Identifying and Removing Suspicious Browser Extensions

Objective

To ensure browser safety and performance by identifying and removing potentially harmful or unnecessary extensions.

Tools Required

- Google Chrome

  Or

- Mozilla Firefox
- Internet connection (for checking reviews and permissions)

Step-by-Step Guide

1. Open Extension/Add-ons Manager

Google Chrome:

- Click the three-dot menu (⋮) in the top-right corner.
- Go to **Extensions** > **Manage Extensions** or visit `chrome://extensions/`.

Mozilla Firefox:

- Click the menu icon (≡) in the top-right corner.
- Select **Add-ons and Themes** > **Extensions** or visit `about:addons`.

---

2. Review All Installed Extensions

- Carefully check the list of all installed extensions.
- Identify extensions you do not recognize, do not use, or do not remember installing.

---

3. Check Extension

Details

For each extension:

- Click **Details** (Chrome) or **More Options** (Firefox).
- Review the following:

a. Permissions

- Look for permissions like:
  - "Read and change all your data on the websites you visit"
  - "Access your clipboard"
  - "Capture content of your screen"
- These may indicate privacy risks if not justified by the extension's purpose.

b. Reviews and Ratings

- Visit the Chrome Web Store or Mozilla Add-ons site.
- Check user reviews and ratings.
- Be cautious of extensions with:
  - Low ratings
  - No reviews
  - Complaints about ads, redirects, or suspicious behavior

c. Developer and Update History

- Verify if the developer seems legitimate.
- Check the last updated date—very outdated extensions may be unsupported or vulnerable.

---

4. Identify Suspicious or Unnecessary Extensions

Mark any extension that is:

- Unused or unknown
- Installed without your knowledge
- Asking for excessive permissions
- Poorly rated or reviewed
- Causing browser slowdowns, popups, or redirections

---

5. Remove Unwanted Extensions

In Chrome:

- Go to `chrome://extensions/`
- Click **Remove** next to the extension
- Confirm removal

In Firefox:

- Go to `about:addons`
- Click the three-dot icon next to the extension
- Select **Remove**
- Confirm removal

---

6. Restart the Browser

After removing unwanted extensions, restart the browser.

- Check for improvements in speed and responsiveness.
- Ensure normal functionality of websites.

---

7. Understand the Risks of Malicious Extensions

Malicious extensions can:

- Steal login credentials and personal data
- Redirect search queries or inject ads
- Monitor browsing activity
- Install additional malware

Being aware of these risks helps maintain a secure browsing environment.

Thank You