5 SIMPLE WAYS TO SECURE YOUR WORDPRESS SITE

Exclusive Report

“5 Simple Ways To Secure Your WordPress Site”

Your *self-hosted* WordPress website is your home on the Internet. It's your own little slice of the Internet real estate, and just like any house you own, protecting it will fall squarely on your shoulders.

If you notice, I've specifically mentioned self-hosted WordPress websites. If your website runs on WordPress.com, then it's not self-hosted. Securing your WordPress.com website is easier, in fact, you probably don't need to think too much about it.

Why? Because WordPress.com owns your website, so it's up to them to protect it, and all the other free websites that's hosted on their platform.

Self-hosted WordPress sites run on free, open-source software called WordPress. Websites built on this software are highly customizable thanks to the thousands of themes and plugins you can choose from.

Because of this flexibility, millions of people have chosen to build their web properties on this platform. And due to this popularity, WordPress has long been a favorite target of hackers and bots.

Without further ado, here are five simple ways you can secure your WordPress website.

1. Update your WordPress software, themes, and plugins

With WordPress being open source software, anyone can get access to the code, including hackers. Hackers can go through the code, study it, and look for vulnerabilities so they can find ways to break into WordPress sites. This is why WordPress gets updated frequently, to close off those vulnerabilities.

Each update also brings about bug fixes, new features, improved performance, and other updates to stay up to date with current industry standards.

Now, if you don't update your software regularly, you're leaving your website open to attack. Not to mention, you're missing out on key improvements and new features.

It's not difficult updating your WordPress files. You don't have to log in to your web hosting control panel or cPanel, or download the latest version of the software and then upload to your site.

> ***If that's what you're thinking, then you're in for a treat! Updating your WordPress website is as easy as 1-2-3.***

Here's what you need to do:

First, log in to your WordPress admin. Then check your dashboard. On the menu section on the left-hand side, you'll see a section which says 'Updates.' Check on that and go through the list of files (this includes WordPress, themes, and plugins) which needs to be updated. And, that's it! I told you it was easy.

When you've updated your software, you're helping your website remain secure. When hackers search for non-updated sites to attack and victimize, you're safely off that list. And you can breathe easy knowing you've got time until the next update!

Which brings us to our next point. Checking for updates will only take a few minutes of your time, but if you've got a busy schedule, then you won't always be able to accommodate update checks in your workflow.

The best way to keep yourself abreast with important updates is by downloading a security plugin which will send you email notifications every time a new version of WordPress is released, or a new theme or plugin version is released.

One such plugin that's highly rated on the WordPress Plugin Directory is WordFence. Try it and make sure to go through the notifications settings.

2. Don't use 'admin' as your username and password

It might sound strange, but yes, people still do use 'admin' as both their username and password. That's kind of silly when you think about it. It's practically the first login combination people use when they try to access a website they have no authority to!

If you really want to make your website secure, then you have to think harder. After all, I'm pretty sure you don't want to give just about anyone access to your files so they can do with it as they please.

You also don't want to use your name, your last name, your birthday, or something easy like that as your username and password. If your name's John, Edward, Michael, Grace, Helen, or whatever common name you have, don't use it as your username.

Especially if your domain is a combination of your first name and last name! That's far too easy to guess, and you're really giving your hackers a chance to access your website.

When thinking of a username and password, you can use a combination of upper and lower case letters, numbers, and symbols. I know you'll probably

find it hard to memorize, but you can always keep your log in details somewhere safe.

You can either write it down the old-fashioned way, and hide it somewhere safe, away from prying eyes. Or you can use a free password manager like LastPass, which can generate hard-to-guess usernames and passwords for you.

The thing with password managers though is you have to remember the master password. If you lose your master password, you may find it hard to recover your private details. Never forget where you keep a copy of your master password, so you don't inadvertently lose access to login details for your favorite websites.

Alternatively, you can also try looking into using two-factor authentication for your WordPress website. When you log in to your site, you'll also get a passcode sent to your smartphone or tablet which you then need to enter in your site within 5 or 10 minutes.

This lessens the chances of anybody hacking into your site. Because even if they know the username and password, but they don't have access to your device, then they still won't be getting in. The idea is really simple, but it works to keep your website safe from hackers and other malicious people!

3. Secure your content: protect what is yours

The problem with being online is that with a simple copy and paste, someone can easily rip off your content. Sometimes they even copy verbatim and post it as if it was their creative juice that came up with the content.

Thus, it is important to secure your posts, photos, videos, music, and the lot. Piracy is a thing, and it is eating the blogging and website industry.

First off, make sure to put watermarks on your photos and videos. Don't make it obnoxiously big though, just the right ratio between the actual watermark and the photo.

Some use their own logo, some use graphics, some use simple text and just put in their website address. Whatever your preference in watermark is, make sure you turn it into a habit. Protect what's yours.

Second, disable copy-paste and right-clicking. Content piracy can be done by anyone, regardless if they are a "techie" or not. You can minimize content theft by disabling keyboard shortcuts like Cut, Copy, and Paste.

For your self-hosted WordPress site, there are a lot of free plugins that you can install such as "*WP Content Copy Protection & No Right Click.*" This plugin will disable keyboard shortcuts like Ctrl+A, Ctrl+C, Ctrl+X, Ctrl+S and Ctrl+V in just a few clicks.

Protecting your content is important. After all, you spend hours creating just one piece of valuable content! So, it's truly unfair if someone were to steal all your hard work without giving you credit for it.

While making your site thief-proof is a challenge, you can add a Terms of Use page for your website where you let people know how they can use your content.

4) SSL: Protect your customer's data

SSL stands for Secure Sockets Layer. It's what makes a website's URL go from "HTTP" to "HTTPS". Websites with "HTTPS" are secure, and normally your browser will display a green padlock at the top if your site has SSL.

If you haven't installed SSL yet, browsers like Chrome and Firefox will tell your website visitors that they are visiting an unsafe website which will turn most of your visitors away!

This is important if your website is an online store where you require your buyers to enter their sensitive information, such as their name, address, contact information, and payment information.

> ***Having SSL gives your customers the confidence to give you their information.***

If I'm a buyer, and I see that my information will not be secure if I buy from you, then I won't be buying no matter how enticing your product is.

With SSL installed on your WordPress website, your customers won't have to worry about having their payment details stolen by third-parties like hackers and bots. SSL allows encrypted data to be shared between your web server and your customer's browser, so hackers "listening" in on the transaction won't be able to make sense of the data being transmitted.

If you search "google requires SSL," you will see that Google itself aggressively encourages eCommerce websites to have SSL, or they will flag your site as "not secure." You and I both know that is not going to look good to your clients and potential customers.

Many commercial web hosts now include free SSL with their hosting plans. If your host doesn't offer free SSL, you can still use Let's Encrypt SSL which is a free, automated and open Certificate Authority.

Installing though will take some technical know-how, so if you're not confident in your technical skills, you can either hire a developer to do it for you or you can just go with a web hosting provider that offers free SSL!

5) Back up your WordPress website regularly

> ***I cannot state this enough - make sure you do regular backups of your website***.

Popular sites can get defaced by hackers at any time. Even if you are a “small” website, make sure that if unfortunately, that happens to you, you are secured by the fact that you have a copy of everything, and it’s just a matter of re-uploading your content.

It’s not just about the hackers, though. It is important to have a copy of everything should there be a case where your files on your local computer get corrupted.

Sometimes, your hosting provider might do an update for added features or added security, and the update MIGHT go wrong, erasing all your files. You panic for a minute, then you rest easy because you have a copy of your site’s data and you can simply re-upload it to your web server.

Or, how about the horror of viruses! A malicious email or software opened by a naïve employee, and your files will be gone forever. Avoid this by having regular backups, and perhaps train your employees to learn how to recognize malicious software from a legit one.

Human as we are, we tend to make mistakes. Employee errors on website files? That can be catastrophic. If you have a back-up of your site, you can go back to a working version of your site and continue with your business as usual.

Just think about it this way: with regular backups, you’ll have the reassurance and peace of mind that you have all your WordPress files saved.

Final Words

Admittedly, some of the tips above can be challenging to set up if you don't have a technical bone in your body. And just because you do all the things above doesn't mean your site is 100% secure either. But, at least, you're doing your part to minimize 100% data loss which would be truly devastating.

What I can guarantee though is that whatever measures you take, it will be worth it in the end. Prevention is better than cure, as the saying goes. Yes, it might be a bit challenging to set up your site's security.

But really, a little pain today will be the joy of tomorrow. You don't want to rest easy now and avoid responsibilities, just to panic when your site gets attacked.

> ***Look at the end game and always be proactive when securing your site.***

I highly recommend going through the suggested steps above, having peace of mind never hurts anyone.