

Need to block malicious visits to your WordPress site?

Putting the word malicious into any statement related to your WordPress website is obviously not a good thing. The internet is the Wild Wild West and it is full of many bank robbers and train hijackers.

A malicious visit to a WordPress website is intended to do one of the two things below or sometimes both.

1. The first and most common intention is to share spammy content that includes click-bait.
2. The second intention which is the worst of the two is to **infect and harm your website**.

Now before we dive in deep about how to block malicious visits to your WordPress website, it is important to first understand that these visits are not being brought upon because of something that you are not doing.

Hackers and **spam bot** programs alike are constantly on the hunt for websites that they can inject their malicious activity into your website. You could be one of those targeted locations that is being hit with malicious activity and you are not even aware of it.

This malicious activity that may be happening on your website might never lead to anything that causes worry but it can affect the overall performance of your website.

You see every visit to your website triggers resources on your server that need to run in order for that visit to take place. If these resources are being used by malicious activity, it is

pulling away server power that can be used for the visits that are not malicious.

In this article we are going to identify any malicious visits to your WordPress website and then show you exactly how to block malicious visits to your WordPress website.

1. How to Identify Malicious Visits to Your WordPress Site

In order for us to take action to block malicious visits to your WordPress site, we need to identify which visits are malicious and where they are coming from.

Every visit to your website has a unique IP address which is the address of the visitor's origin device. We need to find this information and there are a few plugins that are free to use which will be our visitor detectives.

They are going to be a few ingredients that we will need on our website in way of plugins to identify and block malicious visits to your WordPress site.

THE INGREDIENTS:

1. Akismet Spam Protection Plugin

Akismet checks your comments and **contact form** submissions against our global database of spam to prevent your site from publishing malicious content. You can review the comment spam it catches on your blog's "Comments" admin screen.

The main reason for this plug-in is to take a proactive approach in isolating malicious or spam focused comments on your WordPress website. If you are running a WordPress

website that does not allow the ability to comment on content you can ignore the use of this plugin. It is only used to filter and target comments that are visitor generated.

There definitely are other spam fighting plugins available and you are welcome to use another one versus what we are recommending here as long as it will be a plugin that takes action in the background to isolate spam generated comments on your WordPress website.






Once you have this plugin installed and set up it will add a category under the comments section in your administrative area called "***Spam***". This plugin will automatically identify the spam comments on your WordPress website using dynamic spam filters.

We will now have a place where we can look at the malicious visits that are happening in the comments section of our WordPress website and identify the IP address in which these visits are coming from. Please take a look at the image below.

Comments

All (952) | Mine (270) | Pending (0) | Approved (952) | **Spam (15)** | Trash (17)

Bulk actions All comment types

<input type="checkbox"/>	Author	Comment	In response to	Submitted on
<input type="checkbox"/>	 Hello World x83mnnm@gmail.com 103.101.194.34	https://sdokf34h35hdfgb.com https://sdokf34h35hdfgb.com	How to Lower Bounce Rate on Your WordPress Site – 10 Tips View Post	2021/09/08 at 8:40 pm
<input type="checkbox"/>	 Hello World hcutfbfo@gmail.com 103.101.194.34	https://sdokf34h35hdfgb.com https://sdokf34h35hdfgb.com	Hide WooCommerce Cart Icon When Empty View Post	2021/09/08 at 8:39 pm
<input type="checkbox"/>	 Hello World jec4t3bt@gmail.com 103.101.194.34	https://sdokf34h35hdfgb.com https://sdokf34h35hdfgb.com	What Should You Do To Remove WordPress Google Blacklist View Post	2021/09/08 at 8:39 pm
<input type="checkbox"/>	 Hello World r7fed6nn@gmail.com 103.101.194.34	https://sdokf34h35hdfgb.com https://sdokf34h35hdfgb.com	What is WordPress Malware and How Can You Remove It View Post	2021/09/08 at 8:38 pm
<input type="checkbox"/>	 Hello World lmr6nz5r@gmail.com 103.101.194.34	https://sdokf34h35hdfgb.com https://sdokf34h35hdfgb.com	Speeding Up Your WordPress Website – 4 Easy Methods View Post	2021/09/08 at 8:37 pm

 BAD SPAM COMMENTS – Block Malicious Visits to Your WordPress Site

2. SiteGround Security Plugin

The main reason we will be using this plugin is for the feature included which is the **Activity Log**.


With this feature, you can monitor in detail the activity of registered, unknown and blocked visitors. If your site is being hacked, a user or a plugin was compromised, you can always use the quick tools to block their future actions.

The Activity Log feature of this plugin will give you a snapshot of each visit to your website in regards to what URL is being visited and from what unique IP address.

Take a look at the image below on how you can use the Activity Log in this plugin to view the visits to your website and know

instantly the URL that is being visited and the IP address that is generating the visit.

SiteGround Security - Activity Log

 The activity log can help you monitor your site and login page for unauthorised visitors or brute force attempts. You can easily block and unblock IPs or visitors that look suspicious and prevent them from malicious actions.

UNKNOWN REGISTERED BLOCKED

Unknown Visitors Activity

Timestamp	Visitor Type	IP Address	Page Visited	Response	Actions
2021-09-09 07:55	Googlebot	66.249.73.187 ⓘ	/product/standard-kis-plan	301	⋮
2021-09-09 07:55	Googlebot	66.249.73.191 ⓘ	/unlimited-monthly-wordpress-support/	301	⋮
2021-09-09 07:55	Human	154.13.48.70 ⓘ	/allow-access-to-your-site-without-a-username-and-password	301	⋮
2021-09-09 07:49	Human	223.91.3.17 ⓘ	/contact-us/	301	⋮
2021-09-09 07:49	Human	223.91.3.17 ⓘ	/shop/my-account/	200	⋮
2021-09-09 07:48	Human	180.150.38.97 ⓘ	/shop/my-account/	200	⋮
2021-09-09 07:47	Human	157.245.117.2 ⓘ	/feed/	200	⋮
2021-09-09 07:46	Human	178.159.37.172 ⓘ	/stop-wordpress-spam/	200	⋮
2021-09-09 07:46	Human	178.159.37.172 ⓘ	New comment posted by DianePhons on Best Way to Stop Wo...	200	⋮
2021-09-09 07:45	UptimeRobot	63.143.42.253 ⓘ	/	200	⋮
2021-09-09 07:45	UptimeRobot	216.245.221.91 ⓘ	/	200	⋮

 SEE ALL SITE VISITS – Block Malicious Visits to Your WordPress Site

2. Auto Trash Spam to Block Malicious Visits to Your WordPress Site

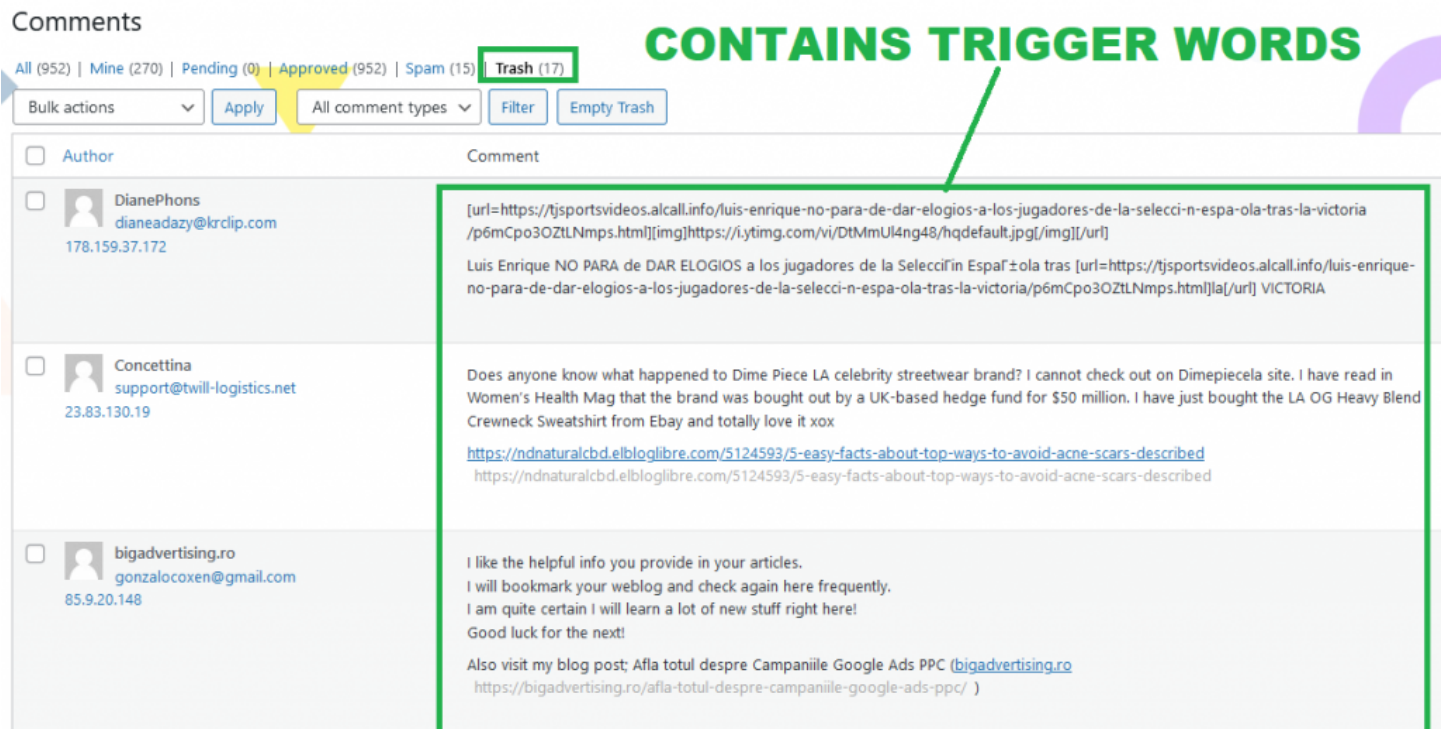
There is a power move that you can do in order to auto trash the majority of spam comments that are created on your WordPress website. This is an important step as well to block malicious visits to your WordPress website.

What this means is that you can set up certain words that will trigger an automatic response from your WordPress website to not approve the submitted comment and directly move it to the trash bin.

Check out the image below to see an example of comments that were submitted to a site which contained trigger words and were automatically put into the trash bin in the Comments area.

We have compiled a detailed post on how you can set up these trigger words which you can read all about at the link below.

<https://www.wpfixit.com/stop-wordpress-spam/>



The screenshot shows the WordPress 'Comments' management interface. At the top, there are filters for 'All (952)', 'Mine (270)', 'Pending (0)', 'Approved (952)', 'Spam (15)', and 'Trash (17)'. The 'Trash (17)' filter is selected and highlighted with a green box. A green arrow points from the text 'CONTAINS TRIGGER WORDS' to the 'Trash (17)' filter. Below the filters, there are buttons for 'Bulk actions', 'Apply', 'All comment types', 'Filter', and 'Empty Trash'. The main area displays a list of comments. Three comments are visible, each with a checkbox, author information, and the comment text. The comment text for the first comment is highlighted with a green box. The comment text for the second comment is also highlighted with a green box. The comment text for the third comment is also highlighted with a green box.

Comments

All (952) | Mine (270) | Pending (0) | Approved (952) | Spam (15) | **Trash (17)**

Bulk actions | Apply | All comment types | Filter | Empty Trash

Author	Comment
<input type="checkbox"/> DianePhons dianeadazy@krclip.com 178.159.37.172	[url=https://tjsportsvideos.alcall.info/luis-enrique-no-para-de-dar-elogios-a-los-jugadores-de-la-selecci-n-espa-ola-tras-la-victoria/p6mCpo3OZtLNmps.html][img]https://i.ytimg.com/vi/DtMmU4ng48/hqdefault.jpg[/img]][/url] Luis Enrique NO PARA de DAR ELOGIOS a los jugadores de la Selecci'in Espaf±ola tras [url=https://tjsportsvideos.alcall.info/luis-enrique-no-para-de-dar-elogios-a-los-jugadores-de-la-selecci-n-espa-ola-tras-la-victoria/p6mCpo3OZtLNmps.html][a]a[/a] VICTORIA
<input type="checkbox"/> Concettina support@twill-logistics.net 23.83.130.19	Does anyone know what happened to Dime Piece LA celebrity streetwear brand? I cannot check out on Dimepiecela site. I have read in Women's Health Mag that the brand was bought out by a UK-based hedge fund for \$50 million. I have just bought the LA OG Heavy Blend Crewneck Sweatshirt from Ebay and totally love it xox https://ndnaturalcbd.elbloglibre.com/5124593/5-easy-facts-about-top-ways-to-avoid-acne-scars-described https://ndnaturalcbd.elbloglibre.com/5124593/5-easy-facts-about-top-ways-to-avoid-acne-scars-described
<input type="checkbox"/> bigadvertising.ro gonzalocoxen@gmail.com 85.9.20.148	I like the helpful info you provide in your articles. I will bookmark your weblog and check again here frequently. I am quite certain I will learn a lot of new stuff right here! Good luck for the next! Also visit my blog post; Afla totul despre Campaniile Google Ads PPC (bigadvertising.ro) https://bigadvertising.ro/afla-totul-despre-campaniile-google-ads-ppc/)

🔪 TRASH THOSE NASTIES – Block Malicious Visits to Your WordPress Site

3. How to Block Malicious Visits to Your WordPress Site

Let's now move on to the next phase in order to block malicious visits to your WordPress website.

In the first phase we talked about using some free [WordPress plugins in order to identify the malicious](#) visits and gather some information on where those visitors are coming from.

The information that we gathered is the unique IP address that the visitor was using to deliver their malicious visit.

Now simply put, we are going to take action and block that IP address from visiting your website.

Doing this will make sure that if another visit is delivered from that IP address, that visit will not be completed.

Ban IP Addresses From Commenting on Your Site

If you just want to stop users with a specific IP address from leaving a comment on your site, then you can do that inside your WordPress admin area.

You would use the information that you gathered earlier in this post which is the IP addresses of these malicious visits that we tracked down.

Head over to Settings » Discussion page and scroll down to 'Comment Blacklist' text box.

Disallowed Comment Keys

When a comment contains any of these words in its content, author name, URL, email, IP address, or browser's user agent string, it will be put in the Trash. One word or IP address per line. It will match inside words, so "press" will match "WordPress".



IP_ADDRESS_GOES_HERE

 **BLOCK IP FROM COMMENTS** – Block Malicious Visits to Your WordPress Site

Copy and paste the IP addresses that you want to block and then click on the save changes button.

WordPress will now block users with these IP addresses from leaving a comment on your website. These users will still be able to visit your website, but they will see an error message when they try to submit a comment.

Ban IP Addresses From Your Site Completely

Of course, you may also want to block users with a pattern of suspicious activity from accessing your site altogether. To do that, you can make a simple addition to one of your WordPress files. Make sure you have [a recent backup](#) in place first, as a security precaution.

This is a much better approach because while you may identify that these malicious visits are generating spammy comments, they also may be trying to infiltrate and attack the integrity of your website through infectious processes.

It is better just to block the entire IP address altogether.

You will need to log into your site directly using File Transfer Protocol (FTP). If you've never done this before, you can check out [a beginner's guide to FTP](#).

With your FTP client open and running, look for your website's root folder. This is often named after your domain, but might also be called *www* or *root*. With this folder highlighted, find [the .htaccess file](#):



Right-click on this file, and select *View/Edit*. This will open the file in your default text editor, enabling you to make changes.

On a new line at the bottom of the file, paste in [the following snippet](#):

```
Order Allow,Deny
Allow from all
Deny from 111.222.333.444
```

You will want to replace the string of numbers in the final line with the first IP address you want to block.

Then you can add additional *Deny* lines, each with a new IP. Save the file, and users from those IP addresses will no longer be able to access your site.

If you don't like editing your *.htaccess* file directly, you can also use the free [IP2Location Country Blocker](#):

This plugin enables user to block unwanted traffic from accessing your front end (blog pages) or back end ([admin area](#)) by countries or proxy servers. It helps to reduce spam and unwanted sign ups easily by preventing unwanted visitors from browsing a particular page or entire website.

IP2Location Country Blocker

Frontend

Backend

Statistic

IP Query

Settings

Enable Frontend Blocking

Block countries listed below.

Block all countries **except** countries listed below.

Canada ✕

India ✕

Nigeria ✕

Do not block bots and crawlers.

Show the following page when visitor is blocked.

Default Error 403 Page

Custom Error Page:

URL:

Permanently **block** IP address listed below:

Conclusion – Block Malicious Visits to Your WordPress

Blacklisting might initially sound like a bad thing, but it's actually a very useful method for protecting your website.

By learning how to block IP addresses in WordPress, you can keep hackers and spammers at bay without inconveniencing your legitimate users.