WordPress Malware Removal Guide

Its popularity also makes WordPress the most targeted CMS platform in the world. More than 70% of top ranking websites hosted on WordPress displayed serious security vulnerabilities. Well, your website could also be one among them if you are not strong on the security front.

Here is a quick guide to remove malware from WordPress site. The things you ought to know and do to keep your WordPress website from succumbing to a malware attack.

Contents

So, does it hurt to be at the bottom of the Google results (SERPs)? Indeed, Google has posted this site may be hacked message instead of your site to inform visitors to stay away. If this happened because of an error on your part (bad referencing, use of fraudulent links techniques, etc.) it's quite a thing. But if your site has been hacked and now contains malicious code and your wordpress site is redirecting to another site, it just adds fuel to the fire - and can really hurt your reputation.

If it is hacked, Google will probably add it to the blacklist. Google will not take chances with its reputation. So, if your site is the slightest concern, the search engine will add you to the blacklist, lower your rank in the rankings for which you worked so hard, drop your position in the SERPs and inform all visitors to stay away because your site represents a danger to them.

There are several ways your site can be blacklisted. But in general, when a search engine detects a code or suspicious activity on your site that its internal algorithms determine that it is malicious software, it immediately removes the site from the search results. Rather than jeopardizing the integrity of search results and their security for users, deleting the dubious site is the least resource-intensive action that the search engine can take.

Now, what exactly is malware? In this case, it can be anything that Google deems suspicious, including phishing or phishing schemes, hacks, retrieval of information or email addresses by scrappers, Trojan horses, etc. The sad thing about all this is that in most cases you will not even know that your site has been hacked until your organic search traffic has dropped sharply.

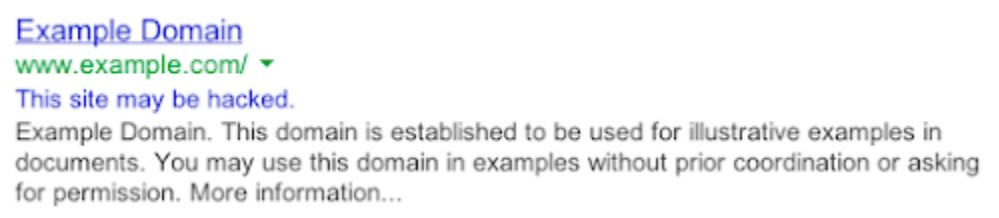
In some cases, however, there will be telling signs that something is wrong. It may look like suspicious things you are experiencing yourself, warnings, stops, or other actions taken by external sources.

Let's face it. There is no 100% secure system in the world. That is why you need WordPress Security services!

There will always be some risks in your system. However, you must take preventive actions, mitigate risks to make sure your website is not vulnerable to attacks.

Most websites usually get hacked due to poor system administration, not using the latest WordPress version, using a weak username/password, Malware infection among many other cases.

However, it is quite easy to secure WordPress if you have good practices and implement the few WordPress malware removal tips that we will provide in this tutorial! Let's go!



Types of Malware Attacks

- Cross-site scripting
- SQL injection:
- Path disclosure:
- WordPress DDoS attacks
- Arbitrary code execution: eval base decode hack
- Cross-site request forgery:
- Data breach (information disclosure):
- File inclusion & remote code execution - Script to exploit this vulnerability are publically available and a Metasploit module has been released too!

What are the symptoms of Malware on a WordPress website?

Improving the security of your site is a very important step. Many hackers choose to make their hacking progressively by starting quietly to set up scripts or malware on your site and then add a wordpress backdoor, for example:

1. Auto download malware, trojans, viruses on page loading.
2. Site Redirecting to another malicious site..
3. Receives a message from Google Search Console that your website is hacked or has malware.
4. Web-host blocks your account.
5. Strange URLs loading in the browser status bar.

The main reason why it is important to start verification of your own site (instead of just visiting it) is that the hacker could know your IP address and put in place a code that shows that your site is secure while in reality, it contains malware.

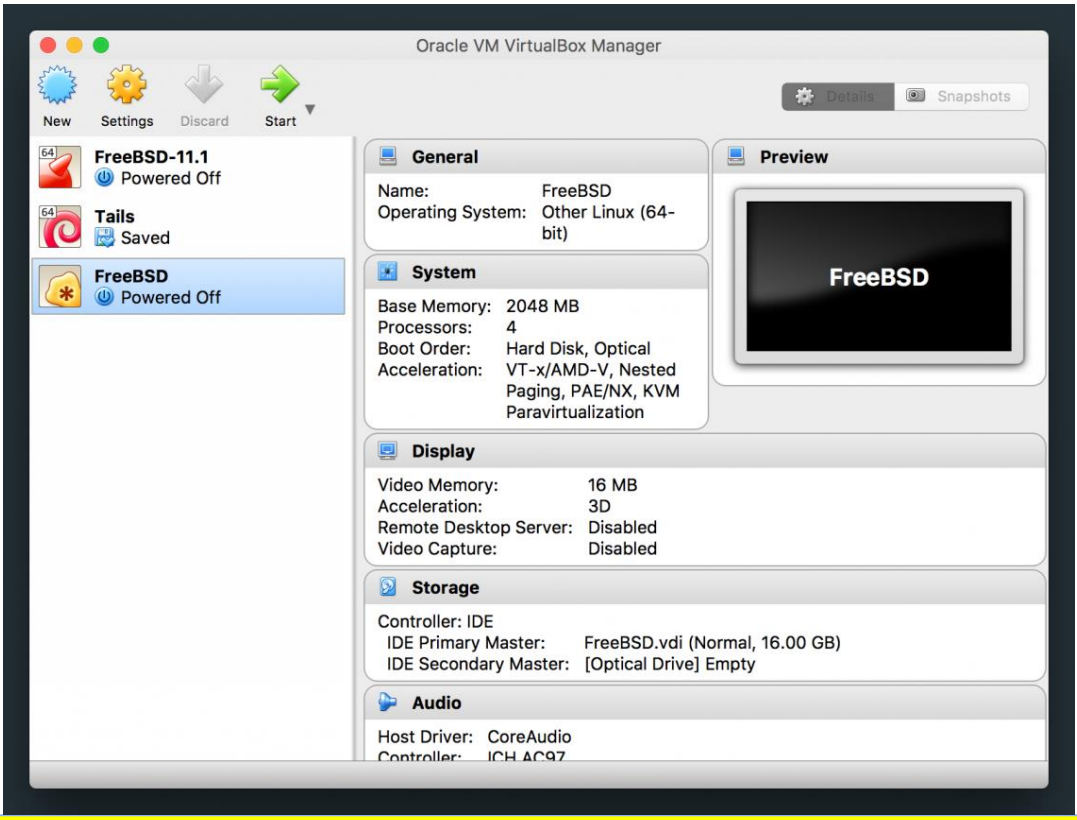
How To Remove Malware From WordPress.

Summary of things you can do for easy WordPress Malware Removal:

- **Run An Antivirus Scan**
- **Run Website Malware Scan**
- **List Files By Modification Date**
- **Scan Downloads Folder**
- **Back up WordPress site**
- **Deactivate Plugins/Clean Up WP-Themes**
- **Change Passwords**
- **Find Malicious Code**
- **Remove Default 'admin' Account**
- **Lock WP Login**
- **Install Security Plugins**
- **Change Hosting Provider**
- **Restore Backup**
- **Request Google Security Review**

1. Diagnose Hacked WordPress Site	2. Be Prepared for future
3. Shut down your site temporarily	4. Regenerate WordPress salts and security keys
5. Change all WordPress passwords	6. Take Full backup of WordPress theme and other important files
7. Take WordPress Database Backup	8. Use GWT and Google Chrome to identify malware issues.
9. Search WP files for malicious code	10. Scan WP folders for malicious files
11. Find Hidden IFRAMES	12. Check User generated Content (UGC)
13. Check location of open redirects	14. Scan internal and external links of your website
15. Check Final destination Of Website traffic	16. Scan Downloadable WP files
17. Check your wp-config.php file	18. Scan your .htaccess file
19. Scan Vulnerable WP plug-ins	20. Find and delete backdoors
21. Look for hidden administrators	22. Scan your computer for Trojans & Viruses
23. Change your web hosting service provider	24. Visit and use "Code Guard.
25. An ultimate solution – intrusion tests	

Get a virtual machine for better security



A virtual machine has its own operating system that uses the hardware resources of an underlying host system. It is a security safeguard that limits the security issue to the virtual-machine and keeps your actual system safe. A virtual machine is an answer to the question, how to recover your hacked website or recover a hacked website.

The virtual machine is based on hypervisor software (or VMM for Virtual Machine Monitor). The hypervisor operates as an application on the hosted hypervisor or directly on bare metal hypervisor hardware and manages the hardware resources provided by the host system.

The hypervisor software creates an abstraction layer between the physical hardware and the virtual machine. In this context, we speak of encapsulation. Processes within a virtual machine do not affect the host or other virtual machines on the same hardware. Oracle, is free cross-platform, install a suitable VM guest OS and follow the steps inside a virtual machine.

Disable your website and block it all?

You have been able to verify that your site has been hacked, unfortunately. At this point, you do not need to act immediately to prevent the increase in the problem from becoming more serious than it is.

1. The first action to take is to Disable your website site, put it offline or establish a redirection to another page. This will prevent hackers from doing more damage.
2. Stop the infected website from being live.
3. An infected website may be defaced and could infect the computer system of visitors.

4. Stop the hacker from doing anything further. Once the website is offline, the hacker shouldn't have access to it, thus limiting the extent of damage already done.
5. Save the reputation of your brand. Your ranking in SERPs, as well as the trust of users.
6. Website passwords must be changed immediately. These include, for example, FTP access passwords, but also passwords for user accounts of content management systems.

Because hacker attacks are often large, there is a high probability that other websites will also be affected. In this case, it is advisable to contact the hosting provider, who may already have information available or, in the best case, already have a solution.

It is important at this point to find out where the attack occurred and what is the cause. The answer to this question can be found in the log files and in the data processing history. Unfortunately, in most cases, it is not possible to identify the aggressor or the cause.

What exactly does blocking mean and how to block your website

Point-wise note down everything you are doing on a paper with a pen. Screenshots and data on the computer might get erased so keep everything you have done on a piece of paper.

1. Put your website into maintenance mode. WP Maintenance Mode plugin by Designmodo is an excellent choice to disables public access to your website.
2. Hosting companies provide you with some sort of access to a control panel which could be VirtualAdmin, Webmin, cPanel, WHM, etc. By using this feature you can limit access to your site.
3. Update the control panel passwords. Once you are done with everything then change it again later.
4. Often you may have multiple users who have access to the hosting account, revoke their access at least temporarily.
5. Change the password for MySQL / mariadb, PHPMyAdmin, FTP, ssh and WordPress admin backend.

Don't keep this backup on the server. Download it to your virtual machine.

Backup as a precaution

It is obviously not a good choice to backup your infected site. But you still need a backup. Well, you know how to make backup copies of your WordPress by saving the files on your website and its database.

But it is an ideal to make a timely backup, weekly or monthly backups since you save having an unnecessarily installed plugin and in five minutes you have it done.

We have several reasons to make a backup of your WordPress:

- The backup contains the most recent posts, pages, and other data.
- It also has evidence of the security issue which you can use to study things later and do a root-cause-analysis.
- The latest backup can help you recover stuff if situation goes wrong.

Identify the problem?

So, what is wrong with your WordPress site? We will now give you some tips on how to Identify the issue on your WordPress site and what you can do to fix it.

- **The source of the web page**

This is how Google has detected the Malware infected website and the evidence is supposed to be presented in the HTML file of the web page. Check the HTML file thoroughly to check if a few pages or the entire website is affected.

Here are the steps to follow:

1. Just pick a URL where the problem is reported and scan code to code carefully.
2. Go through each line and look for problems (this is how the professional will try to fix the infected website).
3. Check all the JavaScript files included in the source of a web page.
4. See if everything is loading normally

Sometimes it may not be possible to identify the problem from the source code of the web page. The integrated browser development tools are very useful:

- **Open the browser tool pane and navigate to the Network tab.**

Go to the website and search for what is loaded like everything from external domains in particular, but also look for something suspicious about the local domain too.

https://wp-malware-removal.com/wp-content/uploads/2018/05/browser-developer-tools-network-console-1136x368.png

- **Run an automated malware scanner**

Automated scanners are not able to use JavaScript code and database malware because the problem does not relate to the script content or the content of the database itself. The issue comes from the rogue external malware site it is loading. Do not leave anything to chance and always run a malware scanner and let it work throughout any suspicious items.

- **Included scripts**

The Cross-Site Scripting or XSS Attack, are one of the vulnerabilities concerning the most known web applications and the most used as vectors of attacks. Cross-Site Scripting occurs when moving from a context where data is secured to a context where it is misinterpreted.

As a result, by adding content to the website, a user can take control and change the behavior of the application for other users. Javascript would then dynamically load a hidden iFrame, etc. to download malicious software on the visitor's machine. JavaScript files are available on the server. Initially, you need to scan those that are included in the target page.

Look at the root of the WordPress installation, in .htaccess, in the folder wp-content, the files contained in your active theme, plugins, plug-ins essential and plug-ins to integrate.

- **Looking for more similar infected files**

If you have shell access to your hosting, then you can run a grep command to parse all files for that particular string.

- **Inline scripts and content**

Once you have found the unreliable script, you will need to scan the website to see if there is anything else suspicious in the database. You can use PHPMyAdmin or the MySQL command line to search for strings like an iframe, NoScript, base64, eval and display (which you will find there and many of them are legitimate).

Once the attack has been verified, it is necessary to accept the extent of the damage caused. Google, for example, can help because the domain is kept under constant scrutiny. Other control options include the Google Search Console, virus detectors and a look at the server logs and .htaccess or index file.

Once the damage has been identified, the next step should always be to eliminate the malicious code. A recent backup can be useful in these situations. If available, codes can be compared to eliminate any errors manually. If the insertion is too tedious, you can simply import the full backup.

Finally, it is necessary to report the successful removal of the malicious code to Google so that the alert in the search results can be removed as soon as possible. The site could return to normal in the search engine after a few days to a few weeks, depending on the type and size of the attack.

Root-Cause-Analysis & Finding Security Loopholes

More and more people understand and know the typical security loopholes that are made when programming dynamic web pages, there are even efforts and projects to catalogue these types of errors as if it were a security encyclopedia. But it is very difficult to cover each security loophole in a list since everyday new loopholes are discovered.

However, this is an unrealistic approach to the problem, WordPress security is not about applying certain patterns to try to find security loopholes, it is not about what you should and what you should not do. Try exclusively to look for everything, to ask yourself if what you see is just how you see it, or can be looked at from another point of view. WordPress security is often about wondering if the code we see does only what it says it does, or can do something else.

The primary task is you identify the attack vector (how it happened) and fix the root-cause of the problem so that it doesn't reoccur.

Following are some of the most common attack vectors:

1. Allowing (unauthenticated) user-upload of files.
2. Hidden plugin (must-use plugin) that does mischievous things.
3. Unknown users with special privileges inside WordPress.
4. Too many users for their account with access to your hosting/WordPress/FTP/SSH.
5. Allowing user-upload of unsanitized data/rogue plugins serving unescaped data.
6. Rogue WordPress Theme or Plugin.
7. Some rogue script that your web-developer leftover when migrating your WordPress website.
8. Some clipboard content that automatically got pasted when copying the text over from some other webpage and included inline script(s).

9. Easy to crack passwords.
10. The misconfigured server that misbehaves or leaks confidential information contained in PHP files.

Verifying That The Site is Clean and free of infection

First, check quickly if there are no security loopholes open and Google has detected any issues on your site. Now website is clean and ready to go live, run it through malware scanner again.

You can use Google's free site verification service. This service uses Google's secure browser technology to check if your site is potentially harmful to your visitors and inspect any suspicious files left.

Give yourself 48-72 hrs. and watch out for any troubles or recurrence.

If you haven't used Google Search Console then you'll need to register and verify your site in Google's Search Console.

Sign in to Search Console and go to "Security & Manual Actions" → "Security Issues" section.

You can also inspect your site from the "Site Status" menu of the Google Console. If Google has previously reported that your site is hosting malware, the alert will go away once you've cleared your site of malicious software. Effective (and free) to identify the presence of malware on your site, this tool is a good starting point.

Go ahead and "Request a review". Once Google verifies that your site is clean and isn't infected anymore, they'll remove the "This site may be hacked" message.

When there are no more issues reported with the website, it's time to take a backup.

Now finally you can change the passwords once more to something stronger than before.

Preventing WordPress Malware Attacks in the Future

If you are a beginner then that was a lot to take into consideration. However, all we have mentioned in this article is a step in the right direction. The more you worry about the security of your WordPress site, the harder it is for a hacker to violate the website.

Cutting Edge WordPress Security Tips To Safeguard Your Site From Malware

Website security, essentially, comprises three main aspects:

- software security (CMS, scripts)
- server security (hosting)

- administrator awareness of the need for website security and his accuracy and precision in performing website administrative tasks

If all the elements are properly controlled and function in a correct way, your website will be protected against hackers and malicious software.

To protect your site, it is useful to adopt a number of security measures at different levels: during the installation of WordPress, when updating WordPress and WordPress extensions. Do not forget that you should not use any free third-party plugins or scanning services. they charge monthly, send cryptic notices about security issues and play on FUD: Fear Uncertainty Doubt ending up confusing users forcing them to buy useless stuff.

When creating your website with WordPress, you must make sure to choose a reliable, efficient and responsive web host. You must then secure access to your database (just like your FTP) through the adoption of a secure password.

Follow the steps below to prevent future WordPress attacks:

1. Don't leave rogue data, files, forms on the server. They can be used for various types of attacks.
2. Keep your WordPress installation, themes and plugins updated to keep the environment stable and compatible.
3. Keep your hosting server properly configured with a well-secured firewall and other security infrastructure.
4. Keep your accounts secure manually.
5. Passwords can be stolen from emails, stolen phones and more.

Secure WordPress by protecting the login page and preventing brute force attacks

Everyone knows the URL of the WordPress login page. The back-end of the website is accessed from there, and that is the reason why spammers use brute force methods to access. Just add/wp-login.php or /wp-admin/ to the end of the domain name and voila.

And if this is your case, it is because your website is completely insecure, but calm in this article you will learn how to optimize the security of your WordPress very easily.

To solve this "small" BIG problem, it is to customize the URL of the login page and even the interaction of the page. It is the first thing that must be ensured when publishing a web page.

Here are some suggestions for the security of the WordPress login page:

6. Change the name of the access URL to secure your WordPress website
7. Use your email to login
8. setup wordpress 2-factor authentication
9. Install and configure a user and host blocking feature

Secure your WordPress website through the Admin Panel

The first part was to ensure by all means the beginning of the session, now we will ensure the internal part.

For a hacker, the most intriguing part of a website is the administration dashboard, which is, in fact, the most protected part of all. Therefore, attacking the strongest part is the real challenge. If done successfully, the hacker will get a moral victory and access to do a lot of damage.

This is what we can do to ensure the security of the WordPress administration:

10. Add user accounts with strong passwords
11. Secure the WordPress administration panel
12. Protect the "wp-admin" directory
13. Use SSL security certificates to encrypt data
14. File Monitor
15. Change the admin username

Secure your WordPress website with Hosting

Almost all hosting companies intend to offer an optimized WordPress environment, One of the best provider which I use for my websites is Host and protect. You can still go one step further and ask to:

16. Disable file listing with .htaccess
17. Correct permissions on directories and files
18. Do not allow file editing
19. Protect the wp-config.php fil
20. Block all hotlinking

Secure your WordPress website through themes and plugins

The updates are indicated directly from their outputs, and the same goes for plugins. Do not forget to update your plugins, they are often the source of successful hacking.:

Find out how to secure your WordPress themes and plugins: [**Read more on** Wordpress theme security]

21. Update regularly
22. Remove WordPress version number

WordPress Malware Scanners Online

Malware scanners can help you check your website for very common security risks. For example, they may search for malicious code, suspicious links, suspicious redirects, the WordPress version, and so on.

However, they are quite limited because they can not run tests on your WordPress database, user accounts, WordPress settings, plugins, and more.

These malware scanners incorporate Behavioral analysis, Static page scanning & Dynamic page analysis in their scanning process.

Let's take a look at some of the best WordPress malware scanners that you can try.

1. WP Hacked Help

WP Hacked Help checks your website for known vulnerabilities and suspicious code. They maintain an index of vulnerabilities detected by their system and check your website for these security leaks.

It also tries to detect your version of WordPress, installed plugins and robots.txt files. After the analysis, the results are presented in an easy to understand format with the explanation of each element.

It runs a comprehensive test by trying to detect your WordPress plugins, usernames, WordPress version, active theme, and more.

It provides a detailed report of the state of your site with a brief explanation of each element. These are mainly the elements that are the best current WordPress security practices like using the latest version of WordPress and keeping your plugins updated. It implements the cutting edge technique to identify:

- Hidden Redirects
- Obfuscated Malware Injects on the Page
- Blackhat SEO Links and Spam
- Malicious Downloads and Drive-By Attacks
- Website Defaces
- Dangerous Widgets, Adware and E-Commerce Spyware
- Website Blacklist Status: Google and 64 Others Website Errors

Realtime Scanning: Easy Check, Quick Report. No download and installation needed. No FTP/SFTP/SSH access required.

Just provide us with an URL (address of web site) that you want to test and press "Scan Website" button.

2. Sucuri SiteCheck

SiteCheck is an online tool of Sucuri, one of the best firewall and security services WordPress. It offers a thorough check of your website for malicious code, spam injection, website modification, and more.

It also checks your website on several blacklisted domain name tools, including Google Safe Browsing. The Sucuri SiteCheck tool not only analyzes the URL you enter but also explores the other pages linked to it to provide a complete and fast analysis.

3. Google secure browsing

The secure Google navigation tool lets you know if a URL is considered dangerous by Google. Google monitors billions of URLs, and if it suspects that a website is distributing malware, it considers it dangerous to view them.

This could potentially damage the reputation of your website because users from Google Search or Google Chrome will receive a warning page when they visit your website. If you use Google Search Console, you will be notified when your website is marked as dangerous with instructions for the warning to be removed.

4. Scan WP

ScanWP is a very basic WordPress vulnerability scanner. It tries to detect your version of WordPress to see if you are using the latest version. It also detects the WordPress builder's label, and whether your site shows it or not.

The builder tag shows which version of WordPress you are using. Some security experts think this could help hackers to effectively target a website and they recommend removing the WordPress builder's tag.

Hackers can easily hide malicious code and go unnoticed to these basic security checks. That's why we recommend using the services of the WPHH scanner. It's a complete website security service that detects and neutralizes malicious code even before it reaches your website.

Further Reading:

10-Point WordPress Security & Hardening Tutorial

ULTIMATE WORDPRESS SECURITY CHECKLIST 2019 By WP Hacked Help

WordPress Security Guide For Beginners

Common WordPress Errors

“Are You Sure You Want to Do This” Error WordPress

WordPress HTTP Image Upload Error

HTTP 503 Service Unavailable Error

WordPress Stuck in Maintenance Mode

Parse Error: Syntax Error Unexpected WordPress

“This Account Has Been Suspended”

WordPress Not Sending Email, WP Mail SMTP Not Working

THE END