WORDPRESS SUCCESS

GUIDE 7:

Securing Your WordPress Site Against Modern Day Hackers

Securing Your WordPress Site Against Modern Day Hackers

If you're wondering why anyone would want to hack your WordPress website, you're not alone. Read this guide to find out why your site is being targeted, and better yet, what you can do to protect it!

WordPress powers a quarter of all websites in the world. That translates to millions of websites. With WordPress being open-source software, developers, users, and hackers alike can view the entire code that makes the platform what it is.

> *This makes it relatively easy for hackers to find vulnerable areas on a WordPress website.*

In older movies, hackers are often portrayed as individuals sitting in front of a computer trying to get access to a website. There are still individual hackers that do this today, but often they target high-value websites so they can hold them for ransom.

More often than not, bots and botnets attack WordPress websites looking for vulnerabilities so they can take over and use the site or the server where it's hosted to spam other websites.

Bots are programs written by hackers. They scan WordPress sites looking for known security holes. Botnets, on the other hand, are a network of bot-infected machines that try to hack into a huge number of sites.

Sounds scary, right? Since bots aren't slow like us humans, they can infect a large number of sites very quickly.

This is why it's extremely important to update your core WordPress software, your themes, and your plugins. Because if a bot gets to your site first before you update, then your site is as good as compromised!

Why Hackers And Bots Attack WordPress Websites

To learn how to protect your site, it's important to know first why your WordPress site is being attacked. Most of the time, hackers create bots to be able to do the following malicious activities:

- **Steal your website data** – if you collect people's information on your website, that is if you have a mailing list or a membership website, then you're a prime target for hackers.

  They can use or sell your stolen data to other people. Depending on the kind of data they steal, they can use the information to send spam emails or use the more sensitive info to commit identity theft.

- **Use your site to send spam** – hackers can control your website and use it to send spam emails. You won't even realize it, but when it's time for you to send emails to your list, no one's going to receive any of your emails. That's because your site has already been blacklisted by email servers!

- **Host malicious content** – sometimes hackers use other people's resources to hide illegal and immoral content. They don't want these files showing up on their web properties, so they look for an unwilling and innocent participant to hide their files in.

- **Attack other websites** – hackers are clever people. Instead of relying on a single bot, they've found a sophisticated way to attack even more websites.

> First, they'll infect your site, and then they'll use it as part of their botnet or bot-network to launch massive attacks on even more websites!

I hope you now understand why even your new WordPress website is not immune to attacks. It's not because the hackers hold a grudge against you, it's nothing personal really.

> *They don't know you, but they want to use your website and your resources to run their malicious and illegal activities.*

Top Security Measures To Keep Your WordPress Site Safe

There are a number of ways you can protect your WordPress site from getting hacked. I'll begin with the simple ones you can implement right away on your website.

1. Update your core WordPress software, themes, and plugins

WordPress gets updated frequently. So do your themes and plugins. Updating your software is not a choice, it's a must. Using outdated software leaves your website extremely vulnerable to bot attacks.

Updating your WordPress site is easy. When you log in to your WordPress dashboard, you'll immediately see which files need updating. All you have to do is click on the Update button, wait a few minutes, and voila! You've just added an extra layer of protection to your WordPress website.

But what if you don't have the time to log in to your WordPress account every few days?

Well, the solution is to install a security plugin like WordFence (https://wordpress.org/plugins/wordfence). This plugin can send you an email notification every time something needs to be updated on your website.

That way, you only need to login to your account whenever you receive a notification from WordFence.

2. Make your username and password very difficult to guess or crack

Bots try to gain access to WordPress websites by guessing the username first. As a rule, you should never use common usernames as your username, especially not *admin*. Make it extremely difficult for bots to guess your username.

For passwords, use a combination of numbers, upper and lower case letters, and symbols. You should also remember to change your password frequently.

I know writing everything down is a hassle, which is why I recommend you generate and store your passwords using a password manager like LastPass (https://www.lastpass.com).

3. Disable directory browsing

If you go to this URL on your website – *yourdomainname.com/wp-includes/* and you're able to see a list of filenames, then you need to disable directory browsing right now.

If you don't, hackers can simply look through your files, and it will be easy for them to look for the most vulnerable file to gain access to your site!

To disable directory browsing, you're going to have to use an FTP client such as Filezilla so you can edit your **.htaccess** file. Once you've downloaded your .htaccess file, simply add this line at the very bottom of the file "**Options All -Indexes**" (don't include the quotation marks).

Before you attempt to do this on your own, please backup your .htaccess file. If you don't think you can manage this small tweak yourself, please get the help of someone who knows his way around FTP and WordPress.

To confirm directory browsing has been disabled, simply refresh the page *yourdomainname.com/wp-includes/*. If you see a **Forbidden** error, then you've successfully disabled directory browsing.

4. Use two-factor authentication

Most modern apps that handle sensitive information now use two-factor authentication. For example, if you log in to your online banking account, you'll be asked to enter your username and password.

When you enter the right credentials, you'll get a message on your screen telling you to enter the one-time password that's been texted to your phone or emailed to your default email address.

You then need to enter the code within a short period of time. This is how two-factor authentication works. As you can tell, this makes a bot or hacker's job more difficult.

There are quite a few two-factor authentication plugins for WordPress, but if you've installed WordFence security plugin as we've suggested earlier, then you can simply activate this feature on the plugin.

5. Hide or rename the default WordPress login page

The default WordPress login page ends with */wp-login.php* or */wp-admin*. If you rename the page, then it makes a hacker's job more difficult to try and attack your website.

One such plugin available in the WordPress Plugin Directory is **WPS Hide Login** (https://wordpress.org/plugins/wps-hide-login). To make sure you don't make your login page invisible to yourself, don't forget to bookmark the new login link!

6. Get an SSL certificate for your website

If you've ever wondered what the difference is between HTTP and HTTPS websites, it's that HTTPS websites are secure because they have an SSL certificate. SSL stands for Secure Sockets Layer which encrypts all communications between the website and your browser.

Sites with a valid SSL certificate displays a green padlock on your browser. If you click on the padlock, it will say something like 'it's a secure connection and your information is private when it's sent to the site'.

SSL certificates can go anywhere from free to hundreds of dollars per year. Many commercial web hosting companies like WordPress.org's recommended web hosting companies Bluehost, DreamHost, and SiteGround, all offer free SSL with their hosting plans.

7. Limit login attempts

WordPress allows you to log in as many times as possible until you finally enter the right credentials. This is mainly why hackers do brute force attacks on WordPress, trying out username and password combinations until they manage to guess the right credentials!

There are many plugins that can help you limit the number of login attempts on your website.

However, if you've already installed WordFence like we've suggested a couple of times in this guide, then you can simply activate this feature on your WordFence dashboard.

8. Install a WordPress security plugin

The most popular free WordPress security plugin by far on WordPress.org is WordFence. It's got a premium version, but most people just use the free version and are pretty happy with the results.

Now, WordFence is not perfect, but with it being installed on millions of websites, it's a testament to how good people find this plugin.

If you want to skip WordFence altogether, **Sucuri** (https://wordpress.org/plugins/sucuri-scanner) or **iThemes Security** (https://wordpress.org/plugins/better-wp-security) are good alternatives.

Sucuri is considerably more expensive than WordFence's premium version, but reviews do say Sucuri is well worth the price.

iThemes, on the other hand, has got a good reputation on the WordPress Plugin Directory, and their annual plans are affordable.

If you do go for a premium security plugin, make sure you check out reviews and read the product description to see if all your security needs are going to be met.

Final Words

The tips we've listed in this guide aren't by any means the complete, foolproof way of keeping your site safe, but it should help a lot. WordPress security is a very complex and highly technical subject.

With hackers continuously looking for new ways to get into WordPress websites, you have to be on the lookout and be aware of what's happening on your site at all times.

Most security experts edit WordPress code to fight hackers, so if this is something you're not comfortable in, I would suggest hiring a qualified WordPress security expert to help make your site as secure as possible.