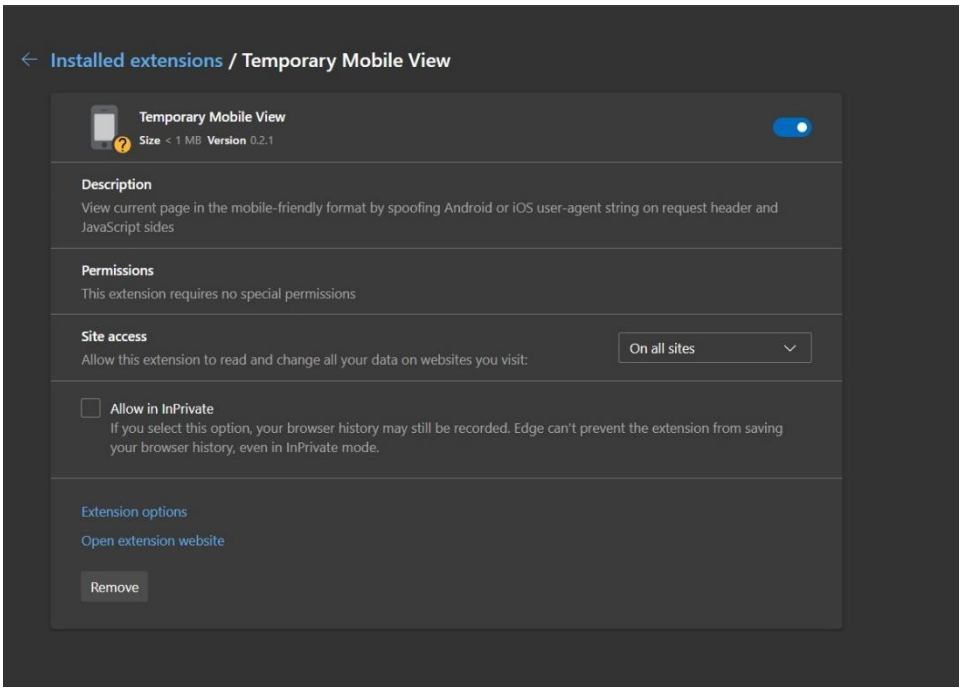
- You'll see all your installed extensions here.
- Look at each one's name, description, and status (enabled/disabled).



Step 3: Check Permissions & Details

- Click **Details** for each extension.
- Look at:
    - The **permissions** it has (does it need to read all your websites?).
    - The **source** (from Microsoft Edge Add-ons or third-party?).
    - If needed, search its reviews online (e.g., “Is the Extension safe?”).





Step 4: Identify Suspicious or Unused Extensions

- search for the extension name + “safe or malware” in Google.
- Is Reader View edge extension safe?

  The **Reader View** extension for Edge (based on Mozilla’s open-source Readability library) is generally considered **safe**, provided it’s sourced from the official Microsoft Edge Add-ons site. It’s a popular open-source tool with over 66k installs and positive feedback—no red flags for malware or data harvesting.

- Is React developer tools extension in edge safe?

  the **React Developer Tools** extension for Edge is widely used and backed by Meta, but it **has had a known security issue**—a vulnerability that allowed a malicious webpage to make arbitrary fetch requests through the extension.

Step 5: Remove Extensions

- Click **Remove** below the extension you don’t want.
- Confirm the removal when prompted.

Step 6: Restart Edge

- Close Edge completely and open it again.
- Test if your browsing feels smoother.

Step 7: Research How Malicious Extensions Can Harm You

- Malicious browser extensions can **steal sensitive data, track user behavior, and inject unwanted advertisements**. And at worst, they can even take over a user’s browser entirely. In this blog, we’ll take a deep dive into what malicious browser extensions can do and how to mitigate their risks.

Step 8: Example:

Extension Name	**Action Taken**	**Reason**
Mobile View Switcher	Removed	Unused
Temporary Mobile View	Removed	Unused

Summary:

In this task, I reviewed all installed browser extensions in Microsoft Edge to identify any suspicious or unnecessary ones. I removed extensions that were unused or had risky permissions to improve my browser’s security and performance.