

How to Protect & Secure Website From Hackers? (Website Protection Guide)

by Nirvana | March 30, 2021



Your website is valuable: for you and for your site's visitors. And also, for hackers.

To build good defences against malicious attacks, you need a no-nonsense guide on **how to protect website from hackers**.

This is that hacker protection guide!

How are we so confident? MalCare protects 25000+ websites, and our support team ferrets out the most elusive malware from websites every day. We know a thing or two about how to protect your website from hackers and other malicious attacks.

***TL;DR:** The best security measure is to [install a security plugin](#) that runs on autopilot. We also recommend that you implement all the security measures we've described in this article.*

Before you begin

Seeing a long list of security measures to protect website from hackers can be somewhat daunting. We realise that. So, in order to make implementing these security measures easier, we have organised this hacker protection list by ease. We suggest bookmarking this article, and coming back to it as you work your way through it.

There are a mix of protective steps on this list: things that you should do, things that you shouldn't do, and a few busted myths just as well.

The goal of this article is to demystify security, by cutting through the clutter that is available elsewhere. However, the biggest takeaway should be that protecting your website from hackers and viruses is not a one-time activity; but more on that as we progress.

6 Basic Steps to Protect Your Website from Hackers Immediately

The protective measures in this section are the easiest to implement, and honestly will set you up reasonably well. At first glance, they may seem technical or advanced, but take it from someone who isn't an engineer: you got this!

1. Install a good firewall

Hackers don't manually hack into websites. A good hacker will create a bot that sniffs out vulnerable sites and automates most of the process. Now, bots are programmed to carry out very specific actions. They're not sentient.

At its core, a firewall is code that identifies malicious requests. Every request for information made to your website first goes through the firewall. If the firewall detects that the request is malicious, or being made from an IP address that is known to be malicious, the request gets blocked instead of being processed.

Avoid changing firewall configuration

Some firewalls will allow you to configure settings. However, we don't recommend it unless you are a bonafide website security professional. Firewall rules are created after significant security research and a lot of firsthand malware removal.

For instance, most [WordPress security plugins](#) have rules in place that prevent anyone without administrator access from accessing the wp-config.php file. The wp-config.php file is a core WordPress file that contains a lot of sensitive information. So, the firewall checks every request made to the website to see if it contains the text "wp-config.php". If that rule is triggered, the request is denied by the firewall.

Additionally, since hackers attempt to hack as many websites as possible when a vulnerability is discovered, this brings to light hacker IPs. WordPress firewalls

track and [block malicious IPs](#) preemptively, based on these attacks.

Of course, no firewall is 100% unhackable. But it's way better to have a firewall that blocks most malicious software, than to have no firewall at all. But all firewalls are not the same, and some are far more effective than others. So, we made a list of the [best WordPress firewalls](#) for you to choose from.

2. Have a strong password policy and use a password manager

We've been in [WordPress security](#) for over a decade now. You'd be surprised to know how many websites were hacked simply because the password was weak.

Easy to guess passwords are used by hundreds of thousands of websites. 5% of hacked sites that used MalCare to remove malware used weak passwords.

Hackers have a list of such passwords called rainbow tables and they constantly generate larger tables to use as a dictionary of sorts. Using these tables, a hacker can launch an attack known as a '[dictionary attack](#)'.

Dictionary attacks are mostly a variant of [brute force attacks](#). But that's not the only way to hack a password. Therefore, strong passwords are recommended.

Strong passwords are a combination of letters, numbers, and symbols.

Uncommon combinations are hard to crack and can take brute force algorithms years to decode. Also, the longer a password, the more difficult it is to crack.

[This article](#) will help you create your own epic password.

You can also use plugins to enforce strong passwords from all your WordPress users with the plugin [Password Policies Manager for WordPress](#). This plugin will help you create policies that force all your WordPress users to create strong passwords when creating their accounts.

3. Install SSL and use HTTPS on your website

Secure Sockets Layer (SSL) certificate, is a security protocol that encrypts all communication to and from a website. Installing one will ensure that even if a hacker intercepts data from your website, they'll never be able to understand what it is.

We've created an entire guide around [installing an SSL certificate](#) the right way. Seriously, the hype is justified. Get an SSL certificate for your website now. As an added bonus, you'll get SEO benefits too.

4. Scrutinise admin users carefully

Most people assume that hackers will only install malware on their website and leave. That's not true. The really smart hackers will create a ghost account with administrator privileges so that they can waltz back in whenever they want.

Reviewing and removing WordPress users on a regular basis can resolve this issue.

Yes, it can be a time-consuming activity if you have a large team managing your website. But it's worth it. Deleting users who no longer contribute to your site is the first place to start. Then, make strong passwords mandatory so that your writers and editors don't accidentally compromise your site.

You may follow great security practices for your passwords, but if one of your admins falls prey to a phishing scam, for instance, then your website will also be affected.

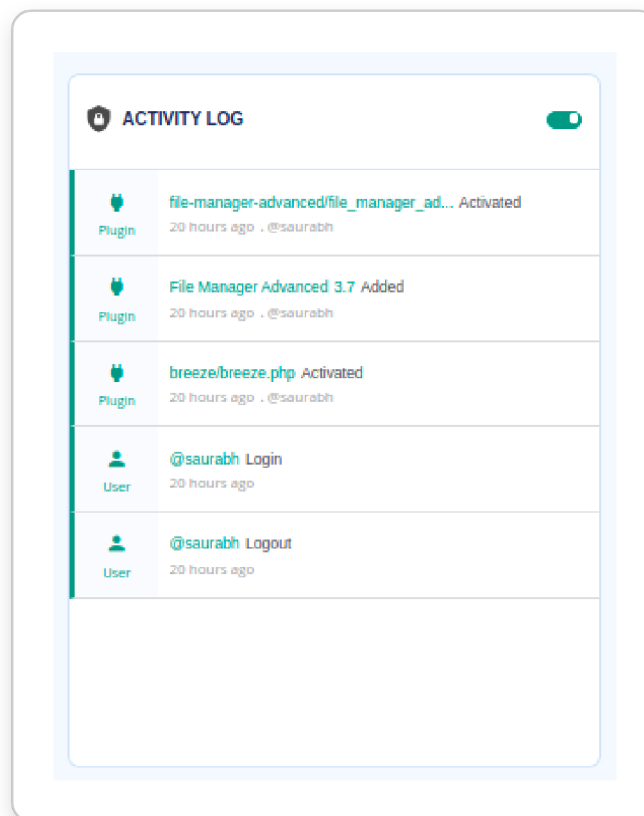
Make full use of WordPress user roles to restrict access as far as possible. For instance, if someone is only writing and uploading articles, give them 'Author' access, and not 'Admin' access. Read our article on [WordPress roles](#) to figure out how to get everything done painlessly.

5. Use an activity log

Seeing something unexpected on your website can raise a timely alarm in several situations. Consider if an admin account was created without your knowledge; or a plugin deactivated (a security one, for example) without consensus.

These are all examples of legitimate website admin actions, however they can also be symptomatic of unauthorised access. Activity logs will tell you what is happening on your site, and you can then evaluate whether these actions are legitimate or not.

This one practice has [saved our bacon](#) many times over.



Most hackers are extremely careful so as to not get caught, because they can only control your website for as long as they don't get caught. Activity logs help in signalling changes, so you can nip unauthorised activity in the bud.

MalCare comes [bundled with an activity log](#) on the dashboard, and there is no configuration necessary to set it up.

6. Take regular backups

Taking backups is quite possibly one of the most underrated tactics you can apply. Always take daily backups so that you can quickly [restore your website](#) in the event of a catastrophic failure.

[Choose a good backup plugin](#) that is reliable, because manual backups are difficult to execute correctly without considerable expertise.

In fact, before you proceed with any of the steps in this article, take a [full backup of your website](#) and set up daily backups immediately. This is always good practice when making any changes to your site.

5 Intermediate Steps to Protect Your Website to The Next Level

The basic steps in the article are a good start, and shouldn't take too much time to set up. In this section, apart from two-factor authentication and limiting login attempts, the steps are ongoing security measures.

As we said earlier in this article, it is important to think about [website security](#) in the right way. It is not a one-time set up or activity, and must be considered a regular part of your site administration.

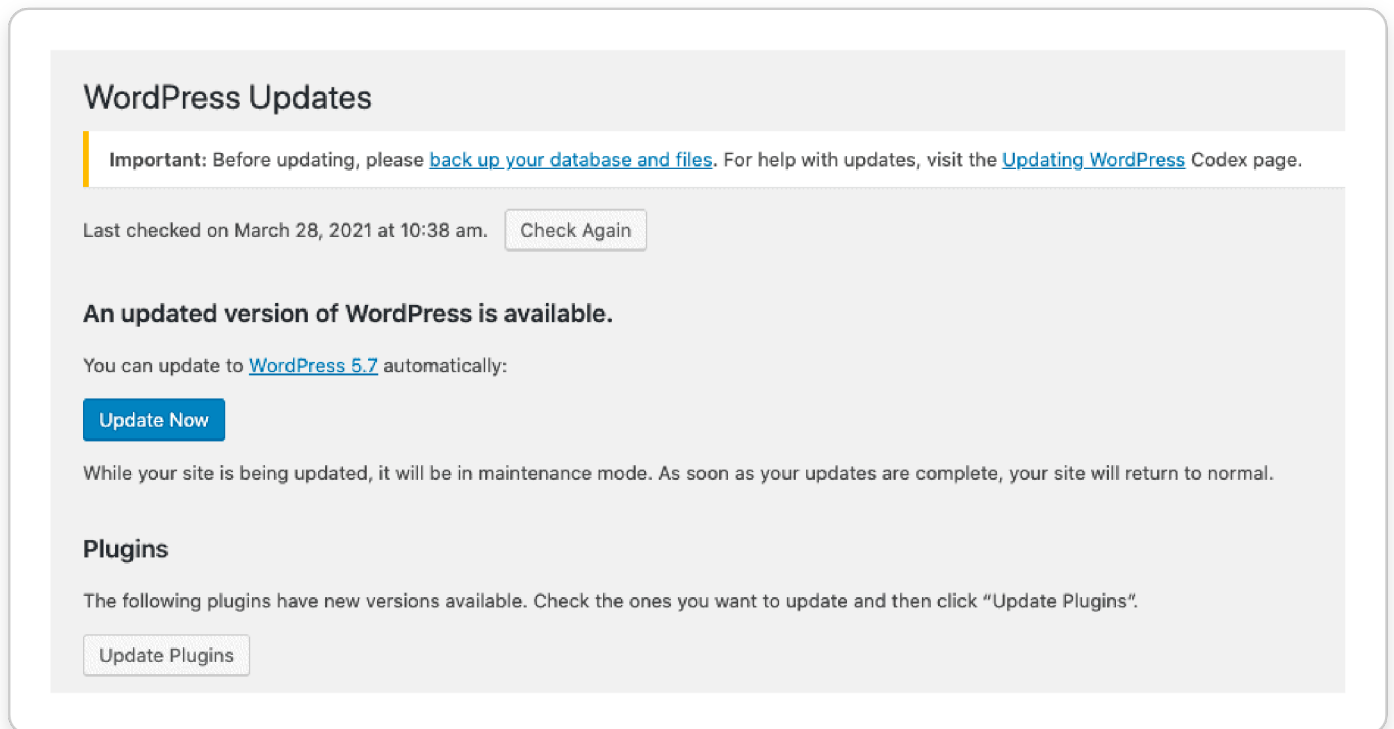
1. Update everything

Over 90% of hacks occur because hackers have identified a vulnerability in a theme or plugin, and exploited it over several websites.

So what is a vulnerability? Themes and plugins are software. Like any other software, they are pieces of code that will invariably have bugs. Some bugs are relatively harmless and may just cause a minor glitch while updating. Others can render the code vulnerable to exploitation.

When vulnerabilities are discovered, mostly by security researchers, they are disclosed to the plugin developer for patches. Responsible developers will

release a fix, and websites with the plugin installed will see that an updated version of the plugin is soon available.



Once the fix is released, the vulnerability is disclosed publicly. If you were one of the websites that updated the plugin or theme with the security fix, that's excellent. If not, your site will become the target of amateur hackers (called script kiddies) looking to make a quick buck.

Therefore, it is always best to keep everything—right from WordPress to plugins—updated at all times. We know that updates can sometimes break websites in unexpected ways, so to circumvent any inconvenience, use staging to update safely. But do please update everything.

We created a guide on [updating WordPress websites](#) safely and with minimum disruption.

2. Choose good themes and plugins

If you notice from the previous section, we referred to developers who release updates to patch vulnerabilities as responsible. In short, good developers actively maintain their software.

This is by no means a universal state of affairs. Sad, but true.

Thus, we strongly advocate the use of good plugins and themes for your website. Understandably, “good” is a relative and somewhat vague term. So we are listing factors you should consider when opting for a plugin for your website:

- **Regular updates:** A plugin or theme that consistently releases updates, and keeps patching any vulnerability that it discovers. This will tell you that the developer is serious about the security risks of their product.
- **Active installs:** A popular plugin with millions of installs will always have a target on its back. [Contact Form 7](#) is a very clear example of this trend. The flip side is that popular plugins also tend to be more secure because they usually have a bigger and better team working to improve the product. So choose wisely, after doing adequate research.
- **Credibility:** Avoid installing a plugin or a theme developed by freelancers that no one has heard of. Only use plugins and themes developed by reputed developers and brands. If you’re buying from a marketplace, make sure you trust the developer and not just the marketplace.
- **Paid versions:** Typically, paid plugin vendors spend more time and money on finding and patching vulnerabilities. If you’re on a very tight budget, then a free plugin will make more sense. But if you’re worried about your website’s security, we highly recommend using premium themes and plugins instead.

As a side note, you may be tempted to use [nulled plugins and themes](#). Don’t do it. The risk is just not worth it.

Nulled software spreads malware. That’s why you’re getting a premium product for free. But even if the zip file doesn’t contain any obviously malicious code, any nulled plugin or theme user knows that they can’t update the software. That makes the website vulnerable to a hack, as we said in the previous section.

3. Implement 2FA

Two-factor authentication (2FA) is a security measure that adds another device or token that you must have access to in order to login, in addition to your password.

There are a few protocols that are used for 2FA, like TOTP (time-based one-time password) or HOTP (HMAC-based one-time password). They each have their pros and cons, but for the purposes of login security, we don't need to delve into those details.

There are several paid and free apps that can be used to add 2FA to your login page, and they support the most popular protocols. For more help, check out this article to see [how to set up WordPress 2FA](#). If you have many contributors to your website, it's definitely a good idea to implement this security feature.

4. Select a good web host

Most people hold web hosts responsible for even the security of the website. But it's rarely the web host's fault if your site gets hacked. In fact, in the rare cases that a web host is responsible for a security breach, the ramifications are enormous. Thousands of sites are affected.

The shoe is on the other foot most of the time, and a good web host is instrumental in protecting your website from hackers. Thus, you should aim for the most secure hosting service. Here's a list of the [best WordPress hosting providers](#) we compiled to help you select a good web host.

5. Limit login attempts

One easy way to block brute force bots and attackers is to deny entry to an IP address after 3 failed attempts. [MalCare firewall](#) comes integrated with this feature. Limiting login attempts is a highly effective way to protect your website without many downsides.

You can use the '[Limit Loginizer](#)' plugin when installing WordPress as well. But if you get your own password wrong 3 times, then you'll have to ask your web

host to unblock your IP address to try again.

2 Expert Steps to Really Amp up Your Website Protection

Even if you have managed to complete the steps in the previous sections, you are sitting pretty in terms of protecting your site from hackers. The following measures are effective, however they require some amount of poking around in the code.

We want to reiterate that most hacks occur because of [vulnerabilities](#), so taking care of those will protect your website from hackers and viruses quite well. If you are uncomfortable with trying out the following steps yourself, you can ignore them, or send them along to your developer to implement. Either way, your site is still well protected from hackers.

1. Block PHP execution in the uploads folder

There's an entire class of vulnerabilities called [Remote Code Execution](#) vulnerabilities that allow hackers to upload malicious PHP code to the Uploads folder. Typically, the Uploads folder is not meant to contain any executable code. It's meant to contain your media files. But the nature of the Uploads folder is that it allows files and folders to be stored within it.

Once the code is uploaded to your website, a hacker can run it and gain effective control over your site. However, if you block PHP execution in the Uploads folder, then the attack can never take place.

If you're using MalCare you can block PHP execution in the Uploads folder with the click of a button as part of the [WordPress hardening measures](#).

2. Change WordPress security keys

If you have been hacked recently, you can change your WordPress security keys. This is a string that is hashed along with your username and password to manage logged in sessions for users.

You can set this string to anything at all, however like with passwords, it is best to use a randomly generated alphanumeric string. Read more about [security keys and how to change](#) them.

2 BONUS Tips for Website Protection Against Hackers

1. Keep yourself updated on security news

Staying informed, asking questions and consulting with the community are all excellent ways to keep track of the latest hacks and changes in the threat landscape. For instance, if a plugin vulnerability is discovered, you can deactivate it from your dashboard till the update is available and installed. Whatever inconvenience you face will pale in comparison to the losses sustained from a hacked website.

2. Conduct regular security audits

Many website owners mistakenly believe that their sites are too small to be considered worthy of hacking. This is nowhere close to the truth. Hacks happen for a variety of reasons, and if your website is, say, not lucrative in terms of user data, it still has enough SEO authority to be used as a [phishing site](#).

Regular security checks will help uncover unsafe practices as well as potential vulnerabilities in your website. By keeping an eye on the happenings of your website—via an activity log, or reviewing users, for example—you will save yourself a ton of grief in the long term.

Things That Will NOT Help To Protect Your Website

We advocate being security conscious, but not paranoid. Also, we have seen that there is a great deal of bad advice for website owners out in the wild. The advice may come from a good place, however it can have unintended consequences, like creating a poor user experience, or locking you out of your own website!

So please don't do the following.

1. Hide your wp-login page

Many security plugins still believe that this age-old trick works.

If the hacker can't find the login page, they can't carry out [brute force attacks](#), right? No, not really. Instead:

- It makes your website very difficult to use. If you forget the new login URL, then recovering your account can be difficult.
- If you use the default URLs that come with the security plugin, it's easy for the hackers to guess your new URL.
- Even if hackers can't find the wp-login page, they can still hack your website using the [XML-RPC vulnerability](#).

This option achieves nothing in the end and can cause quite a bit of trouble.

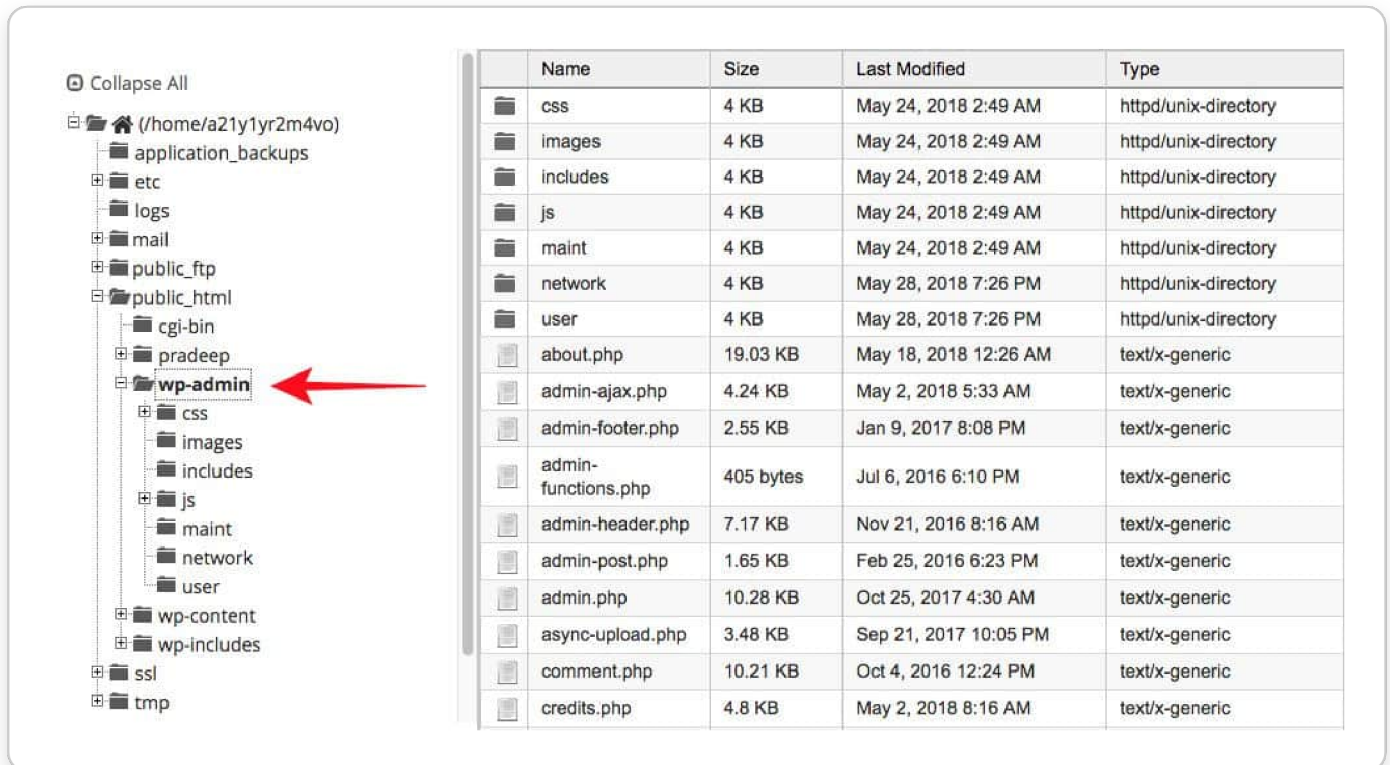
2. Geo-blocking

[Geo-blocking](#) is essentially blocking out traffic from countries where your product or service is not available or relevant. This is usually seen as a security measure but it's actually a way to reduce the billing for consumed server resources.

It's quite possible that you think that traffic from Gabon isn't helping your business. But blocking all traffic from Gabon solves nothing at all. With a good VPN, anyone can bypass even Netflix's geo-blocking.

Also, you run the risk of blocking Googlebot and yourself out as well!

3. Password-protecting the wp-admin directory



The screenshot shows a file manager interface with a sidebar on the left displaying a directory tree. The path is /home/a21y1yr2m4vo. The wp-admin directory is highlighted with a red arrow. The main pane on the right shows a table of the wp-admin directory's contents.

Name	Size	Last Modified	Type
css	4 KB	May 24, 2018 2:49 AM	httpd/unix-directory
images	4 KB	May 24, 2018 2:49 AM	httpd/unix-directory
includes	4 KB	May 24, 2018 2:49 AM	httpd/unix-directory
js	4 KB	May 24, 2018 2:49 AM	httpd/unix-directory
maint	4 KB	May 24, 2018 2:49 AM	httpd/unix-directory
network	4 KB	May 28, 2018 7:26 PM	httpd/unix-directory
user	4 KB	May 28, 2018 7:26 PM	httpd/unix-directory
about.php	19.03 KB	May 18, 2018 12:26 AM	text/x-generic
admin-ajax.php	4.24 KB	May 2, 2018 5:33 AM	text/x-generic
admin-footer.php	2.55 KB	Jan 9, 2017 8:08 PM	text/x-generic
admin-functions.php	405 bytes	Jul 6, 2016 6:10 PM	text/x-generic
admin-header.php	7.17 KB	Nov 21, 2016 8:16 AM	text/x-generic
admin-post.php	1.65 KB	Feb 25, 2016 6:23 PM	text/x-generic
admin.php	10.28 KB	Oct 25, 2017 4:30 AM	text/x-generic
async-upload.php	3.48 KB	Sep 21, 2017 10:05 PM	text/x-generic
comment.php	10.21 KB	Oct 4, 2016 12:24 PM	text/x-generic
credits.php	4.8 KB	May 2, 2018 8:16 AM	text/x-generic

The wp-admin folder is one of the most critical directories in any WordPress installation. So, naturally, every hacker wants to get into it. Security professionals initially thought that password protecting the directory would be a good idea, but we have since come to realise that it is not good practice.

Password protecting your wp-admin directory [breaks AJAX functionality](#) on your WordPress website and causes many plugins to malfunction. If you're running a WooCommerce website, broken AJAX code can wreck your search functionality and other critical UX elements.

Why Should You Protect Your Website From Hackers?

This article already has a lot of info on the how to protect your website from hackers, and perhaps we've already mentioned this a few times, but it bears repeating. Your site is valuable.

When we say it is valuable, we aren't just talking about you and your visitors. Maybe you have a small online shop or a hobby blog that a small group of people visit regularly. The deal is that even if the direct monetary gain from hacking your website is not large, the benefits of having a clean website to hawk illegal or grey market wares still makes the hack worth it for the hacker.

So, a small website is not protection against nefarious intent.

Secondly, it behoves upon us all to protect the data and identities of our users. They are placing a certain amount of trust in a site by visiting it at all, and we should be mindful and considerate of them while considering website security.

Conclusion

You can stop a hacker by being vigilant and taking a proactive approach to security. It is important to realise that protecting your website from hackers and malicious attacks is an ongoing process. There are steps you can take once, but mostly you need to be aware of the changes in the threat landscape.

Furthermore, there is no one-stop, definitive article that can help you stop all possible hacks against your website. Any article or website or expert that claims to do so is not being truthful.

So, while we can't really promise that this article will keep your website safe and secure forever, we have given you some general security tips that will make your website pretty difficult to hack. Using the tips in this article, you will be able to patch several flaws in your website security.

FAQs

How do I protect my website from hackers?

There are several steps you can take to protect your website from hackers. Here are some top security tips:

1. Install a security plugin with a good firewall
2. [Implement two-factor authentication](#)
3. [Limit login attempts](#)
4. [Keep your plugins and themes updated](#)
5. [Install SSL](#)
6. [Select a reputable web host](#)

Why should I protect my website from hackers?

Hackers always have a lot of gain from attacking your website. Apart from the actual monetary loss you are likely to face, your visitors' data will be compromised and they too will face ramifications of having their data stolen.

Good websites do not have to be big to be lucrative. There are many nefarious and illegal activities that can be done on a small hacked website just as well.

Should I implement two-factor authentication?

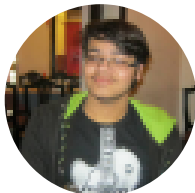
Yes, [two-factor authentication](#) is an excellent system to have in place for website logins. It requires an additional token when signing in, apart from the username and password. The premise here is that, even if a hacker has somehow gotten your credentials, they are unlikely to have your device (or whatever you use to receive the second token). This is an effective mechanism to thwart unauthorized access, and is already widely used on the internet.

How many measures should I take to protect my website from hackers?

It is a common misconception that doing everything makes your website as secure as possible. One of the reasons we have left out a great deal of commonly found information from this article is because doing everything does not actually make your website more secure. On the contrary, for little additional benefit, you will end up making your website harder to use.

This article contains the measures you can safely take to amp up website protection against hackers, without sacrificing too much on the user experience front.

Category: Security, Wordpress



Nirvana

Nirvana is a WordPress enthusiast, and enjoys sharing their experience with fellow enthusiasts. On the MalCare blog, Nirvana distils the wisdom gained from building plugins to solve security issues that admins face.

Share it:



You may also like



Post-Hack Cleanup Enhancement: Reset WordPress Keys Easily

February 27, 2024

Security keys in WordPress are used to store a lot of critical information. For instance, they are used to manage logged-in sessions securely. Most of the time, you can forget...



MalCare blocks attacks on vulnerable Bricks Theme Builder v1.9.6

February 26, 2024

MalCare recently blocked over 26,000 remote code execution (RCE) attacks on its customer websites. These attacks exploited a vulnerability found in the popular Bricks Theme Builder. Our firewall is protecting...



How To Manage WordPress Security Maintenance

February 22, 2024

Your WordPress site can be threatened for a whole host of reasons. Vulnerable plugins and weak passwords, for example, are some of the popular roots of a hack. A hack...

How can we help you?

If you're worried that your website has been hacked, MalCare can help you quickly fix the issue and secure your site to prevent future hacks.

My site is hacked – Help me clean it

Clean your site with MalCare's AntiVirus solution within minutes. It will remove all malware from your complete site. Guaranteed.

Clean your Site →

Secure my WordPress Site from hackers

MalCare's 7-Layer Security Offers Complete Protection for Your Website. 300,000+ Websites Trust MalCare for Total Defence from Attacks.

Protect your Site →

Company

Key Features

Comparison Pages

Top Articles

Also from us



Copyright 2023 Malcare. All Rights Reserved.

[Privacy Policy](#) | [GDPR](#) | [Terms & Conditions](#) | [Cookie Policy](#)



Company

[About Us](#)

[Contact Us](#)

[Careers](#)

[Become an Affiliate](#)

[MalCare for Agencies](#)



Comparison Pages

[MalCare vs WordFence](#)

[MalCare vs iThemes](#)

[WordFence alternatives](#)

[Sucuri alternatives](#)

Also from us



Key Features

[Malware Scanner](#)

[Malware Removal](#)

[WordPress Firewall](#)

[Bot Protection](#)

[Vulnerability Scanner](#)

[WordPress Backups](#)

[Activity Log](#)

[Emergency Cleanup](#)

Top Articles

[The Ultimate WordPress Security Guide](#)

[How to Fix a Hacked WP site?](#)

[How to Remove Malware from WordPress Site](#)

[Scan & Clean WordPress Hacked Redirect](#)

[Best WordPress security plugins \(reviewed\)](#)

[How to remove Google blacklist warning](#)

[Types of WordPress attacks](#)

[Types of WordPress vulnerabilities](#)

[How to implement WordPress login security](#)

