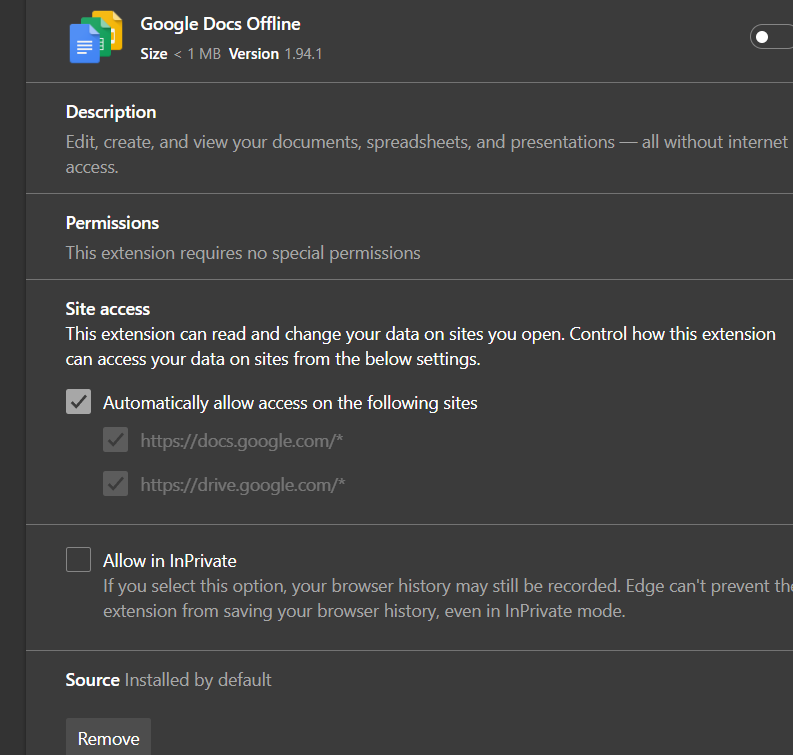
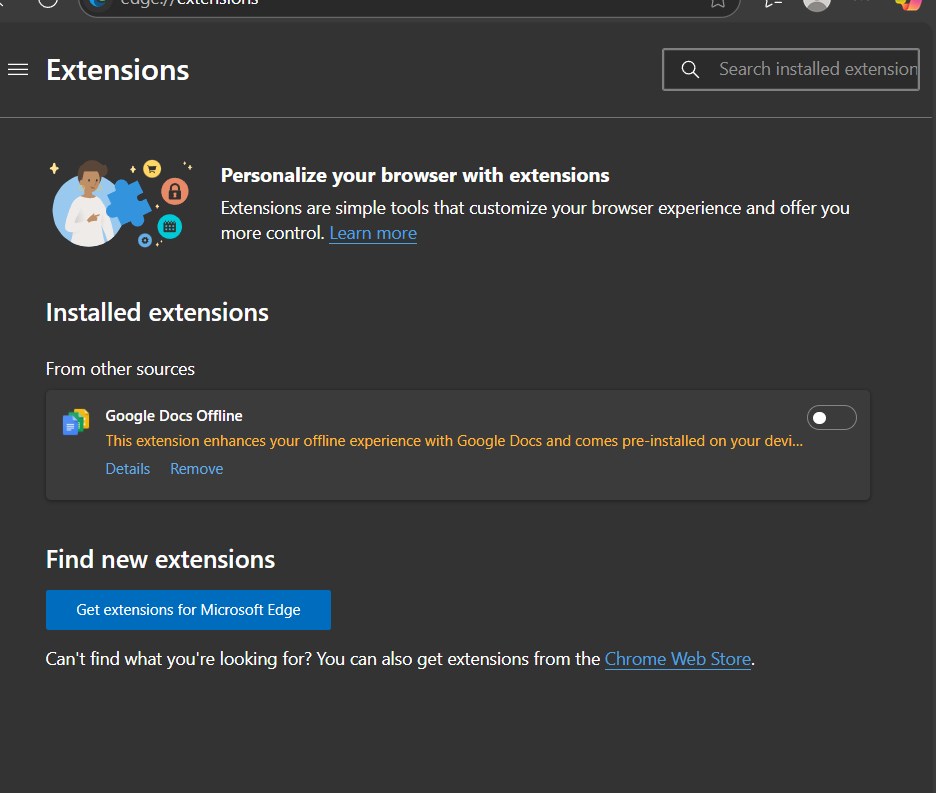
Task 7 : Identify and Remove Suspicious Browser Extensions:



* **Research: How Malicious Extensions Can Harm Users**
* Malicious browser extensions can be highly dangerous, even if they initially appear legitimate. Here are several ways they can harm users:
* **Data Theft:** Malicious extensions may have access to everything you view or type in your browser, including passwords, credit card details, social media messages, and personal identifiers. This data can be stolen and sold or used for other criminal activity.
* **Spying and Tracking:** Some extensions track all pages you visit, building detailed profiles about your behavior or even capturing keystrokes (keylogging).
* **Session Hijacking:** Stolen session cookies can let attackers impersonate you on websites, risking account compromise.
* **Malware Installation/Ransomware:** Extensions can download more malicious software, including ransomware that encrypts your files and demands payment.
* **Remote Browser Control:** Attackers may take control of your browser, redirecting you to phishing sites or changing your browser settings (search engine, homepage).
* **Persistence and Self-Reinstallation:** Advanced malware like ChromeLoader can set up scheduled Windows tasks to reinstall itself, making removal difficult.
* **Performance Issues:** Malicious or poorly designed extensions may slow down your browser and computer, using up system resources.
* **Real-World Example:** Even some extensions in official stores have been compromised after updates, working as “sleeper agents.” They collect user data, inject unwanted ads, or hijack web traffic.



* **Documented Steps Taken and Extensions Removed**
* **Date:** Thursday, August 14, 2025  
  **Time:** 11 PM IST  
  **Browser:** Microsoft Edge
* **Procedure:**
* **Opened the extensions manager in Edge.**
* **Reviewed installed extensions:** Only "Google Docs Offline" was present.
* **Checked permissions:** The extension required no special permissions and was installed by default. Site access was limited to Google Docs and Drive, with no broad permissions.
* **Checked reputation:** Verified legitimacy; "Google Docs Offline" is a well-known extension published by Google and not flagged as suspicious.
* **Determined action:**
* *No suspicious or unused extensions found, so no removal performed.*
* If removal is desired, click the “Remove” button shown in the extension details panel.
* **Restarted the browser:** Closed all Edge windows and reopened as recommended to apply changes.
* **Researched extension risks:** Documented the key threats posed by malicious extensions (see above).
* **Documented steps:**
* Checked Edge extension manager.
* Verified permissions and sources for "Google Docs Offline."
* Found no suspicious extensions; did not remove any.
* Restarted Edge for performance check.
* **Extensions removed:** None (as only a legitimate default extension was present).
* If you later install new browser extensions, repeat this process regularly. Remove any extensions you do not use or that seem suspicious, especially if they request broad permissions or have poor reviews, and always install from the official web store.