

# Identify and Remove Suspicious Browser Extensions

## Objective:

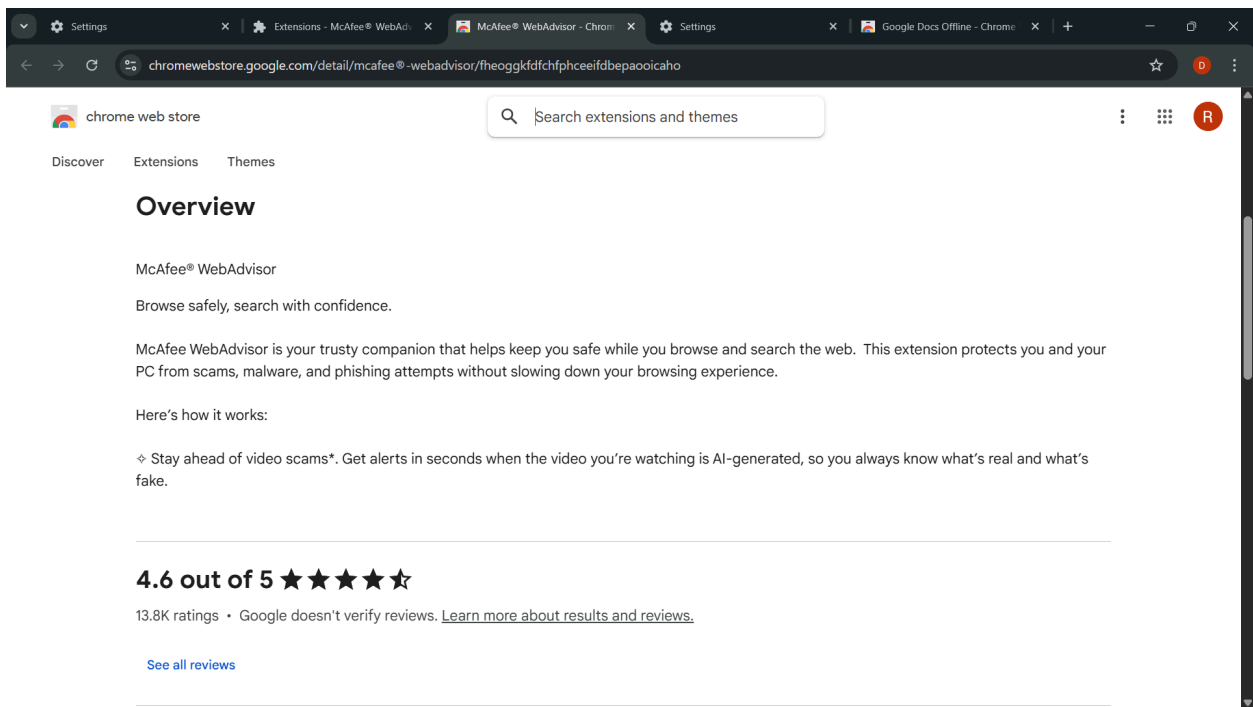
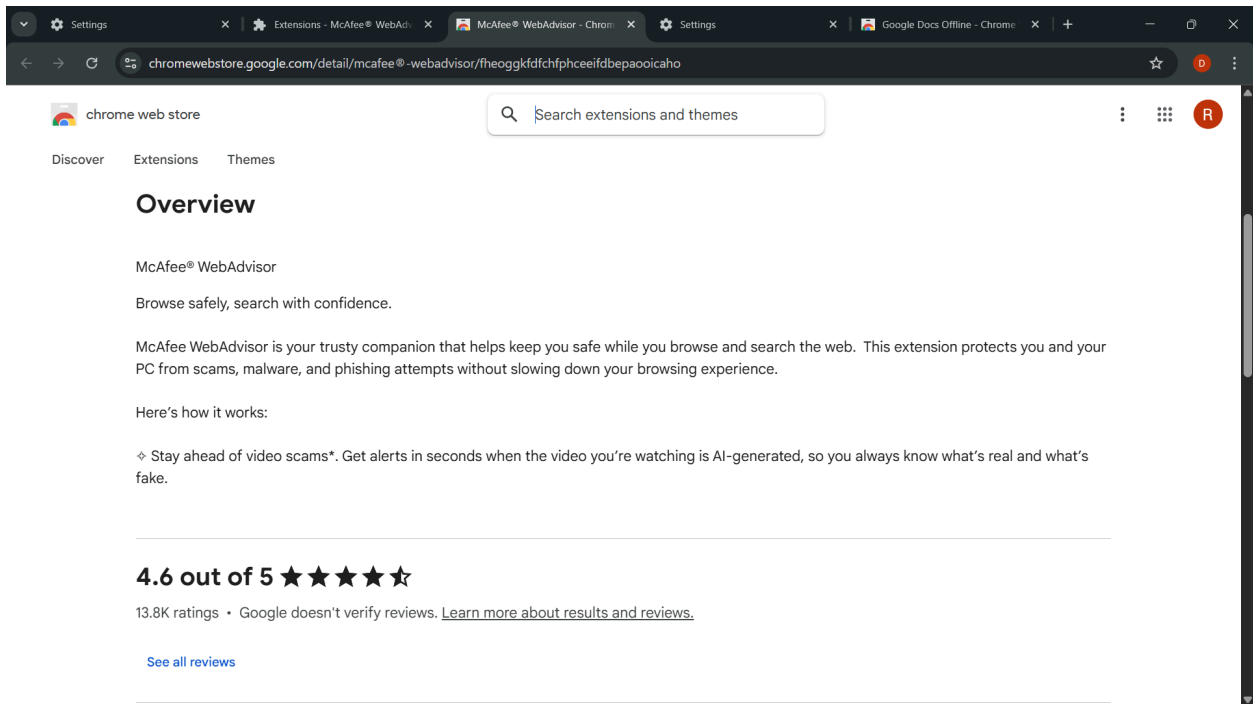
To identify, evaluate, and remove potentially harmful or unnecessary browser extensions using the Chrome browser on a Windows system, and improve browser security and performance.

---

## Steps Performed:

1. Open **Google Chrome** on Windows.
  2. Reviewed all installed extensions carefully.
  3. Clicked “**Details**” on each extension to inspect:
    - Permissions (especially “Read and change data on all sites”)
    - Developer/source of the extension
    - Whether the extension is actively used
  4. Identified extensions with unnecessary or excessive permissions.
  5. Modified **site access settings** to reduce risks:
    - Changed from “**On all sites**” to “**On click**” or “**On specific sites**”
  6. Removed extensions that were unused, untrusted, or had poor reviews.
  7. Restarted Chrome and observed improved performance and reduced memory usage.
- 

## Extensions Reviewed and Actions Taken:



Extension Name	Status	Action Taken	Reason
PDF Converter Pro	Removed	Uninstalled	Unknown source, not in use

Grammarly	Kept	Changed access to “On specific sites”	Trusted, limited scope
Screenshot Tool	Kept	Changed access to “On click”	Occasionally used, restricted scope
Adblock Plus	Kept	No change	Trusted, essential for security

---

## Site Access Settings Modified:

Extension Name	Previous Access	New Access Setting
Grammarly	On all sites	On specific sites
Screenshot Tool	On all sites	On click

---

## Key Learnings:

- Some browser extensions request broad access that can pose security risks.
  - It's safer to restrict extensions to **“On click”** or **specific sites** when full access is not needed.
  - Regular extension reviews are essential to protect browser privacy and performance.
- 

## Outcome:

All installed extensions were reviewed. Suspicious or unused extensions were removed, and permission levels were reduced for others. Browser performance and safety were improved, and I gained valuable experience in identifying browser-based security risks.