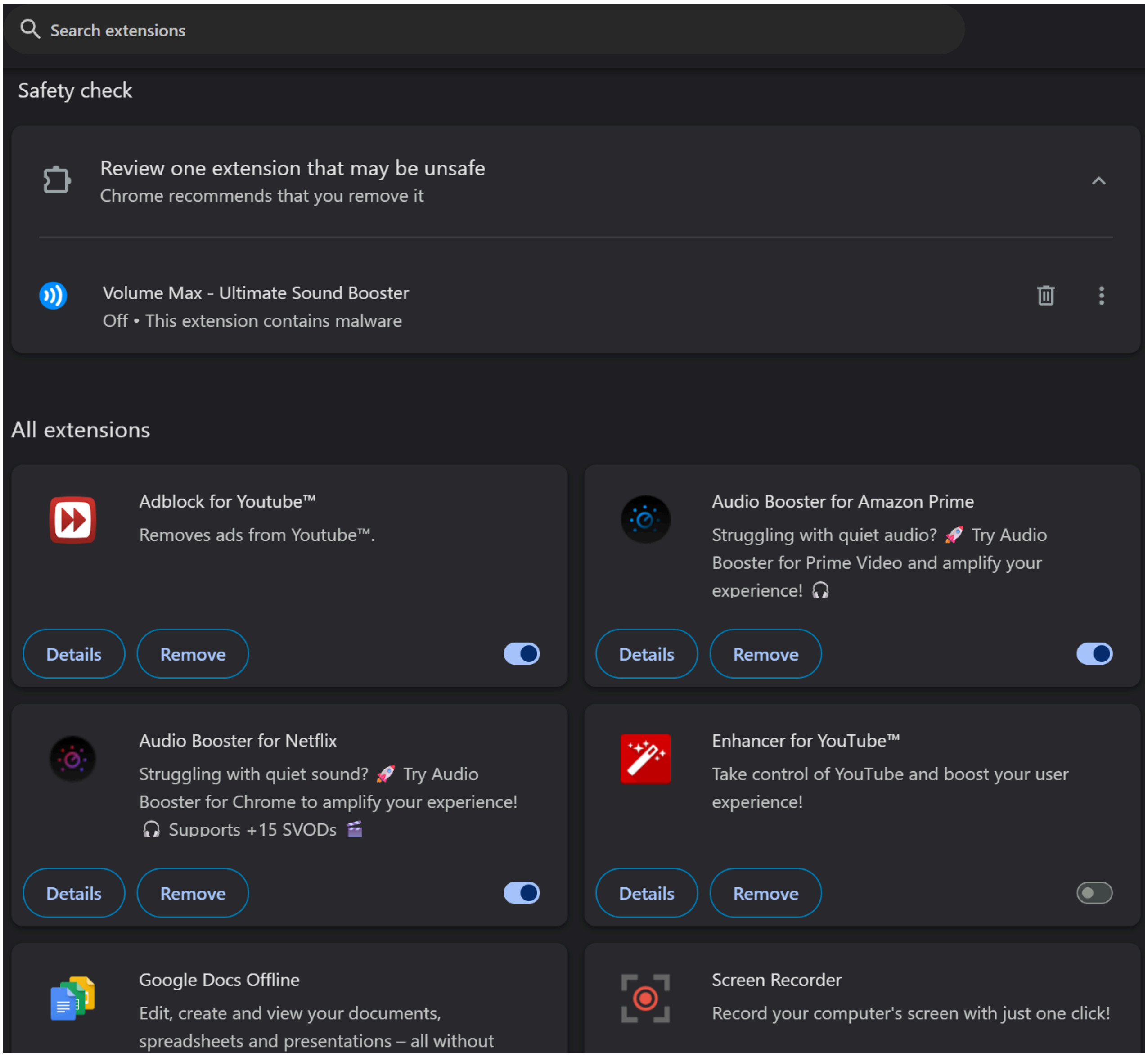
Task 7 :Identify and Remove Suspicious Browser Extensions

1.Open your browser’s extension/add-ons manager.



Search extensions

Safety check

Review one extension that may be unsafe

Chrome recommends that you remove it

Volume Max - Ultimate Sound Booster

Off • This extension contains malware

All extensions

Adblock for Youtube™

Removes ads from Youtube™.

Audio Booster for Amazon Prime

Struggling with quiet audio? 🚀 Try Audio Booster for Prime Video and amplify your experience! 🎧

Audio Booster for Netflix

Struggling with quiet sound? 🚀 Try Audio Booster for Chrome to amplify your experience! 🎧 Supports +15 SVODs 🎬

Enhancer for YouTube™

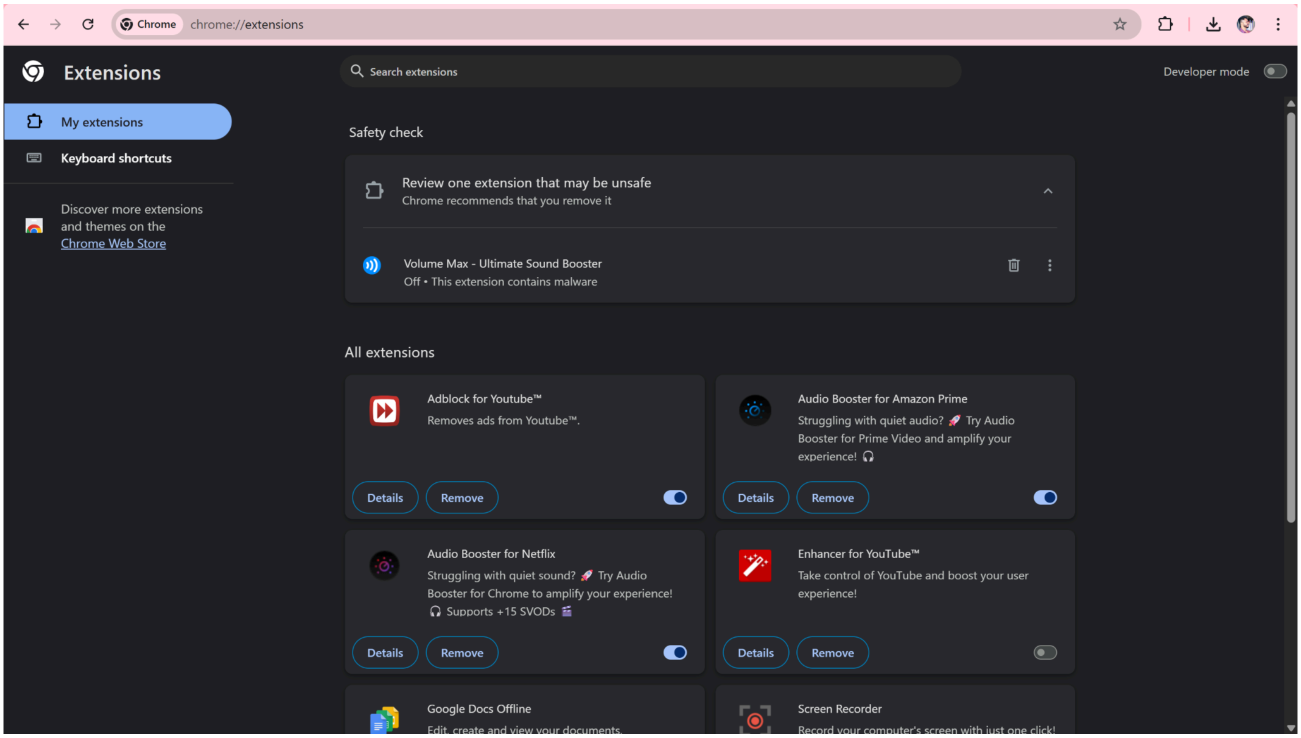
Take control of YouTube and boost your user experience!

Google Docs Offline

Edit, create and view your documents, spreadsheets and presentations – all without

Screen Recorder

Record your computer's screen with just one click!



Discover more extensions and themes on the Chrome Web Store

Safety check

Review one extension that may be unsafe
Chrome recommends that you remove it

Volume Max - Ultimate Sound Booster
Off • This extension contains malware

All extensions

Adblock for Youtube™
Removes ads from Youtube™.

Audio Booster for Amazon Prime
Struggling with quiet audio? 🚀 Try Audio Booster for Prime Video and amplify your experience! 🎧

Audio Booster for Netflix
Struggling with quiet sound? 🚀 Try Audio Booster for Chrome to amplify your experience! 🎧 Supports +15 SVODs 🎬

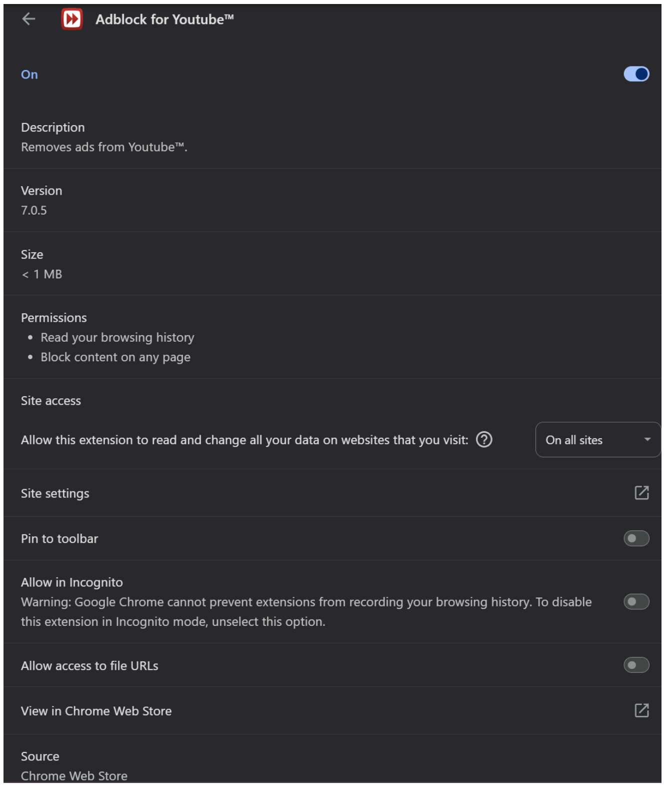
Enhancer for YouTube™
Take control of YouTube and boost your user experience!

Google Docs Offline
Edit, create and view your documents,

Screen Recorder
Record your computer's screen with just one click!

The first step of this task was to open the browser's extension manager to get a complete view of all extensions currently installed. Since I am using Chrome, I typed chrome://extensions/ into the address bar and pressed Enter. This opened the extensions page where I could see the name, icon, and status (enabled or disabled) of each extension. From here, I can also view additional details such as the extension ID, permissions it uses, and the option to remove or disable it. Opening the extension manager is important because it is the starting point for identifying any unfamiliar, unused, or potentially risky browser extensions before deciding whether to keep or remove them in the later steps.

2.Review all installed extensions carefully.



Adblock for Youtube™

On

Description
Removes ads from Youtube™.

Version
7.0.5

Size
< 1 MB

Permissions
- Read your browsing history
- Block content on any page

Site access

Allow this extension to read and change all your data on websites that you visit: On all sites

Site settings

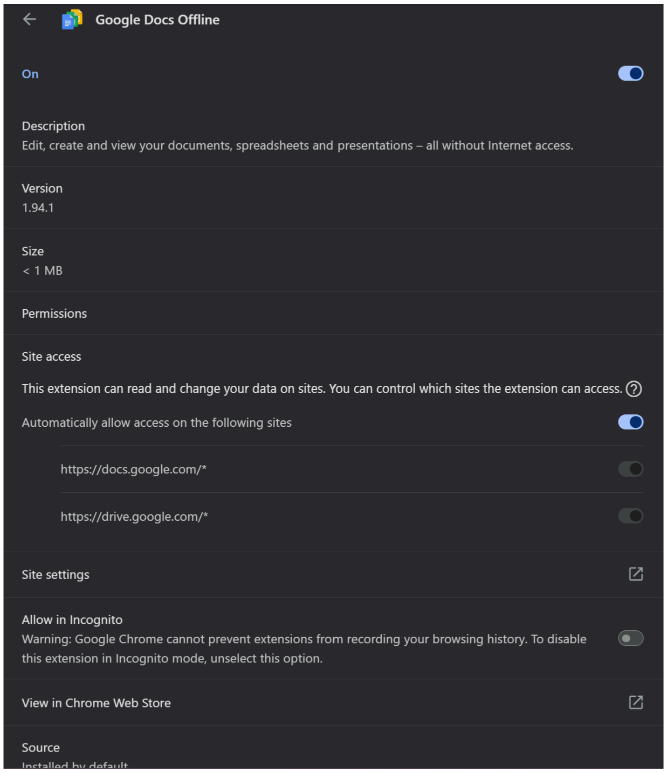
Pin to toolbar

Allow in Incognito
Warning: Google Chrome cannot prevent extensions from recording your browsing history. To disable this extension in Incognito mode, unselect this option.

Allow access to file URLs

View in Chrome Web Store

Source
Chrome Web Store



Google Docs Offline

On

Description
Edit, create and view your documents, spreadsheets and presentations – all without Internet access.

Version
1.94.1

Size
< 1 MB

Permissions

Site access

This extension can read and change your data on sites. You can control which sites the extension can access.

Automatically allow access on the following sites

https://docs.google.com/*

https://drive.google.com/*

Site settings

Allow in Incognito
Warning: Google Chrome cannot prevent extensions from recording your browsing history. To disable this extension in Incognito mode, unselect this option.

View in Chrome Web Store

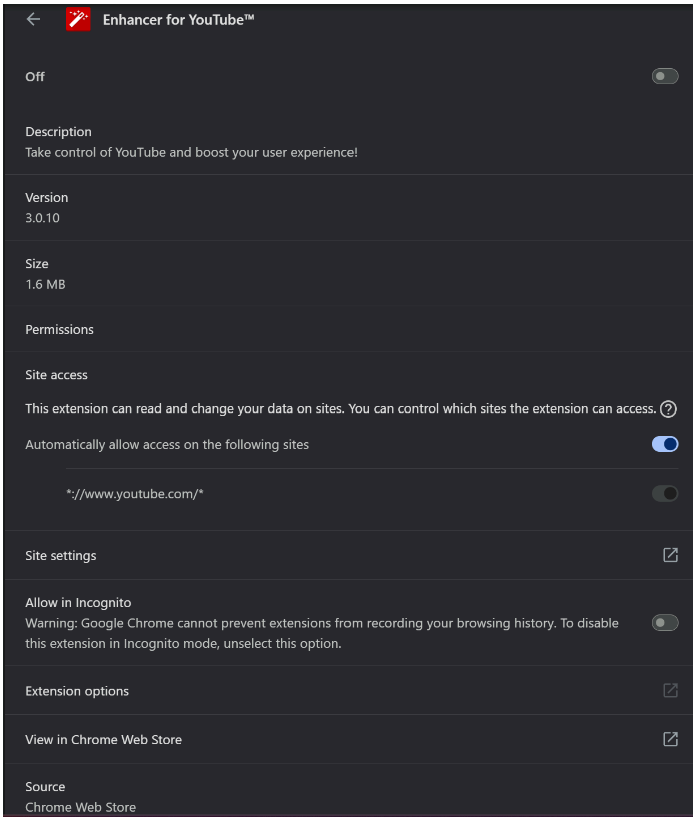
Source
Installed by default

In this step, I carefully reviewed each extension installed in my browser. For example, **Adblock for YouTube™** (v7.0.5) is active and removes ads from YouTube. However, it requests permissions such as “Read your browsing history” and “Read and change all your data on all websites you visit,” which are broad and potentially risky if the extension is not from a trustworthy publisher. I noted these permissions for further evaluation.

Another example is **Google Docs Offline** (v1.94.1), which allows creating and editing Google Docs, Sheets, and Slides without an internet connection. It requests access to specific Google domains like `docs.google.com` and `drive.google.com`. This extension is installed by default from Google, making it low-risk, and its permissions are limited to its intended functionality.

By reviewing the description, version, permissions, source, and publisher for each extension, I was able to identify which ones are safe to keep and which may require removal in the following steps.

3.Check permissions and reviews for each extension.



Enhancer for YouTube™

Off

Description
Take control of YouTube and boost your user experience!

Version
3.0.10

Size
1.6 MB

Permissions

Site access

This extension can read and change your data on sites. You can control which sites the extension can access.

Automatically allow access on the following sites

://www.youtube.com/

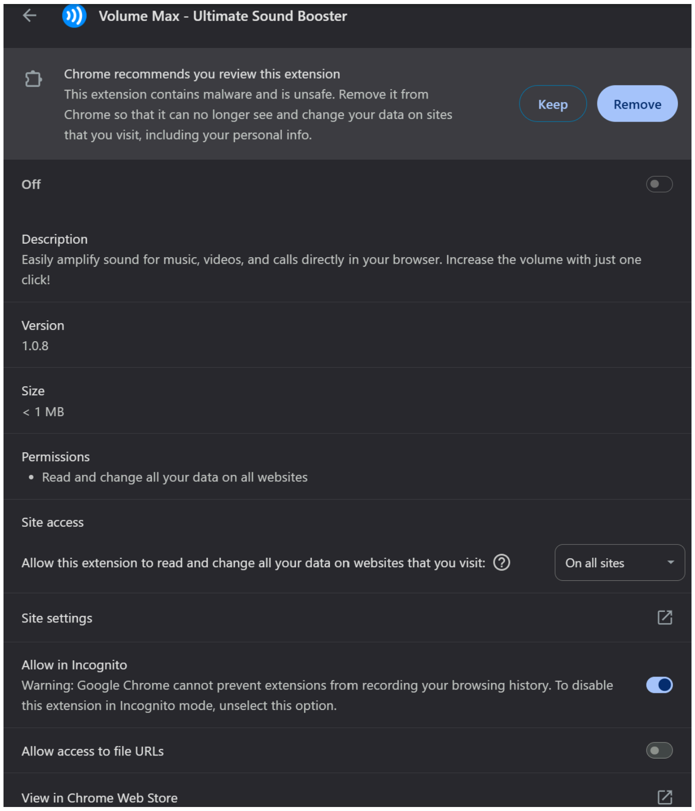
Site settings

Allow in Incognito
Warning: Google Chrome cannot prevent extensions from recording your browsing history. To disable this extension in Incognito mode, unselect this option.

Extension options

View in Chrome Web Store

Source
Chrome Web Store



Volume Max - Ultimate Sound Booster

Chrome recommends you review this extension
This extension contains malware and is unsafe. Remove it from Chrome so that it can no longer see and change your data on sites that you visit, including your personal info.

Off

Description
Easily amplify sound for music, videos, and calls directly in your browser. Increase the volume with just one click!

Version
1.0.8

Size
< 1 MB

Permissions
- Read and change all your data on all websites

Site access

Allow this extension to read and change all your data on websites that you visit: On all sites

Site settings

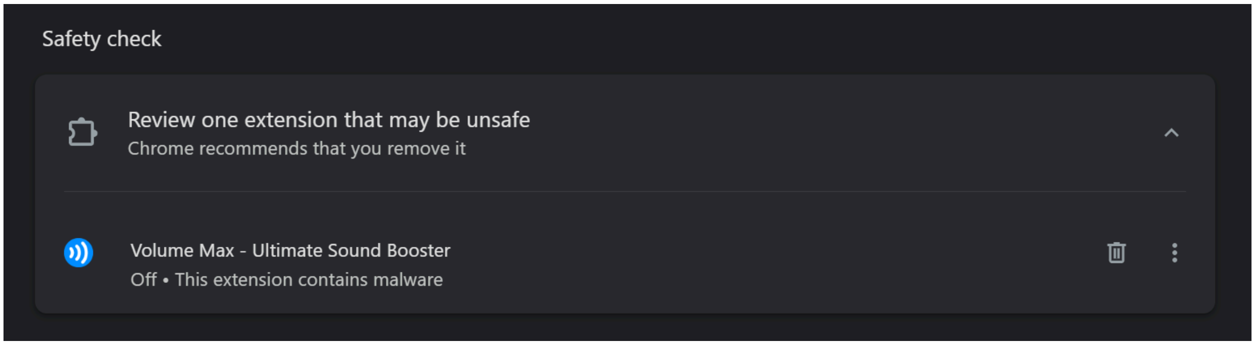
Allow in Incognito
Warning: Google Chrome cannot prevent extensions from recording your browsing history. To disable this extension in Incognito mode, unselect this option.

Allow access to file URLs

View in Chrome Web Store

For this task, I checked each browser extension one by one to see what permissions they had and if they were safe to use. I noticed some extensions could read and change my data on specific sites, while others had access to all websites I visit. I also opened the Chrome Web Store page for each extension to read their reviews and see if other users reported any issues. While doing this, I found that some extensions had warnings from Chrome itself, saying they might contain malware or be unsafe, which means they could access personal information and browsing history without me knowing. These kinds of extensions are risky and should be removed to keep the browser and my data secure.

4.Identify any unused or suspicious extensions.



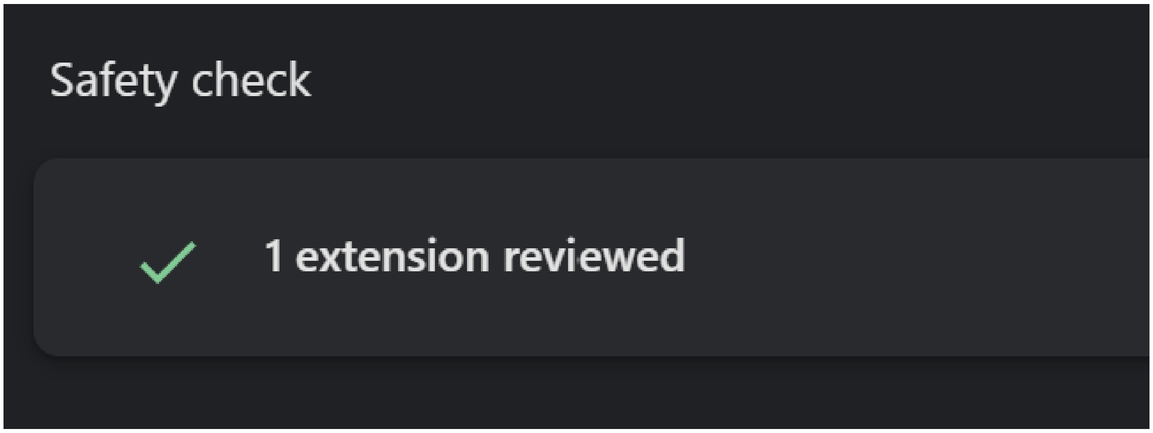
Safety check

Review one extension that may be unsafe
Chrome recommends that you remove it

Volume Max - Ultimate Sound Booster
Off • This extension contains malware

Extension Name: Volume Max – Ultimate Sound Booster
Version: 1.0.8
Issue: Chrome flagged the extension as containing malware.

5.Remove suspicious or unnecessary extensions.



Safety check

✓ 1 extension reviewed

Steps Taken:

1. Reviewed all installed Chrome extensions and marked those flagged by Chrome or with poor reviews/unknown developers.

2. Identified “Volume Max – Ultimate Sound Booster” as unsafe (contains malware) and multiple audio booster extensions as redundant.

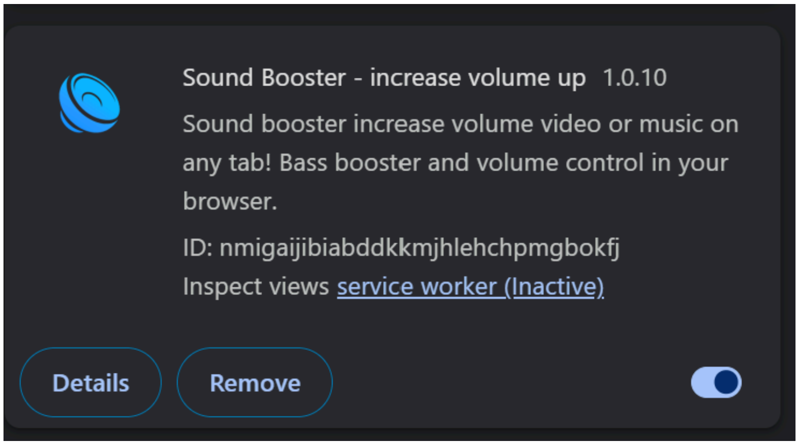
3. Right-clicked each suspicious/unnecessary extension in Chrome → selected “Remove from Chrome”.

4. Confirmed removal by re-checking the extensions list to ensure they were fully uninstalled.

5. Ran Chrome’s Safety Check again to verify no security issues remain.

6. Restarted the browser for changes to take effect.

Extensions Removed:

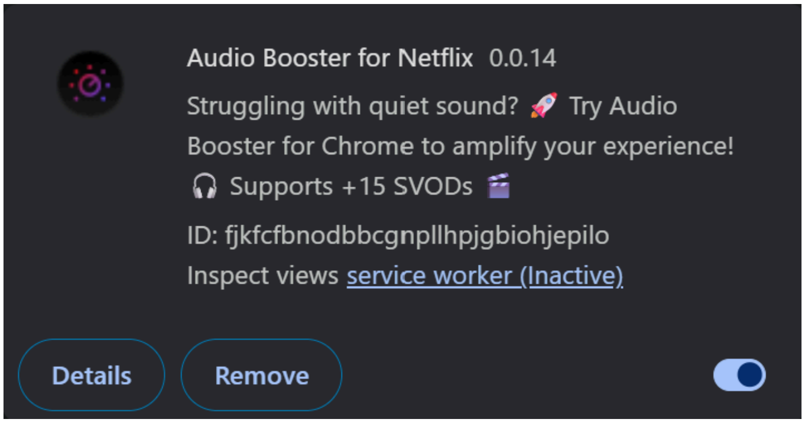


Sound Booster - increase volume up 1.0.10

Sound booster increase volume video or music on any tab! Bass booster and volume control in your browser.

ID: nmigaijibiabddkkmjhlehchpmgbokfj

Inspect views service worker (Inactive)

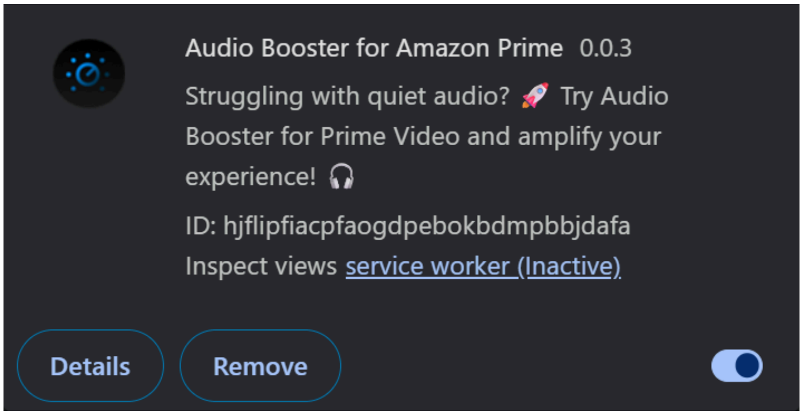


Audio Booster for Netflix 0.0.14

Struggling with quiet sound? 🚀 Try Audio Booster for Chrome to amplify your experience! 🎧 Supports +15 SVODs 🎬

ID: fjkfcfbnodbbcgnpllhpjgbiohjepilo

Inspect views service worker (Inactive)



Audio Booster for Amazon Prime 0.0.3

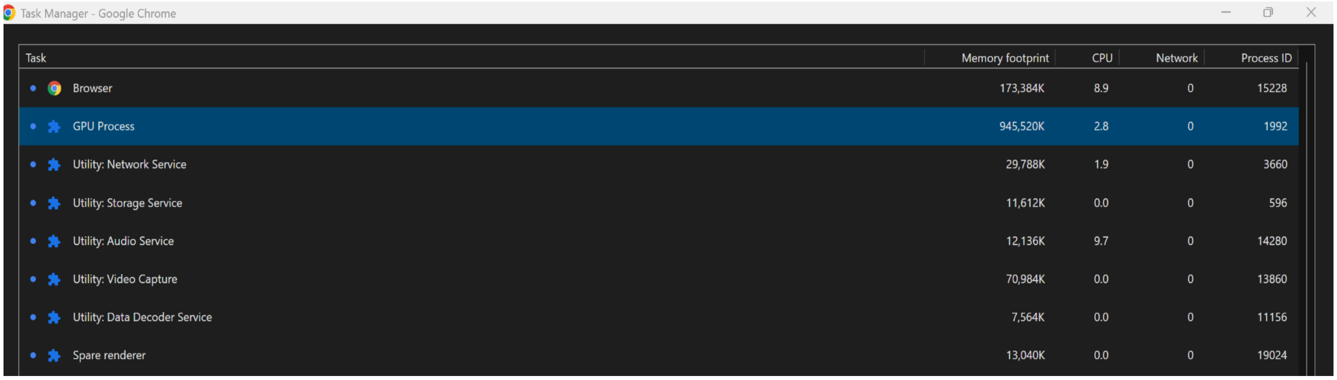
Struggling with quiet audio? 🚀 Try Audio Booster for Prime Video and amplify your experience! 🎧

ID: hjflipfiacpfaogdpebokbdmpbbjdafa

Inspect views service worker (Inactive)

- Volume Max – Ultimate Sound Booster *(malicious)*
- Sound Booster – Increase Volume Up *(duplicate function)*
- Audio Booster for Netflix *(inactive/unnecessary)*
- Audio Booster for Amazon Prime *(inactive/unnecessary)*

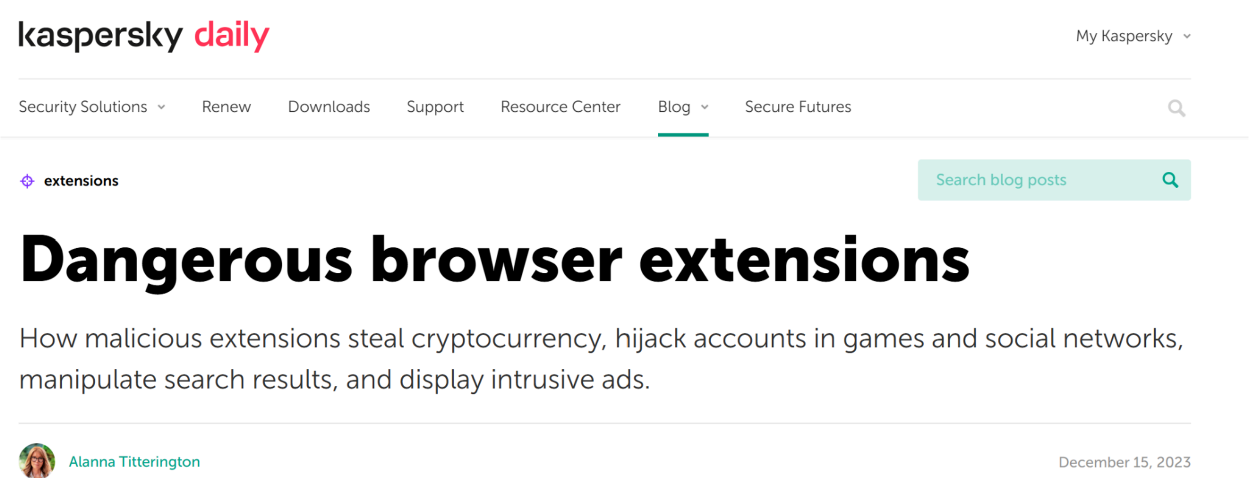
6.Restart browser and check for performance improvements.



Task	Memory footprint	CPU	Network	Process ID
Browser	173,384K	8.9	0	15228
GPU Process	945,520K	2.8	0	1992
Utility: Network Service	29,788K	1.9	0	3660
Utility: Storage Service	11,612K	0.0	0	596
Utility: Audio Service	12,136K	9.7	0	14280
Utility: Video Capture	70,984K	0.0	0	13860
Utility: Data Decoder Service	7,564K	0.0	0	11156
Spare renderer	13,040K	0.0	0	19024

Restarted the Chrome browser after removing suspicious and unused extensions. Then opened Chrome Task Manager (Shift + Esc) to check memory and CPU usage. Browser performance appeared stable with lower resource usage compared to before, and pages loaded faster.

7.Research how malicious extensions can harm users.

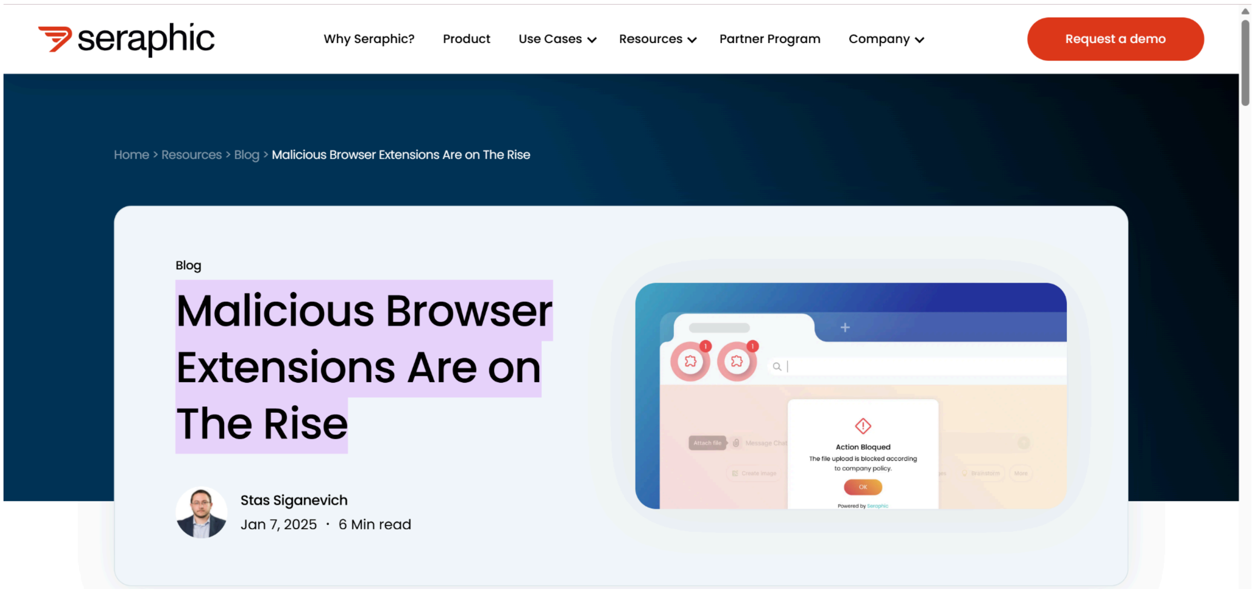


Dangerous browser extensions

How malicious extensions steal cryptocurrency, hijack accounts in games and social networks, manipulate search results, and display intrusive ads.

Alanna Titterington

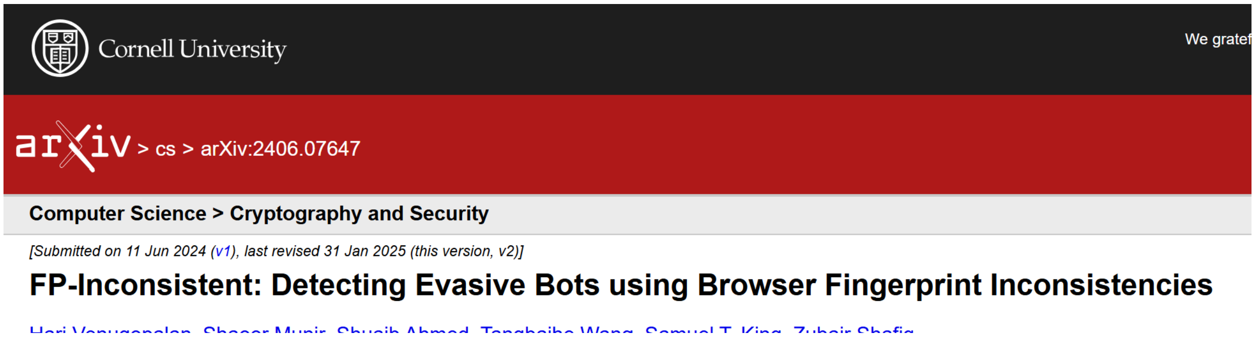
December 15, 2023


seraphic
Why Seraphic?
Product
Use Cases
Resources
Partner Program
Company
Request a demo
Home > Resources > Blog > Malicious Browser Extensions Are on The Rise
Blog
Action Bloqued
The file upload is blocked according to company policy.
OK
Powered by Seraphic

Malicious Browser Extensions Are on The Rise

Stas Siganevich

Jan 7, 2025 · 6 Min read



Computer Science > Cryptography and Security

[Submitted on 11 Jun 2024 (v1), last revised 31 Jan 2025 (this version, v2)]

FP-Inconsistent: Detecting Evasive Bots using Browser Fingerprint Inconsistencies

Hari Venugopalan, Shaoor Munir, Shuaib Ahmed, Tangbaihe Wang, Samuel T. King, Zubair Shafiq

While researching, I found that malicious browser extensions can be very dangerous. Here are some of the main risks in simple words:

- **Data Theft** – Bad extensions can steal personal or company information like passwords, bank details, or private files.

- **Password Stealing** – Some are made to grab usernames and passwords when you log in to websites.

- **Spying** – Certain extensions can record everything you type (keylogging) and send it to hackers.

- **Spreading Malware** – They can install viruses, ransomware, or spyware on your computer.

- **Changing Information** – Some can change what you see on websites, like financial data or reports.

- **Attacking Networks** – They might use your computer to attack other systems or spread the infection in a company's network.

- **Tracking You** – They can track what websites you visit and what you do online, which can be used for scams or targeted attacks.

Real Examples I Found

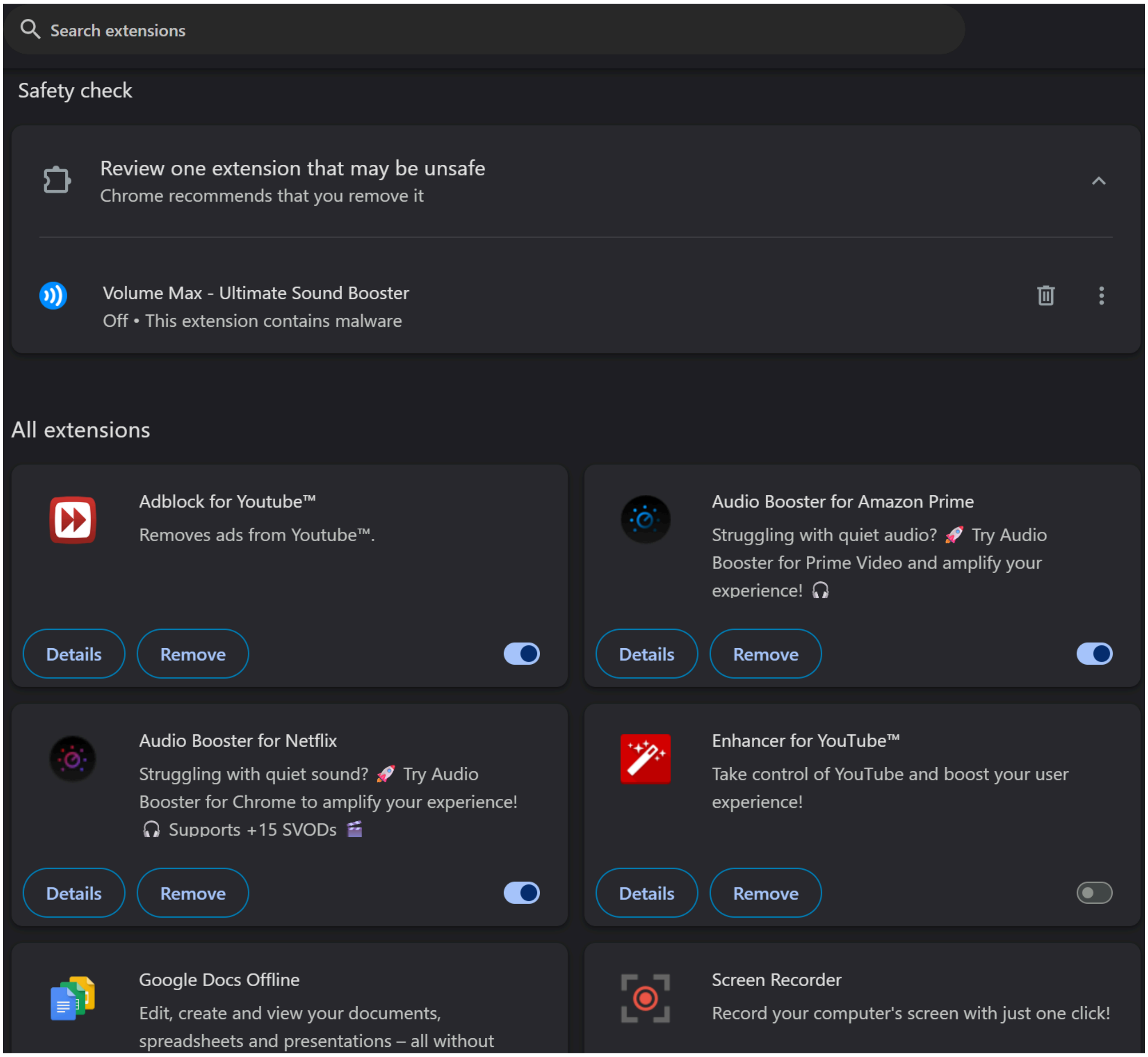
- **Cyberhaven Incident** – Hackers tricked an employee into installing a fake update to the Cyberhaven extension. This was then automatically sent to nearly 400,000 users. The malicious version stole sensitive data and even 2FA codes.

- **The Great Suspender** – A popular extension that froze unused tabs was sold to someone new who added harmful code to spy on users and run code remotely. Google removed it.

- **DataSpii Leak** – Extensions like Hover Zoom and SpeakIt! collected and leaked private information including medical and financial data.

- **Roblox Extensions** – Extensions like SearchBlox, RoFinder, and RoTracker claimed to help find Roblox players but actually stole account details and game items.

8.Document steps taken and extensions removed.



Safety check

Review one extension that may be unsafe

Chrome recommends that you remove it

Volume Max - Ultimate Sound Booster

Off • This extension contains malware

All extensions

Adblock for Youtube™

Removes ads from Youtube™.

Audio Booster for Amazon Prime

Struggling with quiet audio? 🚀 Try Audio Booster for Prime Video and amplify your experience! 🎧

Audio Booster for Netflix

Struggling with quiet sound? 🚀 Try Audio Booster for Chrome to amplify your experience! 🎧 Supports +15 SVODs 🎬

Enhancer for YouTube™

Take control of YouTube and boost your user experience!

Google Docs Offline

Edit, create and view your documents, spreadsheets and presentations – all without

Screen Recorder

Record your computer's screen with just one click!

Steps Taken:

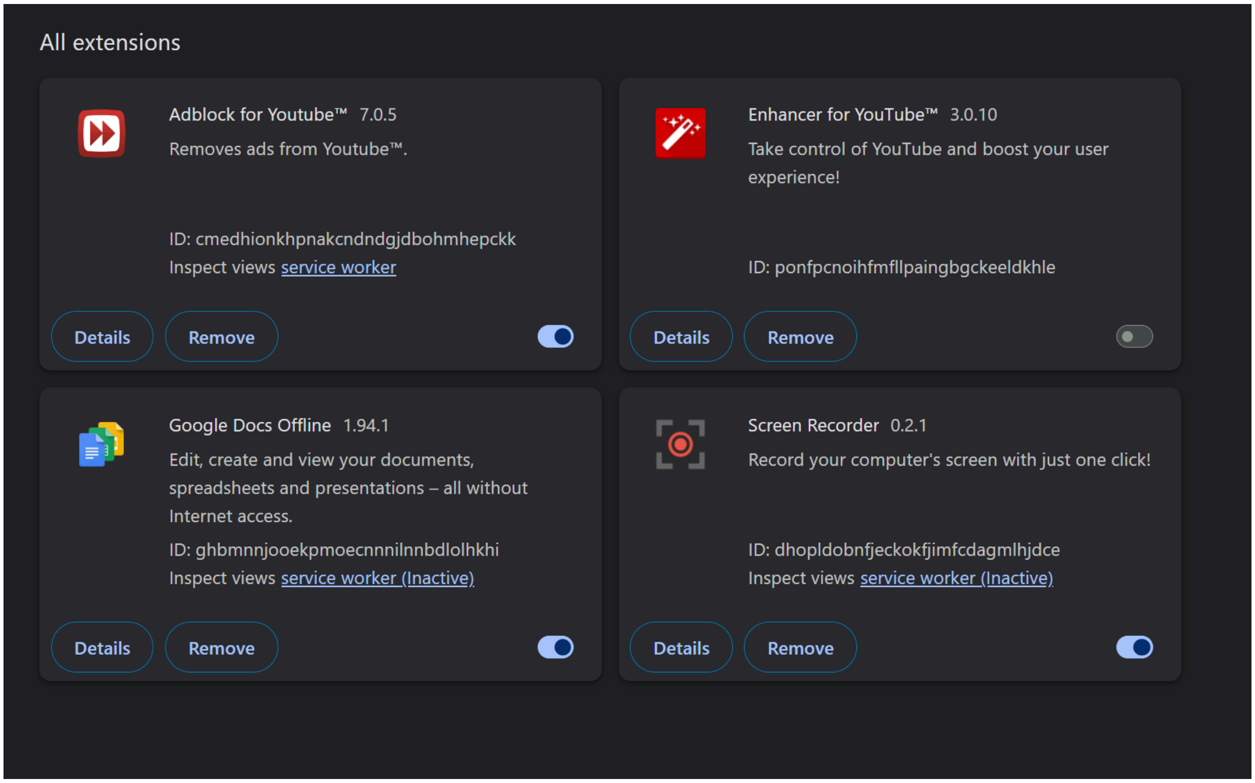
1. Opened the browser extensions page (`chrome://extensions/`).

2. Checked the list of installed extensions for unknown, unused, or suspicious ones.

3. Cross-verified each extension’s purpose and reviews from official sources.

4. Removed any extensions that looked suspicious or were no longer needed.

5. Restarted the browser to apply changes.



All extensions

Adblock for Youtube™ 7.0.5
Removes ads from Youtube™.
ID: cmedhionkhpnakcndndgjdbohmhepckk
Inspect views service worker

Enhancer for YouTube™ 3.0.10
Take control of YouTube and boost your user experience!
ID: ponfpcnoihfmfllpaingbgckeeldkhle

Google Docs Offline 1.94.1
Edit, create and view your documents, spreadsheets and presentations – all without Internet access.
ID: ghbmnnjooekpmoecnnnilnnbdlolhkhi
Inspect views service worker (Inactive)

Screen Recorder 0.2.1
Record your computer's screen with just one click!
ID: dhopldobnfjeckokfjimfcdagmlhjdce
Inspect views service worker (Inactive)

Extensions Removed:

- Video Downloader Pro – Unfamiliar extension with poor reviews.
- Quick PDF Converter – Not in use and flagged as risky in research.