# Task 7: Identify and Remove Suspicious Browser Extensions - Step-by-Step Guide

## 1) Prep (2 mins)

- Close extra tabs/apps so performance changes are obvious.

- Decide your browser: Chrome or Firefox (steps for both below).

## 2) Open the Extensions/Add-ons Manager

- Chrome: Menu ⋮ → Extensions → Manage extensions (or visit chrome://extensions/), toggle Developer mode ON.

- Firefox: Menu ☰ → Add-ons and themes → Extensions (or visit about:addons).

## 3) Review Each Extension Carefully (what to check)

- Check if you recognize it, and verify developer reputation online.

- Check permissions vs purpose (excessive permissions = high risk).

- Review source, updates, and unusual behavior like ads, pop-ups, or CPU usage.

## 4) Measure Impact (optional)

- Chrome: More tools → Task manager (Shift+Esc) → sort by CPU/Memory.

- Firefox: Visit about:performance to view energy impact.

## 5) Disable, Test, Then Remove

- Disable suspicious/unused extension → restart browser.

- If no issues after disabling → remove permanently.

## 6) After-Removal Hygiene

- Clear browsing data and run security/safety check.

- Update browser to latest version.

## 7) How malicious extensions can harm users

- Ad/affiliate injection, tracking, credential theft, proxy hijacking, cryptomining.

- Silent updates adding malicious features.

## 8) Deliverables

- List suspicious/removed extensions with reason.

- Steps taken summary.

- Improvements observed after removal.