**Task 7 Report: Identify and Remove Suspicious Browser Extensions**

**Objective:**

To inspect installed browser extensions and identify any that may pose a security risk, then remove any suspicious or unnecessary ones.

**Browser Used:**

Google Chrome

**Steps Taken:**

* Opened Extension Manager:  
  Navigated to chrome://extensions to access the extensions manager in Google Chrome.
* Reviewed Installed Extensions:  
  Examined all installed extensions manually.
* Checked Permissions and Source:  
  Verified permissions granted to each extension. Cross-checked extension names and developers against the Chrome Web Store for legitimacy and user reviews.
* Analysis of Installed Extensions:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Extension Name | Description | Permissions | Source | Status |
| Chrome Remote Desktop | Remote access to this device | Standard | Google LLC (Official) | Safe |
| Google Docs Offline | Work offline with Docs | Standard | Google LLC (Official) | Safe |

* No Suspicious Extensions Found:  
  All installed extensions are from verified sources (Google). No unnecessary or unfamiliar extensions present.
* No Action Required:  
  No extensions were removed. No suspicious activity or performance issues noted.
* Researched How Malicious Extensions Harm Users:  
  Malicious extensions can:  
  - Steal browsing data and passwords  
  - Redirect traffic or inject ads  
  - Install additional malware  
  - Log keystrokes or spy on users

**Conclusion:**

After thoroughly reviewing the installed browser extensions, no malicious or suspicious items were found. Only two essential and trusted extensions by Google are currently installed:  
  
- Chrome Remote Desktop  
- Google Docs Offline  
  
Browser performance remains stable. Regular extension checks will be continued to maintain browser security and performance.