Task 7: Identify and Remove Suspicious Browser Extensions

Objective:

Learn to spot and remove potentially harmful browser extensions.

Tools:

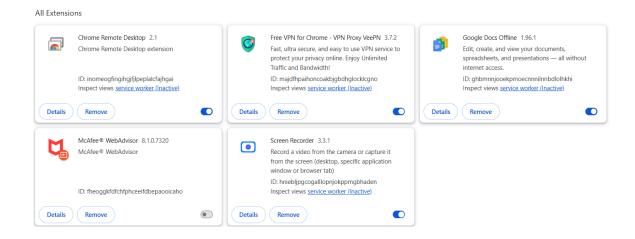
Any web browser (I used Chrome).

Steps Taken:

- 1. Opened the browser's extension/add-ons manager.
- 2. Reviewed all installed extensions carefully, checking permissions, reviews, and usage.
- 3. Identified any unused or suspicious extensions (with excessive permissions, poor reviews, or unknown developers).

Extensions which are reviewed:

- 1. Chrome Remote Desktop
 - ✓ Safe. This is Google's official tool for remote access. Keep it if you use it.
- 2. Free VPN for Chrome VPN Proxy VeePN
 - **↑** Suspicious/High-Risk.
 - Many "free VPN" Chrome extensions track user activity or inject ads.
 - VeePN has been flagged in security forums for questionable practices.
 - Unless you really trust it, I recommend **removing it**.
- 3. Google Docs Offline
 - Safe. This is an official Google extension that lets you use Docs offline.
- 4. McAfee® WebAdvisor
 - - It's legitimate from McAfee, but often slows down browsing and shows unnecessary warnings.
 - If you already have antivirus software, this is usually redundant.
 - Optional: You can disable/remove it for better performance.
- 5. Screen Recorder (3.3.1)
 - ⚠ Needs review.
 - There are many "Screen Recorder" extensions, and not all are safe.
 - If it's not from a trusted developer (like Loom or Screencastify), I recommend **removing it**.
 - Especially risky if it asks for permissions like "Read and change all data on websites."



Suspicious Extensions Found and Removed:

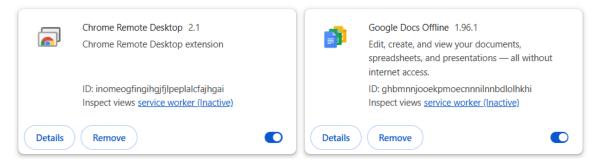
✓ What to Keep

- Chrome Remote Desktop
- Google Docs Offline

↑ What to Consider Removing

- Free VPN for Chrome VPN Proxy VeePN (strongly recommend removing)
- McAfee WebAdvisor (optional, slows down browsing)
- Screen Recorder (if not from a well-known trusted developer)

All Extensions



How Malicious Extensions Can Harm Users:

- **Data theft**: Steal login credentials, credit card details, or browsing history.
- Ad injection: Show unwanted ads or redirect to malicious sites.
- Tracking: Collect sensitive user data and sell it.
- **Browser hijacking**: Change search engine, homepage, or settings.