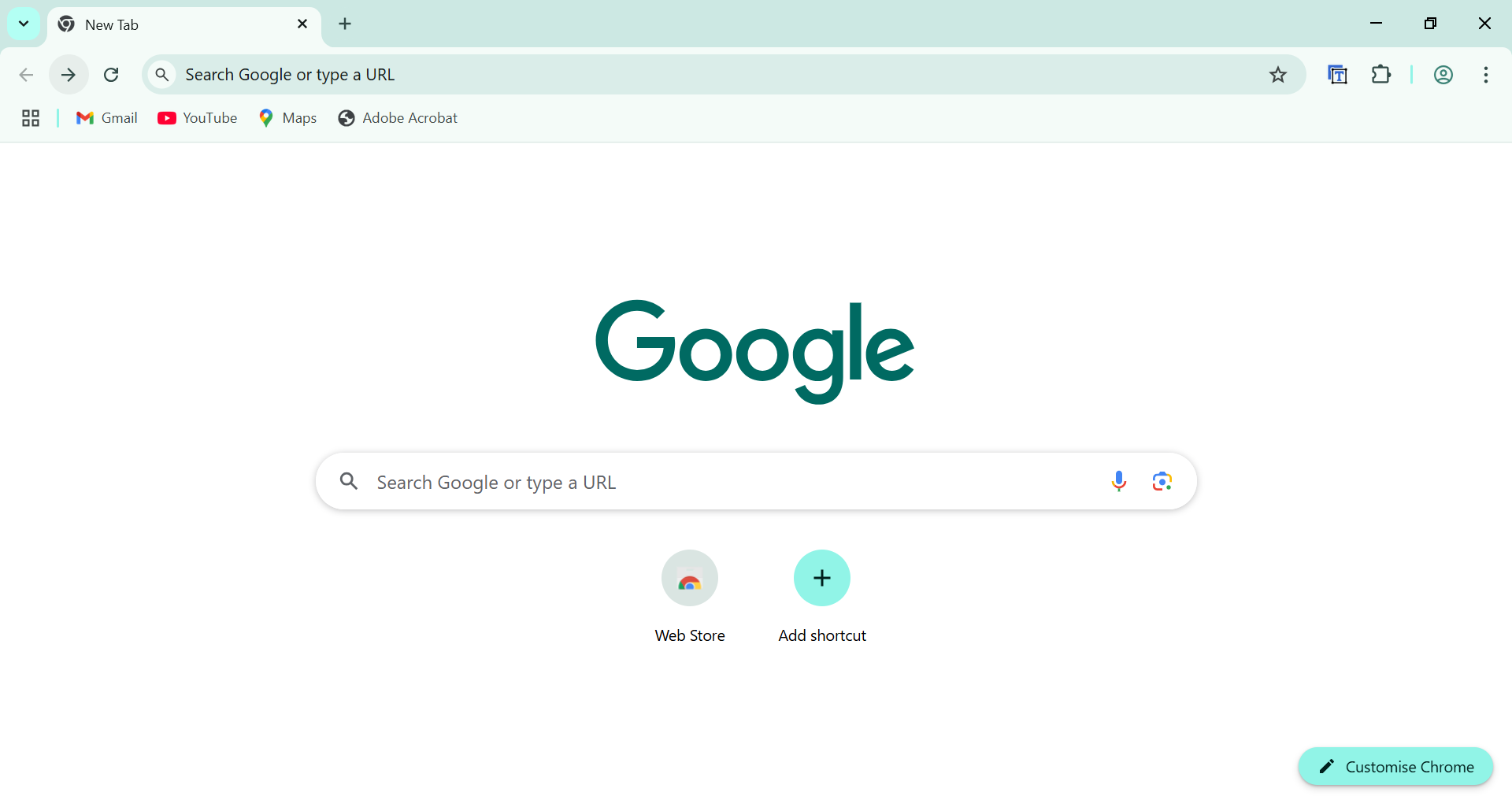
**Open your browser’s extension or add-ons manager.**

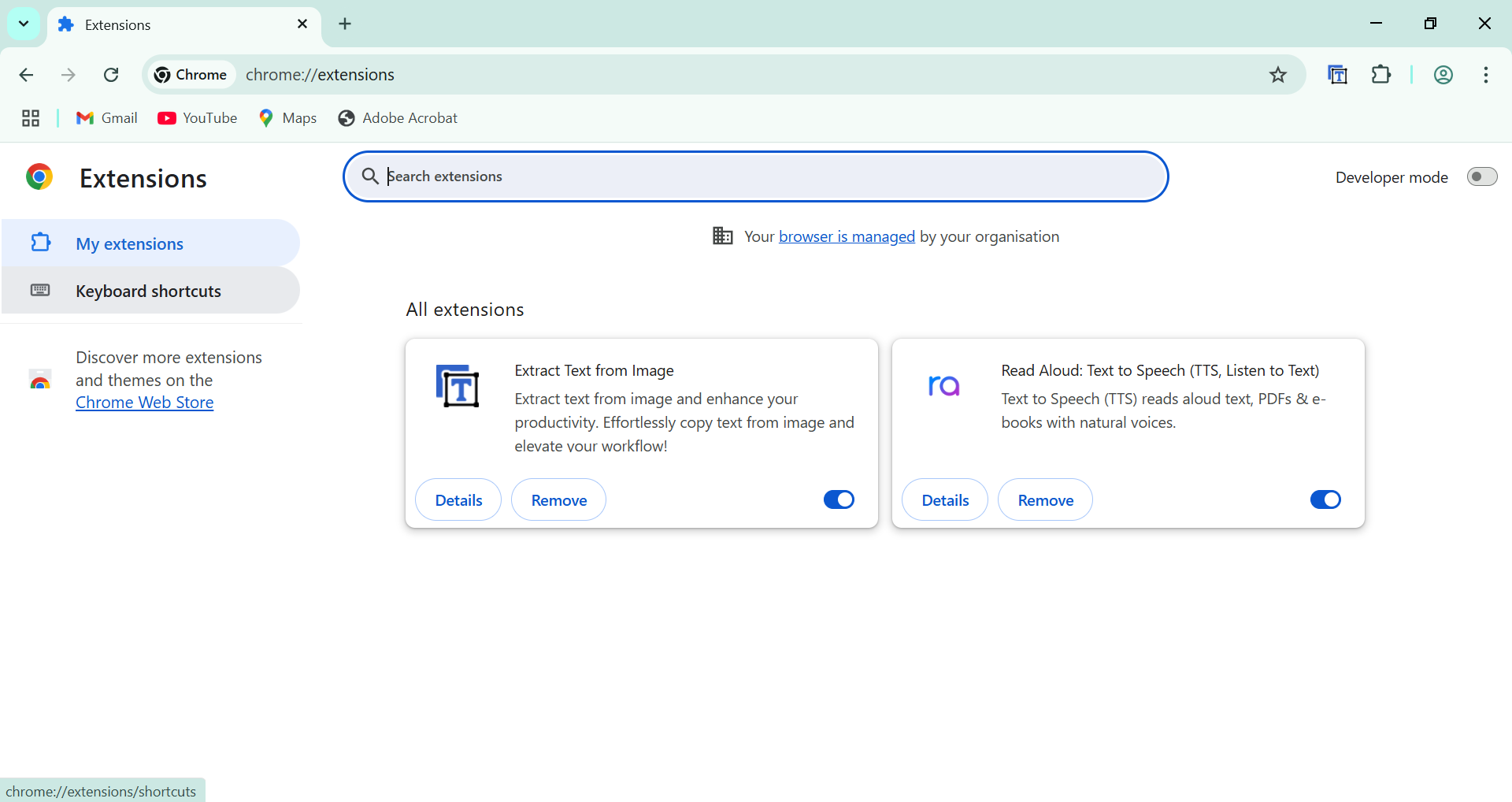
* In Chrome: Go to chrome://extensions/





**Review all installed extensions carefully.**

* Look for extensions you do not remember installing.
* Pay attention to extensions with very few downloads or poor ratings.



**Check permissions and reviews for each extension.**

* Identify what permissions each extension is requesting (e.g., access to all websites, read/write permissions).
* Check reviews and ratings in the extension store to see if other users report suspicious behavior

**Identify any unused or suspicious extensions.**

* Make a list of extensions you no longer use.
* Note any extensions you think may be risky or unfamiliar.

**Remove suspicious or unnecessary extensions.**

* Uninstall or disable these extensions from the manager.

**Restart your browser**

* This ensures any leftover processes from removed extensions are cleared.
* Check if your browser’s performance improves.

**Research how malicious extensions can harm users.**

* Understand common risks, such as data theft, ad injection, or tracking.

A screenshot of a computer

AI-generated content may be incorrect.

