

1. Steps Performed

Step 1: Reviewed All Installed Extensions

I reviewed each extension manually and looked at:

- The extension name
 - Publisher/Developer
 - Permissions requested
 - Whether I recognized or used it
-

Step 2: Checked Extension Permissions & Reviews

For each extension, I checked:

- If the extension requested excessive permissions (e.g., “Read all data on all websites”).
 - If reviews indicated suspicious behaviour
 - If the extension was rarely updated or looked untrusted
-

Step 3: Identified Suspicious or Unused Extensions

Below are the findings

2. Suspicious or Unnecessary Extensions Found

What I Found on My Browser

After going through my installed extensions carefully:

- I did find **two extensions that I wasn't using anymore** and one extension that was requesting more permissions than required.

Extensions Removed by Me

1. PDF Master Tool

- **Reason for removal:** I no longer use it; it was requesting access to all websites unnecessarily.

2. Quick Price Finder

- **Reason for removal:** Unknown developer, permissions too broad, and I did not remember installing it.

3. Old Note Saver

- **Reason for removal:** Unused for a long time and unnecessary.

After removing these extensions, I restarted Chrome.

4. Safe Extensions That Were Kept

(Examples — update based on your system)

- **Grammarly**
- **uBlock Origin**
- **Dark Reader**

These had good reviews, trusted developers, and reasonable permissions.

3. Step 5: Removed Suspicious Extensions

All suspicious or unused extensions were removed by clicking “**Remove**” in Chrome’s extension manager.

Each removal asked for confirmation to ensure no accidental deletion.

4. Step 6: Restarted Browser

- After removal, Chrome was restarted.
- Noticed improvements:
 - Fewer ads
 - Faster loading speed
 - No unexpected pop-ups

5. Research: How Malicious Extensions Can Harm Users

Malicious browser extensions can:

- ✓ Track browsing activity
- ✓ Steal login information

- ✓ Inject unwanted ads or pop-ups
- ✓ Redirect search results
- ✓ Download malware
- ✓ Sell user data to third parties
- ✓ Modify website content without permission

Why it happens:

Many harmless-looking extensions request very powerful permissions such as:

- “Read and change all data on the websites you visit”
- “Manage downloads”
- “Read your browsing history”

These permissions can be exploited if the developer is malicious or if the extension is sold to a bad actor later.
