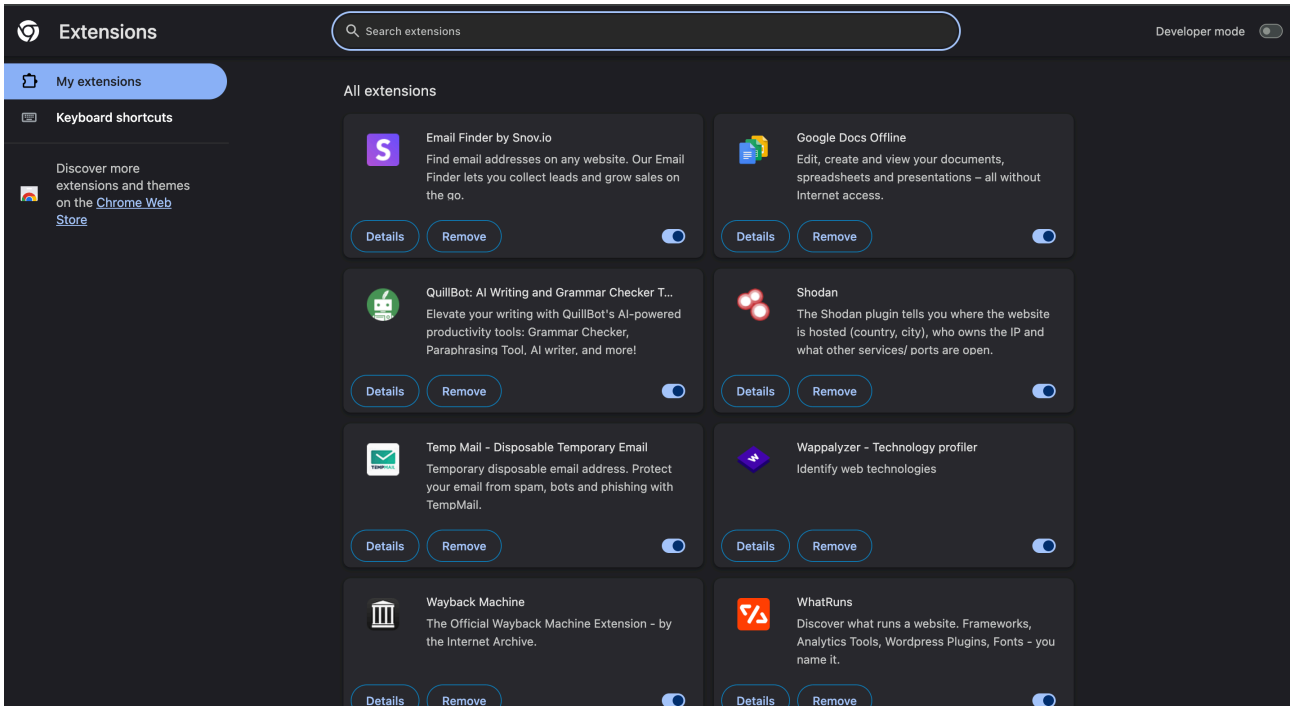
Spot and remove potentially harmful browser extensions

1. Find the Control Panel

Think of this as the garage where you store all your browser tools. You need to open it to see what you have.

- **How to do it:** Open your browser (Chrome, Firefox, Edge, etc.) and go to the **Extensions/ Add-ons Manager**. (Usually found under the main three-dot or three-line menu in the corner).



2. Take Inventory

Look at every single item on the list. Don't scroll past anything. Do you recognize all the names? Do you remember installing them?

3. Be a Detective: Check Permissions & Reputation

This is the most critical step. You need to see what each extension is *allowed* to do.

- **Check Permissions:** Click the **Details** button for any extension you're unsure about. If a simple calculator extension asks for permission to **"Read and change all your data on all websites,"** that's a massive **RED FLAG**.
- **Check Reviews:** If an extension seems shady, quickly search for it online. Look at its rating and the number of users on its official store page. Trust your gut if the reviews are sparse or overwhelmingly negative.

4. Identify the Clutter

Based on your detective work, you should now have a list of extensions that fall into two buckets:

- **The Unused:** You haven't touched it in months. It's just taking up space.
- **The Suspicious:** It has crazy permissions, a weird name, or a bad reputation.

5. Take Out the Trash

It’s time to cut the dead weight.

- **Remove It:** For every suspicious or unused item, click the **Remove** or **Uninstall** button. Don't just disable a suspicious one—**always remove it completely** to ensure its harmful code can't run in the background.

6. The Performance Check

Give your browser a fresh start to make sure the removal worked.

- **Restart:** Completely close your browser (and maybe even your computer) and reopen it.
- **Check the Speed:** Does your browser feel snappier? Are you seeing fewer random ads? You've likely just removed a major performance drag!

7. Research and Document

To protect yourself in the future, take a moment to understand the risks.

- **Learn the Danger:** Search for "How malicious browser extensions steal data" to see why this audit is so important (they can steal passwords, inject ads, and track your every click!).
- **Keep a Record:** Write down the names of the extensions you removed and why. This helps you remember which bad actors to avoid in the future.