Task 7: Identify and Remove Suspicious Browser Extensions

Objective: Learn to spot and remove potentially harmful browser extensions.

Tools: Any web browser (Chrome, Firefox)

Detailed Step-by-Step Procedure

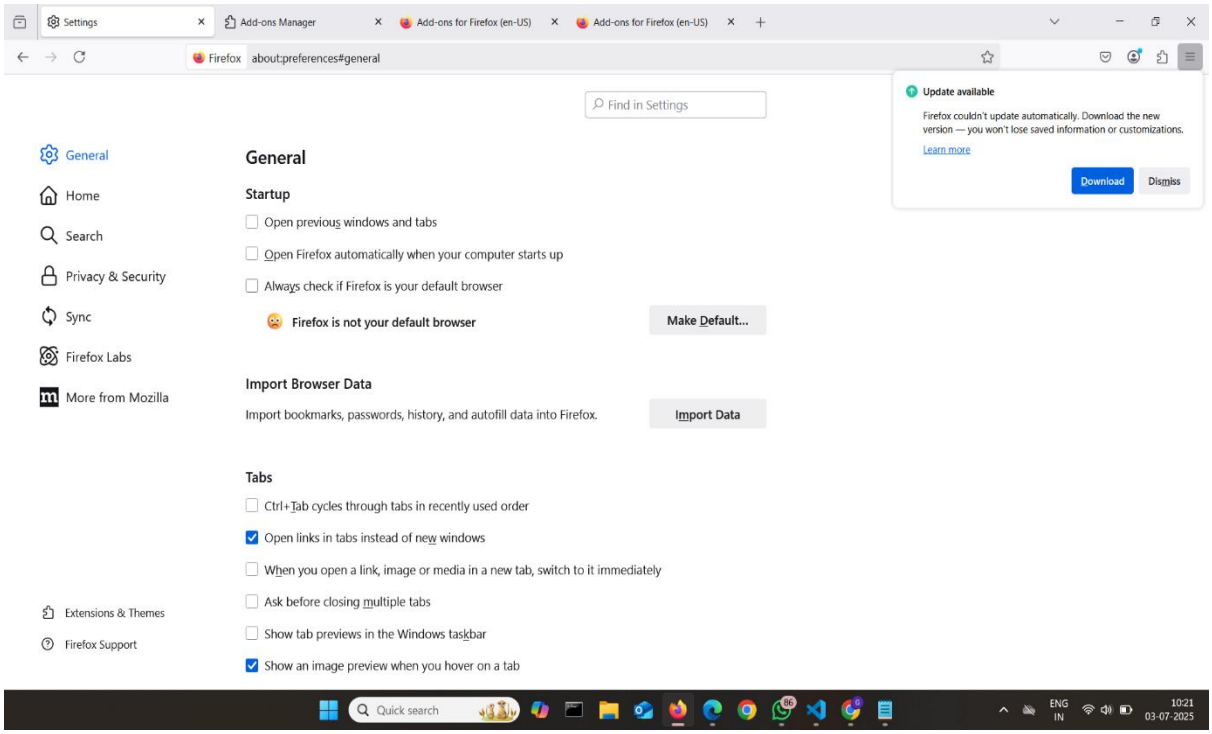
Step 1: Open the Extensions/Add-ons Manager

In Google Chrome:

1. Open Chrome.
2. Click the 3-dot menu (top right).
3. Navigate to: Extensions > Manage Extensions
   Or directly type: chrome://extensions/ in the address bar.

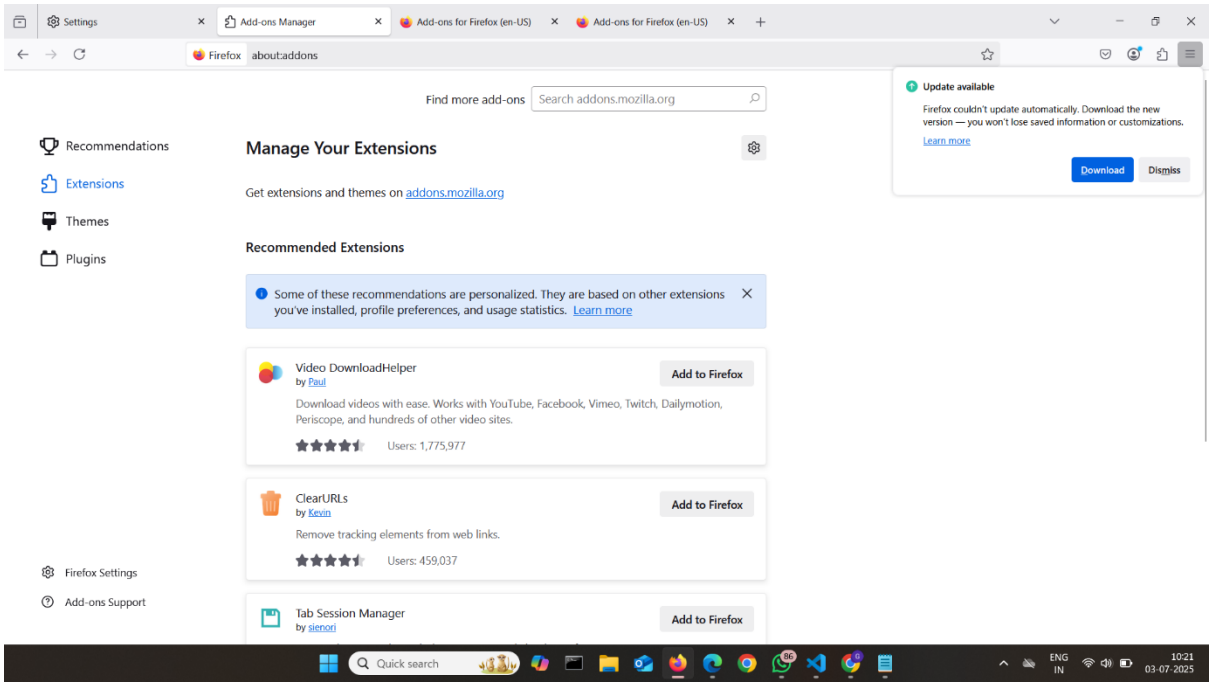
In Mozilla Firefox:

1. Open Firefox.
2. Click the 3-line menu (top right).
3. Select: Add-ons and themes > Extensions.



Step 2: Review Installed Extensions

1. Go through each installed extension one by one.
2. Ask yourself:
    - Do I remember installing this?
    - Do I use this regularly?
    - Does this name look suspicious or unfamiliar?



Step 3: Check Permissions and Details

1. Click the **"Details"** or **"More Info"** button for each extension.
2. Look for:
    - Permissions like “Read and change all your data on all websites” (High Risk).
    - Access to clipboard, browsing history, tabs, etc.
    - Background activity that seems unnecessary.

Step 4: Research the Extension

1. Google the name of the extension (e.g., "PDF Converter Pro Chrome extension").
2. Check:
    - **User reviews** on Chrome Web Store / Mozilla Add-ons.
    - **News articles**, **Reddit posts**, or **security forums** discussing malicious behavior.
    - **Developer name** — Is it a known brand (e.g., Google, Grammarly)?

Step 5: Identify Suspicious or Unused Extensions

Flag extensions that:

- Have very **few or fake reviews**.
- Ask for **broad permissions** without clear need.
- Have **generic or misleading names** (e.g., "Fast Search Tool").
- Are **never used** or have unknown origin.

Step 6: Remove Suspicious or Unnecessary Extensions

1. Click **"Remove"** or **"Uninstall"** for each flagged extension.
2. Confirm removal when prompted.
3. Repeat for all suspicious/unneeded entries.

Step 7: Restart the Browser

1. Close **all tabs and windows** of the browser.
2. Re-open the browser to complete cleanup.
3. Check:
    - Has the browser performance improved?
    - Are previous pop-ups/redirects gone?

Step 8: Scan for Malware (Optional but Recommended)

1. Use built-in antivirus (e.g., Windows Defender) or a tool like **Malwarebytes**.
2. Run a **quick scan** to ensure no malware was left by any removed extensions.

Outcome: Awareness of browser security risks and managing browser extensions.