Identify and Remove Suspicious Browser Extensions

Step 1: Open Extension Manager

- ◆ **Google Chrome:**

1. Open Chrome.
2. In the address bar, type: chrome://extensions/
3. Press Enter.

- ◆ **Mozilla Firefox:**

1. Open Firefox.
2. Click the **menu (≡)** button in the top-right corner.
3. Select **Add-ons and Themes** > **Extensions**.

Step 2: Review Installed Extensions

- Go through the list of all installed extensions.
- Check:
  - Name and icon
  - Publisher name (is it trustworthy?)
  - Description
  - Permissions used (click “Details” or “More”).

Step 3: Check Permissions and Reviews

For each extension:

1. Click **Details**.
2. Note what permissions it has (e.g., “Read your browsing history” or “Access data on all websites”).
3. Google the extension name + “is it safe?” or check https://chrome.google.com/webstore for reviews.

Step 4: Identify Suspicious or Unused Extensions

Look for red flags:

- Extensions you don’t remember installing.

- Extensions that:
  - Have poor reviews.
  - Request unnecessary permissions.
  - Redirect or show ads.
  - Cause browser slowness or crashes.

Step 5: Remove the Extensions

1. On the extensions page:
   - Click **Remove** next to the suspicious extension.
2. Confirm the removal.

Step 6: Restart Browser

- Close all tabs and reopen your browser.
- This clears temporary memory and applies changes.

Step 7: (Optional) Scan with Antivirus or Malware Scanner

- Run a quick malware scan to ensure no threats remain (use tools like **Malwarebytes** or **Windows Defender**).