**Step 1: Open Extension Manager**

**🔸 For Google Chrome:**

* Go to Chrome.
* In the address bar, type:

chrome://extensions

* Press Enter.

**🔹 Step 2: Review All Installed Extensions**

Look at each extension and ask:

* Do I **recognize** this extension?
* Have I **used** it recently?
* Does it have a **weird or generic name**?
* Are there **low reviews or no ratings**?

**Step 3: Check Extension Permissions**

Click “**Details**” or “More Information” for each extension.

Look out for:

* Full access to all websites
* Reading browser history
* Accessing clipboard or file system
* Modifying web content

These can be **dangerous if not from trusted sources**.

**Step 4: Research Suspicious Extensions**

Google the extension name with keywords like:

“Is [extension name] safe?”

“[extension name] malware”

If you find bad reviews, reports, or warnings — it may be malicious.

**Step 5: Remove Suspicious or Unused Extensions**

* Click **Remove** next to the extension.
* Confirm removal.

You can also remove unused or outdated ones to improve performance.

**Step 6: Restart the Browser**

* Close the browser completely.
* Reopen it.
* You may notice **faster performance** and fewer pop-ups.

**Step 7: Research: How Malicious Extensions Harm Users**

Malicious extensions can:

* Track your browsing history
* Steal passwords or cookies
* Inject ads or redirect websites
* Download additional malware