**Task 7: Identify and Remove Suspicious Browser Extensions**

**1. Open Your Browser’s Extension/Add-ons Manager**

* **Chrome**: Menu (⋮) → Extensions → Manage Extensions
* **Firefox**: Menu (☰) → Add-ons and Themes → Extensions

A screenshot of a computer

AI-generated content may be incorrect.

**2. Review All Installed Extensions Carefully**

* Go through each extension
* Look for unknown, rarely used, or suspicious names

A screenshot of a computer

AI-generated content may be incorrect.

**3. Check Permissions and Reviews for Each Extension**

* Click “Details” or similar
* Watch for:
  + Full access to websites
  + Access to browser history or clipboard
* Check user ratings and developer credibility in the extension store
* Look for the following **signs of a suspicious or malicious extension**:

| **🔴 Red Flag** | **🛑 Why It's Suspicious** |
| --- | --- |
| Unknown or generic developer name | May hide real identity |
| Low ratings or poor reviews | Signals bad performance or shady behavior |
| Excessive permissions | Example: Access to *all data on all websites* |
| No clear purpose or vague description | Could be a front for data tracking |
| Redirects your browsing or injects ads | Often adware or spyware |
| Extension that re-installs itself | Indicates malware-like behavior |
|  |  |

A screenshot of a computer

AI-generated content may be incorrect.

**4. Remove Suspicious or Unnecessary Extensions**

* Click **Remove** or **Trash/Delete icon**
* You can also **Disable** them first to test effects

**5. Restart Browser and Check for Performance Improvements**

* Close and reopen the browser
* Test for:
  + Faster browsing
  + No unwanted ads or redirects
  + Normal search behavior restored

**6. Research How Malicious Extensions Can Harm Users**

Malicious extensions may:

* Steal login credentials or credit card info
* Track everything you browse
* Redirect searches or inject unwanted ads
* Open backdoors for malware

**7.Tips to Stay Safe**

* Only install extensions from **official stores** and **reputable developers**
* Avoid unnecessary extensions
* Keep your browser and extensions updated
* Use antivirus or browser security plugins