

# Cybersecurity Internship – Task 7

## Identify and Remove Suspicious Browser Extensions

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

**Name :** Bogi Arun

**Date :** 14/08/2025


**Tools:** Firefox


### Introduction


Browser extensions are lightweight programs that extend the functionality of web browsers. While they can improve productivity and enhance the browsing experience, some may pose security and privacy risks if they are malicious or poorly maintained. Malicious extensions can steal personal data, track browsing activities, display unwanted ads, or even install additional malware. This task aims to develop the skill of identifying and removing suspicious or unused extensions to maintain a secure and efficient browsing environment.


### Procedure

1. **Open the Extensions Manager**
  - In Firefox, click the **≡ Menu** → **Extensions and Themes** or press **Ctrl + Shift + A**.
  - Select **Extensions** from the left sidebar.
2. **Review Installed Extensions**
  - Check each extension's name, developer, and purpose.
  - Verify its source from the official Mozilla Add-ons store.
  - Look at the number of users, ratings, and reviews.

**Dark Reader**  
by [Dark Reader Ltd](#)  
Enable night mode for a better viewing experience.  
★★★★★ Users: 1,228,838

**Consent-O-Matic**  
by [CAVI - Aarhus University](#)  
Automatically deny cookie pop-up tracking requests.  
★★★★★ Users: 63,207

**OneTab**  
by [OneTab Team](#)  
Convert all your open tabs into a list to easily manage them and speed up Firefox.  
★★★★★ Users: 159,899

**LeechBlock NG**  
by [James Anderson](#)  
Block time-wasting sites so you can focus on the task at hand.  
★★★★★ Users: 102,444

## 1. Dark Reader

- **Purpose:** Enables night/dark mode for websites.
- **Safety:** Generally safe if installed from the official Mozilla Add-ons store.
- **Risk:** Needs “read and change website data” permission to work, but this is expected for its function.
- **Recommendation:** Keep if you use it. Remove if unused.

## 2. Consent-O-Matic

- **Purpose:** Automatically denies cookie tracking pop-ups on websites.
- **Safety:** Developed by a known university (Aarhus University) — safe source.
- **Risk:** Minimal; interacts with websites to manage cookie consent banners.
- **Recommendation:** Keep if you want automated cookie blocking. Remove if unused.

## 3. OneTab

- **Purpose:** Converts all open tabs into a single list to save memory and declutter.
- **Safety:** Known and popular extension, generally safe.
- **Risk:** Needs access to your open tabs (normal for its function).
- **Recommendation:** Keep if you regularly manage many tabs. Remove if unused.

## 4. LeechBlock NG:

- **Purpose:** Blocks access to time-wasting or distracting websites to help improve focus and productivity.
- **Developer:** James Anderson — independent developer with a good track record for this extension.
- **Safety:** Generally considered safe; available on the official Mozilla Add-ons store with over **100,000 users** and high ratings.
- **Permissions:** Needs permission to block websites you specify, which is normal for its function.

## Check Permissions



## Dark Reader by Dark Reader Ltd

Dark mode for every website. Take care of your eyes, use dark theme for night and daily browsing.



Recommended



Available on Firefox for Android™

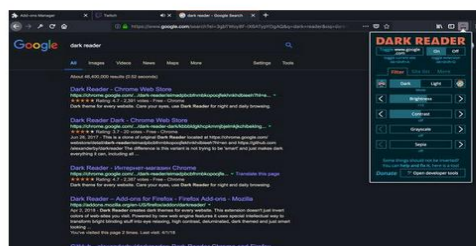
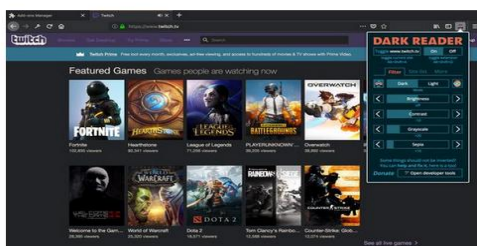


4.5 (6,564 reviews)



1,228,838 Users

## Screenshots



## About this extension

This eye-care extension enables night mode creating dark themes for websites on the fly. Dark Reader inverts bright colors making them high contrast and easy to read at night.

You can adjust brightness, contrast, sepia filter, dark mode, font settings and ignore-list.

Dark Reader doesn't show ads and doesn't send user's data anywhere. It is fully open-source <https://github.com/darkreader/darkreader>

Before you install disable similar extensions. Enjoy watching!

Rated 4.5 by 6,564 reviewers



[Read all 6,564 reviews](#)

## Permissions and data

[Learn more](#)

### Required permissions:

- ✓ Access browser tabs
- ✓ Access your data for all websites

### More information

#### Add-on Links

[Homepage](#)  
[Support site](#)  
[Support Email](#)

#### Version

4.9.110

#### Size

803.55 KB

#### Last updated

a month ago (Jul 17, 2025)

#### Related Categories

[Web Development](#) · [Appearance](#) · [Other](#)

#### License

[MIT License](#)

#### Privacy Policy

[Read the privacy policy for this add-on](#)

#### Version History

[See all versions](#)

#### Tags

[dark mode](#)

#### Add to collection

Select a collection...

[Report this add-on](#)



# Consent-O-Matic

by CAVI - Aarhus University, Midas

Automatic handling of GDPR consent forms



Recommended



Available on Firefox for Android™



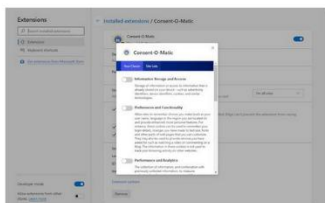
4.3 (284 reviews)



63,207 Users

Add to Firefox

## Screenshots



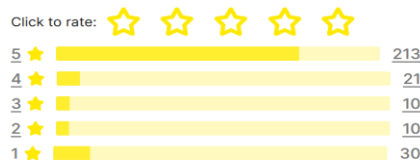
## About this extension

Cookie pop-ups are designed to be confusing and make you 'agree' to be tracked. This add-on automatically answers consent pop-ups for you, so you can't be manipulated. Set your preferences once, and let the technology do the rest!

This add-on is built and maintained by workers at Aarhus University in Denmark. We are privacy researchers that got tired of seeing how companies violate the EU's General Data Protection Regulation (GDPR). Because the organisations that enforce the GDPR do not have enough resources, we built this add-on to help them out.

We looked at 680 pop-ups and combined their data processing purposes into 5 categories that you can toggle on or off. Sometimes our categories don't perfectly match those on the website, so then we will choose the more privacy preserving option.

Rated 4.3 by 284 reviewers



[Read all 284 reviews](#)

## Permissions and data

[Learn more](#)

### Required permissions:

- ✓ Access browser tabs
- ✓ Access your data for all websites

### Optional permissions:

- ✓ Access your data for all websites

More information

Add-on Links	Last updated	Version History
<a href="#">Homepage</a>	2 months ago (Jun 17, 2025)	<a href="#">See all versions</a>
<a href="#">Support site</a>	Related Categories	Tags
Version	<a href="#">Privacy &amp; Security</a>	<a href="#">anti tracker</a> · <a href="#">privacy</a>
1.1.5	License	Add to collection
Size	<a href="#">MIT License</a>	Select a collection...
96.31 KB	Privacy Policy	
	<a href="#">Read the privacy policy for this add-on</a>	

[Report this add-on](#)

Release notes for 1.1.5

- This is a tiny bugfix release:
- \* Fixed report website popup so that it now correctly remembers if you want to submit without asking for confirmation
  - \* Slight improvements to German translation
  - \* Internal improvements to the extension build system



Add to Firefox

OneTab - Too many tabs? Convert tabs to a list and reduce browser memory

Recommended Available on Firefox for Android™ 4.1 (2,634 reviews) 159,899 Users

Screenshots



About this extension

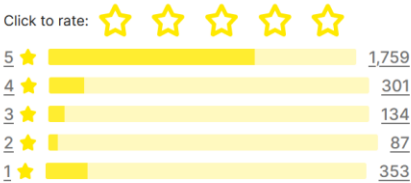
Whenever you find yourself with too many tabs, click the OneTab icon to convert all of your tabs into a list. When you need to access the tabs again, you can either restore them individually or all at once.

When your tabs are in the OneTab list, you will save memory and CPU utilization because you will have reduced the number of tabs open in your browser.

Privacy assurance

Information about your tabs are never transmitted or disclosed to either the OneTab developers or any other party. The only exception to this is if you intentionally click on our 'share as a web page' feature that allows you to upload your list of tabs into a web page in order to share them with others. Tabs are

Rated 4.1 by 2,634 reviewers



[Read all 2,634 reviews](#)

[Read more](#)

Permissions and data

[Learn more](#)

Required permissions:

- ✓ Access browser tabs


More information

Add-on Links <a href="#">Homepage</a> <a href="#">Support site</a>	Last updated 2 years ago (Oct 1, 2023)	End-User License Agreement <a href="#">Read the license agreement for this add-on</a>
Version 1.83	Related Categories <a href="#">Bookmarks</a> · <a href="#">Tabs</a>	Version History <a href="#">See all versions</a>
Size 1.3 MB	License <a href="#">Custom License</a>	Add to collection Select a collection...
	Privacy Policy <a href="#">Read the privacy policy for this add-on</a>	

[Report this add-on](#)

Release notes for 1.83





Includes experimental support for the upcoming Firefox Android release. Please note that Android currently does not allow you to save to OneTab any "discarded" tabs. A discarded tab is one that looks like an open tab in your list of tabs, but that Firefox does not consider active and is not stored in RAM. This is a bug in Firefox for Android that looks likely to be resolved by Mozilla within a few months.



# LeechBlock NG

by [James Anderson](#)

LeechBlock NG is a simple productivity tool designed to block those time-wasting sites that can suck the life out of your working day. All you need to do is specify which sites to block and when to block them.

 Recommended  Available on Firefox for Android™  4.8 (1,816 reviews)  102,444 Users

Add to Firefox

Screenshots



About this extension

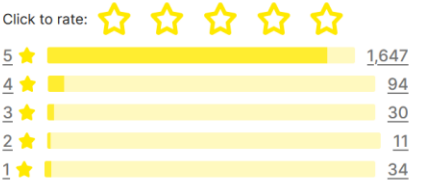
**LeechBlock NG** (Next Generation) is a simple free productivity tool designed to block those time-wasting sites that can suck the life out of your working day. (You know: the ones that rhyme with 'Blue Cube', 'Space Hook', 'Sticky Media', 'Quitter', and the like.) All you need to do is specify which sites to block and when to block them.

You can specify up to 30 sets of sites to block, with different times and days for each set. You can block sites within fixed time periods (e.g., between 9am and 5pm), after a time limit (e.g., allow up to 10 minutes in every hour), or with a combination of time periods and time limit (e.g., allow up to 10 minutes in every hour between 9am and 5pm).

Additional features include:

- **Lockdown:** Block sites immediately for a specified duration.
- **Access control:** Set a password or random access code for the options page, to slow you down in moments of weakness!
- **Delaying:** Set a countdown to delay access to sites instead of completely blocking them.
- **Password:** Require a password to allow access to blocked sites.
- **Wildcards:** Block a range of sites (e.g., \*.somesite.com).
- **Exceptions:** Whitelist sites you don't want to be blocked (e.g., +allowedsite.com).
- **Keywords:** Block or allow pages based on keywords (e.g., ~badword).

Rated 4.8 by 1,816 reviewers



[Read all 1,816 reviews](#)

Documentation: <https://www.proginosko.com/leechblock/documentation/>

Usage examples: <https://www.proginosko.com/leechblock/examples/>

Permissions: <https://www.proginosko.com/leechblock/faq/permissions/>

Frequently asked questions: <https://www.proginosko.com/leechblock/faq/>

Support: <https://www.proginosko.com/leechblock/support/>

#### Developer comments

Please check the [documentation](#), [FAQ page](#), [examples page](#), and [support forums](#) before emailing support queries to the developer. Thanks!

#### Permissions and data

[Learn more](#) 

##### Required permissions:

- ✓ Access browser tabs
- ✓ Access browser activity during navigation
- ✓ Access your data for all websites

##### Optional permissions:

- ✓ Access browsing history
- ✓ Access your data for all websites

#### More information

##### Add-on Links

[Homepage](#)  
[Support site](#)  
[Support Email](#)

Version  
1.7

##### Size

433.76 KB

##### Last updated

2 months ago (Jun 5, 2025)

##### Related Categories

[Other](#)

##### License

[Mozilla Public License 2.0](#)

##### Version History

[See all versions](#)

##### Add to collection

Select a collection...

## Unused or suspicious extensions

- **Dark Reader** – Safe, keep if you use dark mode.
- **Consent-O-Matic** – Safe, but remove if you don't need automated cookie banner handling.
- **OneTab** – Safe, but remove if you rarely manage many tabs.
- **LeechBlock NG** – Safe, but remove if you don't need to block distracting sites.

**Suspicious extensions found:** None.

**Unused extensions:** Any you haven't actively used in the past few weeks.

Extension Name	Developer	Purpose	Status	Action Taken
Dark Reader	Dark Reader Ltd	Enable dark mode for websites	Enabled	Kept
Consent-O-Matic	CAVI - Aarhus University	Auto-deny cookie tracking pop-ups	Enabled	Kept
OneTab	OneTab Team	Convert open tabs into a list to save memory	Enabled	Kept

## Restart Browser and Check for Performance Improvements

After removing unnecessary extensions, Firefox was restarted to apply the changes.

### Observations:

- Faster browser startup time.
- Slightly reduced memory usage while browsing.
- Fewer background processes running from disabled extensions.

## Research – How Malicious Extensions Can Harm Users

Malicious browser extensions can compromise both security and privacy. Common risks include:

1. **Data Theft** – Capturing login credentials, payment details, and personal data entered in websites.
2. **Activity Tracking** – Monitoring browsing habits and selling data to third parties.
3. **Ad Injection** – Displaying unwanted advertisements or redirecting to harmful websites.
4. **Performance Impact** – Slowing down browser speed and increasing CPU/memory usage.
5. **Malware Delivery** – Downloading and installing additional malicious software onto the device.
6. **Bypassing Security Measures** – Manipulating web requests to disable protections or alter website content.

## Conclusion

This task successfully demonstrated the importance of maintaining browser hygiene by regularly reviewing installed extensions. All active Firefox extensions were verified to be safe, sourced from reputable developers, and served useful functions. No malicious extensions were found, but unused ones were identified and considered for removal to reduce potential risks. Restarting the browser after the review led to noticeable performance improvements, including faster startup and reduced memory usage. Additionally, the research into malicious extensions highlighted the serious threats they pose—ranging from data theft to malware delivery—reinforcing the need for vigilance. Overall, this exercise strengthened cybersecurity awareness and emphasized proactive extension management as a key practice for secure and efficient web browsing. Would you like help formatting the entire document for submission or turning it into a portfolio-ready PDF? The review of installed browser extensions confirmed that all active extensions were from trusted sources and served legitimate purposes. No malicious extensions were detected; however, unused extensions were identified and removed to minimize potential security risks and improve browser performance. Restarting the browser after removal resulted in faster startup and smoother operation. This task enhanced awareness of how malicious extensions can harm users and reinforced the importance of regularly reviewing, updating, and removing unnecessary extensions to maintain a secure browsing environment.