

# Protect Your Websites and Beat the Hackers

By: [your name]

# Contents

|   |    |
|---|----|
| Essential Tips to Keep Your WordPress Blog Secure.....                          | 3  |
| How to Use a Password Service to Protect from a WordPress Security Breech ..... | 3  |
| WordPress Site and Dangerous Hackers.....                                       | 4  |
| 10 Must Use Plugins to Improve Your WordPress Security.....                     | 5  |
| Essential Plugins to Harden Your WordPress Security.....                        | 6  |
| 5 Things You Can do to Secure Your WordPress Site.....                          | 7  |
| How to Prevent Hacking of Your WordPress Site .....                             | 8  |
| Discover Just How Hackers Will Determine Your Password .....                    | 9  |
| How You Can Protect Your WordPress Site from Hackers.....                       | 10 |
| Avoid Lock Outs and Protect Yourself from WordPress Hackers.....                | 11 |
| How to Protect Your Website from Plagiarism.....                                | 12 |
| Making Sure Your WordPress is Securely Installed.....                           | 13 |
| Password Security in WordPress .....  | 14 |
| 6 WordPress Security Tips to Protect Your WordPress Site from Danger .....      | 14 |
| Its Easy to Protect Your WorePress Website Against Security Breaches.....       | 15 |
| Using a Password Service to Protect Your WordPress Site.....                    | 16 |
| Say No to WordPress Hackers With Better Security.....                           | 17 |
| 5 Changes to htaccess to Improve Your WordPress Security .....                  | 18 |

## Essential Tips to Keep Your WordPress Blog Secure

If you have a WordPress blog you need to be concerned with security just like you do with any website. Hackers are always looking for an opportunity to attack a site and your WordPress blog could be a target. Here are some essential tips to help keep your blog secure and hacker free.

Hide your login error messages - Error login messages could provide hackers with ideas about whether they have figured out your username and password correctly or incorrectly. It is a good idea to hide it from all unauthorized logins. Just add the following code in functions.php

```
add_filter('login_errors',create_function('$a', "return null;"));
```

Maintaining backups - Keep backups of your entire WordPress blog. This is just as vital as it is to keep your site secure from hackers. If the hackers are successful at least you will have a full backup files to get your site up and running again quickly.

Changing default "wp\_" Prefixes - Your WordPress blog might be at risk if you are using the predictable wp\_ prefixes in your database. Use the WP Security Scan plugin.

Prevent directory browsing - Another security issue is when your directories and all the files in the directory are accessible to public. Use this test to check if your WordPress directories are properly protected:

\* Enter the following URL in browser, without the quotes. "http://www.domain.com/wp-includes/" If it shows blank or redirect you back to home page, you are safe. However, if you see screen similar to the image below, you are not.

To prevent access to all your directories, place this code inside your .htaccess file.

```
# Prevent folder browsing  
Options All -Indexes
```

Keep WordPress core files & Plugins up to date – One the easiest ways to keep your WordPress site safe is to imply make sure your files are always current. Here are few ways you can do that:

\* Deactivate & remove plugins not used – Unused plugin will eventually become outdated and can cause a security risk so it is best to delete them.

\* Login to your dashboard frequently –When an update is available you will see a A yellow notification at the top of your dashboard. Login frequently and keep up to date with the most recent WordPress files. Subscribe to WordPress Releases RSS.

That's just a few essential tips to keep your WordPress blog secure. There are plenty of others. Remember the more you do the less you are at risk.

## How to Use a Password Service to Protect from a WordPress Security Breech

The solution to WordPress password security is to take advantage of one of the password services that will generate up to 50 characters of random gibberish. Then it will memorize that

password for you so you don't have to. Each website will have a new and unique password generated for it.

So how does the password service keeps all these preposterous passwords secure? Easy! You have a master password for the service. This must be something that you are going to be able to remember. It will keep all of the other passwords safe and secure. Even if it's stolen by hackers, to access all of your passwords they would need your master password.

It may seem like a complicated security approach, but it does work. It certainly is a solid method to keep your WordPress site safe, along with the rest of your digital life.

Here are some tips to get the most from your password service:

#1 Have a Good Master Password - The strength of your master password is key. This must be a strong password. It should follow all the criteria that makes a strong password and you will likely need to spend time memorizing it, but it should be one of the few passwords you'll ever have to remember again.

#2 Passwords That You Will Need to Type - Your master password is not the only password you will have to memorize. A password service doesn't work on some passwords. This means even with your password service there are handful of passwords that you will still have to remember. Make sure that they are good ones! Thankfully, by using a password service the number of passwords you will have to remember in total should be way below a dozen.

#3 Remember, it Takes Time – When you transition from taking care of your own passwords to having a password service generate and track your passwords, you need to remember that it's going to take time. So be patient!

#4 Consider Two-Factor Authorization – If you really want to increase your WordPress password security you can use what is called the two factor authorization where there are two levels of authenticity, making it that much more difficult for hackers to gain access to your WordPress site.

A password service is a great way to get the strongest passwords possible and that's good protection!

## **WordPress Site and Dangerous Hackers**

Hackers – they are everywhere – so when you hear about them out on the web looking to wreak havoc on your WordPress website, it's not at an exaggeration by any strength of the imagination. Your WordPress blog and every other website on the internet are at risk if some safety precautions are not put into place.

Malicious hackers have taken down big corporations like PayPal, banks, the US Government, and the list goes on. If they can be hacked, you are probably thinking you don't have a chance at stopping them. You'd be wrong. With a few things that you can do yourself to help protect your site.

Of course, by no means are these tips fool proof, but they will certainly help to increase your site's security and every little bit of help can go a long way towards decreasing your risk. After all, there will be easier targets out there.

If you protect your site and other WordPress users do not, then you are still at risk. If they protect their site and you choose not to then they will still be at risk. This needs to be an undertaking by all users of the WordPress site.

All websites are at risk, but some are at a higher risk than others. If you believe your site is at higher risk, then you need to put stronger measures into place. You might want to hire the pros.

For most of us, there isn't a need for extreme measures. Just the implementation of a couple of simple security steps could save you plenty of hassle. These include a different user name than the default 'admin,' strong passwords, protected files, current backups, installed updates, limited login attempts, and more. Take the time to do the tasks that will protect your website from hackers or at least reduce the likelihood that you will be targeted and your website hacked.

But why are hackers so intent on hacking your WordPress website? There are numerous reasons, but these are some of the most common:

- \* To hijack your website's traffic
- \* To access paid items
- \* To create links back to their website
- \* To collect your users email addresses
- \* To create links to another site (paid for links)
- \* To place content on your site

Being aware of these dangerous hackers is the start to making your website safe and less of a target.

## **10 Must Use Plugins to Improve Your WordPress Security**

If you have a WordPress website, security should be a primary concern of yours. In many cases WordPress blogs are at risk because of outdated plugins and files. These outdated files can be traced by hackers making them a prime choice. If you want to keep your blog away from the hackers make sure you are always up to date and ensure these 10 plugins are installed.

#1 Login Lockdown – The Login Lockdown plugin will assist you to lock attempts after a specified period of time and/or specified number of attempts to log in to your admin panel keeping your site that much more secure, because hackers can't continue to try until successful

#2 Stealth Login - The Stealth Login plugin will assist you to create custom URL addresses for login, for your registering and for your logout of WordPress.

#3 User Locker - If your goal is to stop brute-force hacking on your website, then the User Locker plugin is exactly what you need. The User Locker works on the same system as the

Login Lockdown plugin. However, it is a 5-stars rated WP plugin and those who use it think highly of it.

#4 Login Encryption - Login Encrypt is another security plugin. It takes advantage of complex combinations of DES and RSA to both encrypt and secure logging into the admin panel keeping your site safer.

#5 Antivirus - Antivirus is a popular security plugin which will assist you in keeping your WordPress blog secured against viruses, malwares, and bots.

#6 Exploit Scanner - Search the files and database of your WordPress install for any signs that your files or your WordPress database have been compromised to ruthless hackers. Even though it is another plugin that scans it's still worth trying.

#7 Block Bad Queries - This plugin attempts to block away all malicious queries attempted on your server and WordPress blog. It works in background, checking for excessively long request strings (i.e., greater than 255 chars), as well as the presence of either "eval(" or "base64" in the request URI.

#8 WP-DB Manager -This is an excellent plugin that lets you manage your WP database. You can use it rather than WordPress Backup Manager.

#9 Limit Login Attempts –The Limit Login Attempts plugin blocks the internet address from making any further attempts after a specified limit of retries has been reached. This plugin makes it more difficult for a hacker to use a brute-force attack.

#10 Ask Apache Password Protect - This plugin will not mess with your WordPress database and it doesn't control WordPress but rather it uses reliable built-in security features to add numerous multiple layers of security to your WordPress blog.

## **Essential Plugins to Harden Your WordPress Security**

If you are running a WordPress site, security needs to be your primary concern. In many cases, WordPress blogs are compromised because of outdated core files and/or plugins. Files that are outdated can be traced and you are providing hackers with an open invitation to your site. Here are some essential plugins to make sure you have installed.

### **WP DB Backup**

WP DB Backup is an easy to use plugin that allows you to backup your core WordPress database tables with just a few mouse clicks. Don't let its ease of use fool you – this is a powerful tool and it remains one of the most popular plugins to secure WordPress powered websites.

### **WP Security Scan**

Using this plugin, scanning your WordPress site become a simple task to carry out. It will find the vulnerabilities in your website and it provides useful tips on removing them.

### **WP-DB Manager**

This is yet another terrific plugin that lets you manage your WP database. It can be used as an option rather than using the WordPress Backup Manager.

#### Ask Apache Password Protect

This plugin does not control WordPress, nor will it mess with your database. Rather it uses speedy, proven built-in security features that provide a number of multiple security layers to your blog.

#### Admin SSL Secure Plugin

This is another plugin for keeping your admin panel secure. It acts on your SSL encryption and is extremely helpful against hackers or others who are attempting to get access to your panel that isn't allowed. It is an adversary for the Chap Secure Login Plugin.

#### Limit Login Attempts

Limit Login Attempts blocks the internet address from making any further attempts after a specified number of retries has been reached, which makes a brute-force attack next to impossible.

#### One Time Password

This unique plugin will help you to set a one-time password for your login. This will stop unwanted users from logging in from internet cafes or other open sites.

#### Bad Behavior

Bad Behavior is a plugin that aids in fighting annoying spammers. The plugin will help you prevent spam messages on your blog, and it will also attempt to limit access to your WordPress blog, so they will not even be able even to read it.

#### User Spam Remover

This plugin has a name that gives away just what its function is. This is a popular plugin that helps in the prevention and removal of unwanted spam messages.

There you have it – a handful of essential plugins you should install on your WordPress blog.

## **5 Things You Can do to Secure Your WordPress Site**

Making sure your WordPress site is secure from hackers is important. Being hacked is no laughing matter. It can result in a loss of all your data, the collection of your personal information and that of your customers or followers, and it can put you at risk financially. Let's look at 5 things you can do to help secure your WordPress site.

### **#1 Fix Any Malware Issues**

Find a way to clean up detected malware issues. It's common for blog owners to underestimate the cost of being down related to security problems or the time it takes to deal with an issue. Sucuri is a good solution for removing malware.

### **#2 Choose a Host Provider**

If you have your blog on a server that is shared your security risk goes up tenfold. Consider the risk to your blog and then multiply that risk by the number of other sites and blogs on that

server. That's what your risk is. A dedicated server or VPS may be more than you can handle, but another good choice is WordPress hosting that's managed. It's certainly worth the cost as you get better security, better support, a faster site and automatic backups.

### #3 It's Time to do Some Site Clean Up

You need to keep your blog nice and tidy. Remove old plugins you aren't using. Delete themes you no longer use. Host websites that are in development on a different server than websites that are live.

### #4 Control Sensitive Data

When you are doing your site clean up, make sure you aren't leaving behind any sensitive data for the world to be able to gain access to. Check all of your php files, because these are like road maps to your site setup and give a hacker all of the information they need to 'bust in.'

Don't keep your backups on the server with your site files. That's just encouraging a hacker to download them and use them to hack you're the site. Disable directory browsing to stop a hacker from seeing the blog's folders.

Be careful when you are using the CPanel file manager and having it save copies of your important files temporarily. You are much better off using secure file transfer protocol.

### #5 Don't Let Your Guard Down

This might seem obvious, but it's not always practiced. You need to be vigilant about staying on top of everything on your site. This will decrease the risk of eing hacked.

## **How to Prevent Hacking of Your WordPress Site**

Computer hacking can occur different ways. Your computer system might be hacked and mined for your personal information. If your password is obtained, your blog or site might be at risk. Use all or some of these steps to protect your WordPress from being hacked and other hacking.

There are a number of ways to protect your database-driven ASP or PHP site from being attacked by the hackers, that range from weak to strong security. Learn the most efficient ways to slow down the hackers who use methods like SQL injection attacks and/or XSS by means of the URL query string and form inputs.

Two common types of hacker blocking techniques are input validation and custom error pages. These methods are so simple you won't have any problem doing them even with just basic coding knowledge. Your greatest strategy would be to put up one or more obstacle.

1. SQL database driven websites are at risk.
2. Setup custom error pages.
3. Keep the details of your database from getting into the hacker's hands with the setup of a custom error page for your website. Hackers will not see any detailed error messages. If you do nothing else, this is the one thing that every site needs. Otherwise, you are basically providing



the hackers with an open invitation into your site's database and offering the hackers all the information they require to launch an attack.

4. In addition to hunting for errors, hackers can enter more dangerous code than a simple single quote in the URL query string. In an attempt to carry out malicious scripts on the database, a variety of creative coding is engaged, such as %20HAVING%201=1; shutdown with no wait-- or even a lot worse. Once the hacker can carry out these scripts, the defenseless database is like theirs for the taking. The hacker never needs to have the database login, nor does the hacker need the connection string because he/she is utilizing the URL query string, where there is already has an open connection.

5. To check if the input entered into your URL query string or your text box is actually safe, you can use input validation rules. Using ASP code on your web page(s) can authenticate the input collected from the query string to make sure it includes only characters that are safe. Once it is deemed to be safe, it can then be stored in a new variable, then inserted into the SQL string and sent to your database.

These are a few technical ways to prevent hacking of your website. Put them to good use.

## **Discover Just How Hackers Will Determine Your Password**

We hear a lot about creating strong passwords. So while we are talking about passwords relating to your WordPress blog, the reality is that this applies to any site that you would be logging in to. Sadly, even with all the talk about passwords, many are still creating passwords that the hackers have no trouble breaking. So, let's look at just how a hacker determines your password, because this could help you understand just what you need to do to create a strong password.

Sometimes, it's as easy as a user creating a password like 12345 or 54321 and thinking they are secure that gets them in trouble, but some people actually do try to create a good password and still find they have been hacked. That's because hackers have gotten very smart at cracking passwords.

- \* Variations - The programs these hackers use allow them to try many variations. So simply placing a number or character at the end of your password will not make it any securer.

- \* Tricks - Hackers know most of the same tricks you do for coming up with a password. They know that a person replaces certain letters with numbers or symbols. They know that a person replaces phrases, words or quotes. If you read about a trick to make your password stronger, remember the hackers likely also read about it and so will implement it in their hacking schemes.

- \* Predictable - You may think your password is random, but it likely isn't. People are much more predictable than you might think, and the hackers will take advantage of that. If you think choosing a phrase from the Bible, is safe think again. If you think a phrase from a literature piece is safe, you'd be wrong. Hackers use dictionaries to find words that can be used as passwords, but they also use tools like YouTube, or Wikipedia, to name just a couple, to discover the most common quotes and phrases, to learn what slang is currently popular, and even to find words that have been made up online.

\* Password Breaches - Whenever hackers explore a volume of password data, they are able to get a better understanding of just how people arrive at their passwords that goes far beyond common words and phrases.

\* Brute Force – There is no question that often hackers will rely on what are called brute force technique, which will run through millions of password combinations in short periods of time. Hackers can use these tools offline so using login limiters is of no benefit in these situations.

Now that you have a better understanding of how hackers figure out your password, you'll be able to create a stronger password.

## **How You Can Protect Your WordPress Site from Hackers**

These days your WordPress website security is no laughing matter – in fact, you could say it has become downright treacherous as more and more people come to find themselves left with the devastation of a hacker. Rather than being a statistic, now is a good time to take action and do what you can to protect your WordPress site from hackers. Let's have a look at a few things you can do.

### **#1 Protect Your wp-config.php**

This is an important WordPress file and so you will want to make sure it is protected. You can hide it so it is not available for public view just by putting a few lines of code into your htaccess file.

```
<Files wp-config.php>  
order allow, deny  
deny from all  
</Files>
```

Add this code and it will stop the wp-config.php file from being visible to public users and makes harder for hackers and robot to spot.

### **#2 Never use "admin" to Login**

One of the most common mistakes is to leave the default 'admin' as your login to your WordPress sight. This needs to be changed right away as this is dangerous and allows hackers an advantage. It's very dangerous leaving 'admin' as your login.

### **#3 Use SFTP**

Most people use FTP to upload their files, but you really should use a Secure FTP connection so a SFTP. That way when you send your files they will be encrypted.

### **#4 Using the Login Lockdown Plugin**

Login Lockdown plugin will make sure that you remember your password. Every failed attempt at logging in is registered along with the person's IP address and it will block the ability to login from different IPs if the login has failed after the set number of attempts, which you control. The default setting is 3 failed logins within 5 minutes per hour. You have the control to remove the blocked IP address from the plugin panel in your WordPress dashboard.

### **#5 WP-DB Backup**

You need to have backups regularly not just now and then when you think about it. This is a plugin that will do this for you and then it will send your backup to your email address and/or store it on the server. An offsite backup is wise because should your site be hacked it gives you the best chance of getting things up and run quickly.

There are plenty of things you can do to make your WordPress site more secure – these are certainly a good start!

## **Avoid Lock Outs and Protect Yourself from WordPress Hackers**

If you haven't already experienced a lockout or hacker intrusion, you are one of the lucky ones. The effects of hacking are not minor, they can bring down your entire operation, cause you to lose all of your work. Don't put securing up your website at the bottom of your to do list or it might be too late. Let's look at some things you can do to make sure your site is secure.

### **#1 Start by Creating Solid Passwords**

One of the easiest ways to get through a site's security is with their password. Many people put off creating solid passwords because they claim they take too much time, but think about the time it will take to try to rebuild all your hard work.

- \* Every password on every site should be different
- \* Every password should be at least 15 characters
- \* A password is strongest if it is not a real word
- \* Use a mix of capital letters, lowercase letters, special characters and numbers.

Your password is your first line of defense against hackers, so make sure it's strong. Never write your passwords down, they should always be kept in your head or you can use password manager software.

### **#2 Make Sure Your Site is Up to Date**

WordPress has a lot of updates, too many people don't bother getting all of these updates, and many of them fix security breaches and bugs, as well as providing the latest features. Sure, it's hard to stay ahead of the hackers, but taking every step possible makes good sense.

### **#3 Change Your WordPress User Name**

When you set up your WordPress account, you will get a default login username of admin. You need a good username with a strong password.

### **#4 Protect Yourself from Brute Force Attacks**

You may not be aware, but almost every website receives more than a couple hundred unauthorized login attempts every single day and that includes your website. To guard against a brute force attack make sure you have put into place all of the suggestions. You can also install "limit login attempts," a plugin for WordPress users that will lock out the hacker after a certain number of failed logins.

### **#5 Monitor for Malware**

You must be constantly monitoring your site for malware. WordFence is a good solution for your WordPress site and it's even free. Sucuri is another solution, but it's a paid program, and it has additional features.

## How to Protect Your Website from Plagiarism

The WordPress Protection Plugin offers you complete security for a WordPress site so that you can ensure that data remains secure and plagiarists are not able to copy and steal your data and images off your WordPress pages.

Use the WordPress Protection Plugin (Lite), to block Keyboard Shortcuts (like CTRL+V, CTRL+A, CTRL+C, and CTRL+X), and disable the text-selection, and it will also block the use of right click on your website. You can also purchase the full professional version of WordPress Protection Plugin.

The plugin features:

- \* It disables keyboard shortcuts such as cut, copy and paste
- \* It disables text-selection
- \* It is fully optimized
- \* It doesn't compromise you in for the search engines, such as Google, Yahoo, or Bing, who will still pickup your content.
- \* It disables image drag and drop

The professional WordPress Protection Plugin offers many many features that the lite does not, so you may want to explore that further.

That's one way to stop your blog from becoming a victim of plagiarism, which is theft! Another thing you can do is create a writing style that is very personal and very recognizable and keep your blog posts long. This will deter thieves as they prefer more generic looking content.

Your blog is actually protected by copyright laws the minute you publish it but it doesn't hurt to also mention it on each post. This should be adequate to discourage potential thieves stealing your content. If you would like to take it a step further, you can register your blog with the U.S. Copyright Office, and create a Creative Commons license, but you don't really have to take this action, it's just an option for further discouragement.

You can also use plagiarism sites like Copyscape to make sure your content isn't elsewhere on the web. It will search for content that is identical or similar and then provide you with a link to that content. Handy tools these programs are.

You should watermark all of your images in a location that is difficult for the thief to cut off or cover over. This will help to protect your images from theft. There are a number of programs that can help you with this task.

If you find that your content has been plagiarized you need to immediately contact that website and provide them the information. Ask them to remove the content or provide credit to you by linking back to your blog.

## Making Sure Your WordPress is Securely Installed

The next thing you need to do is take care of security issues on your site. WordPress has a plugin called Better WP Security that lets you change certain WordPress features to make it more difficult for the hackers to gain access. Be sure to take advantage of this tool to give you the best chance at a secure WordPress site.

Better WP Security will let you:

- \* Change the default 'Admin' username to something different
- \* Lock entrance to the admin at specific time periods
- \* Change your admin user ID from 1 to something different
- \* Ban users based on the IP addresses
- \* Automatically email your database backups to yourself
- \* Change the URL you use to login from wp-login to something different
- \* Change your WordPress directory files from wp-content to something different
- \* Change your database prefix from wp\_ to something different
- \* Check the number of hits on 404 pages and lock the user out if they are excessive
- \* Track any file changes
- \* Limit the number of times you can login attempts with the wrong password

And there's more.

One of the easiest ways to get through a site's security is with their password. Many don't take the time to create solid passwords because they claim they take too much time, but compared to the time it will take you to attempt to rebuild your site, it seems like such a small price.

When you are creating a password:

Every password should be at least 15 characters

Every site should be different

Is strongest if it is not an actual word

Is strongest if it is a mix of special characters, lowercase letters, capital letters and numbers.

### Regular Backups

The last thing you need to do is make sure you are taking regular backups of your site files and database(s). That way should the unthinkable happen, you will at least have a backup safely stored away, which will certainly reduce your stress.

One of the most popular plugins for doing this is called 'WordPress Backup to Dropbox.' This will create a backup and then upload that backup to Dropbox for safe keeping. You can also email that backup to yourself. That's because the Dropbox plugin keeps only one backup, so sending to yourself allows you to keep many versions.

Get busy, add your plugin(s), change your passwords, make your backups and make your site as secure as possible.

## Password Security in WordPress

### WordPress Password Security

First things first, you should do everything you can to make WordPress more secure. The Better WP Security plugin will let you do all of these things quickly and easily. We've hired the developer, Chris Wiegman, and are rolling that plugin into an updated version that will be out soon.

#### 1. Don't Use Admin Username

We've hammered on this before, but do not ever use "admin" as your username. If that's your username, change it. Change it now!

#### 2. Hide Your Login Screen

Another tip to shut down the hackers and bots is to hide your login screen. You can give the page a unique URL and keep the bad element from even getting to it.

#### 3. Limit Login Attempts

This might not stop hackers from cracking your password, but it will stop bots from hitting your login page with multiple attempts. Lock it down.

#### 4. Require Strong Passwords

WordPress password security requires you and every other user to have a strong password, because the person(s) who doesn't becomes the weakest link for hackers to access the entire WordPress platform not just that person's site. So do your part to create as strong a password as you can. Here are some tips to help you:

- \* Use Different Passwords – Always use a different password on different sites. Lazy people use the same password all the time. It's easy for you, but all it takes is one breach and ever single one of your logins are at risk of being hacked and compromised. Oops. One way to do this so that you can remember the password is to create a base password with something different for every website. You can create a pattern so that you won't forget what that add on is. For example, you might add the last three letters of the site name to the end of your base.

- \* Never Be Predictable – Never use anything that's predictable. You are actually likely to be far more predictable than you ever imagined. For example, do you follow suggestions, made in articles or on websites about how to create a strong password? You've just become predictable. Do you think you are sneaky changing letters for numbers? You've just become predictable. See it's that easy.

- \* Use Passwords That Are Long – Long passwords are stronger. Of course, there is no need to go 'nuts' about it, but 8 characters are the shortest your password should be.

- \* Never Use Words or Phrases - Just don't use an actual phrase or word, even when it's not a proper English word. These hackers search real world text and can break just about any password that's simply a word or phrase.

## 6 WordPress Security Tips to Protect Your WordPress Site from Danger

When it comes to Content Management System WordPress is by far the most popular anywhere in the world, with more than 70 million users. WordPress hosts over half the blogs that

are found online and it used by some of the largest companies like NBC, CBS, CNN, etc. There are over 2.5 billion WordPress pages that are read by over 300 million people daily, while around 500.000 new posts and 400.000 comments are posted each day.

There are no signs that the growth of WordPress is going to slow, but what is known is that as more users come on board, the security risk grows higher. It is the responsibility of each user to make sure their site is as secure as possible. Let's look at 6 WordPress security tips to protect your WordPress site from the danger of hacking.

#1 Stay Current - is very important that you stay current and up to date with your WordPress site including plugins and themes.

#2 Increase the Strength of Your Password -We hear a lot about strong passwords and yet we still create passwords that are weak and easy for hackers to obtain with automated software. Instead create a password that is not a real word and uses lower case, capital case, symbols and numbers – this will give you a strong password that's less likely to be hacked.

#3 Watch Your File Permission - You should keep an eye on your file permissions. You can set your file permissions with FileZilla.

#4 Use SSL Encryption - SSL Encryption is used to encrypt the data your blog sends out. This means that the data cannot be accessed as it leaves your router, which keeps account information secure. It makes the data difficult to intercept and difficult to decrypt. Usually you have to be prepare for SSL encryption but it's worth the money. However, WordPress SSL encryption costs you nothing – you just need to add define ('FORCE\_SSL\_ADMIN', true) to your wp-config.php

#5 Use .htaccess - You will find the .htaccess file in the default hosting file, which can be used to block certain IPs.

#6 Always Have a Backup - Regardless of how good your security there is always the risk of being hacked, even if it's minimal, so you need to back up at least once a week. Backup your data daily and store it offsite, so that if you do find yourself hacked you will have a good backup to get back up and running.

## **Its Easy to Protect Your WorePress Website Against Security Breaches**

If you have a WordPress site, it is very important that you take at least the basic steps to ensure you are secure from hackers. This isn't really 'news,' after all this has been known for a long time, yet still many people do not stop and consider website security when they are creating their sites. They don't do any reading on the topic because it's too technical and just plain boring, and far too often people think it won't happen to them. Therefore, they also don't do anything to protect their blog or site. The good news is that in under 30 minutes you can improve your security and not spend a dime.

### **#1 Change the 'Admin' Username**

The default login for WordPress is 'admin.' Trouble is most users just keep it that way, making it incredibly easy for hackers to figure out your user name. Now they are already half logged into your site. Change the 'admin' login into something new!

### **#2 Create a Strong Password**

Your WordPress is only as strong as your weakest link, and your password is often that weak link. Hackers use software that scrolls through hundreds of thousands of words looking for a match, which is why you should not be using a real word for your password. You should also not use a logical sequence of letters or numbers. So don't use your pet's name, your birthday, your phone number, etc. You can use a password generator to help you if you trouble coming up with a strong password.

### #3 Delete & Update

WordPress is known for being weak on security. The reality is WordPress is only insecure when the users do not keep it current. Any part of your website that isn't running the latest version is always at a risk of being hacked. Hackers are constantly looking for vulnerabilities and if you aren't staying current you are at risk. So make sure you are running the most current version of WordPress, installed plugins and installed themes.

### #4 Limit the Login Attempts

Install a plugin that will limit the number of times a person can try to login before the site shuts them down. The Limit Login Attempts plugin is one good choice. When you limit the number of times one can try to access your site, you reduce the likelihood of being hacked.

That's it – there's plenty more so don't stop after you've done these four things, but this is a great place to start.

## **Using a Password Service to Protect Your WordPress Site**

It seems all we talk about is creating strong passwords and if you are like most people, you create a password that you thought was solid only to find out it is not. What's the solution? Using a password service is a great way to create a strong password and protect your WordPress site.

There are a number of these services – two that come to mind are LastPass and 1Password. You install the software on your computer and it will create these wild passwords that are up to 50 characters and really just look like gibberish. What's even better is that it memorizes them for you, because there is no way you could remember these passwords. Then to keep all those passwords secure you use a master password. That way even if your passwords are stolen the hackers are going to need the master password.

A good master password needs to be strong – in fact it's critical because all your other passwords lay in the balance of this. Follow as many password rules as you can and this one you need to memorize.

You'll need to memorize your master password and you will also need to memorize any passwords needed to access your computer or if you visit the internet through your television. Apple passwords also often have to be memorized. The passwords you need to memorize shouldn't be more than a dozen and it will likely be more like 5 or 6.

You will need to be patient as it takes time to transition your entire life online to a password service. You'll be surprised at just how often you use passwords. Think about it – every time you login somewhere you use a user ID and a password. Getting the system up and functioning



completely can be a real challenge, but stick with it, because eventually you will be far more secure and have way less passwords to remember.

You should actually have a password service for your mobile devices and your desktop devices. These are different and will require two different downloads and if it's a paid service two different purchases.

If you really want to boost your password security on WordPress use more than one password. Have a two factor authorization. This means that your login will require two parts of information. For example, your password and something you know. It provides an extra layer of protection in a number of applications including Twitter, Apple, Dropbox and Google.

Today is a good day to get started with your password service!

## **Say No to WordPress Hackers With Better Security**

You may have already heard rumblings about the bots attacking WordPress. Bottom line is that every website is at risk and WordPress is no different. It's important for you to do your part to create a higher degree of security, because you see if everyone else does and you do not, then you become the weak link where hackers can access all the WordPress blogs. The same goes true if you create a strong password and others do not – bottom line, this requires a team effort.

Start by making sure your WordPress installation has the most current updates. Reduce the number of plugins you are using if you can and always delete those plugins you no longer use. Make sure you choose passwords that are hard to crack and always backup your data on a regular bases. Finally, protect your WordPress by making use of .htaccess. Great, that's a good place to start by putting these things into practice.

Now it's time to install a WordPress Security plugin that is designed to block IP addresses that attempt to flood or spam a site. It will also restrict the number of login attempts that can occur and it will monitor your live traffic. These plugins are constantly being updated so you can be sure they are on top of security concerns. Wordfence or Better WP Security are two that can do the job for you.

There's been a great deal of controversy over whether free content delivery systems are good or bad. The best thing to do is try it yourself. Yes, there are some that really only want to lure you to their paid service but two free content delivery networks that minimize your security risk and are free include CloudFlare and PageSpeed Service by Google. Don't be afraid to explore what's out there.

We touched on the .htaccess file earlier. This stands for Hypertext Access and when you configure this file you gain control and reduce your risk of security breaches. Editing your .htaccess file is serious and unless you understand at least basic coding you should hire someone that does. You can quickly become overwhelmed by so many options.

These suggestions don't guarantee you will not be hacked, but what they do is significantly reduce your risk because there is going to be someone else out there that will be an easier target.

## 5 Changes to htaccess to Improve Your WordPress Security

Improving your WordPress security is an integral part of keeping hackers at bay and while there are a number of things you can do, we're going to look at 5 changes to htaccess you can make to improve your WordPress security.

### #1 Ban Bad Users

If you continuously have the same IP address attempting to access your site or attempting to use brute force to access your admin pages, you can ban them by putting this little snippet of code in your .htaccess.

```
<Limit GET POST>
order allow,deny
deny from 202.090.21.1
allow from all
</Limit>
```

They will no longer have access to your site. You can easily add more by just repeating the deny line. Here's an example:

```
<Limit GET POST>
order allow,deny
deny from 202.090.21.1
deny from 204.090.21.2
allow from all
</Limit>
```

### #2 Stop Access To wp-content

The wp-content folder contains images, plug-ins and themes. It is one of the key folders within your WordPress install so you will want to prevent access by outsiders.

This needs its own .htaccess file which you will need to add to the wp-content folder, it lets users see images, CSS etc... but it will protect the key PHP files:

```
Order deny,allow
Deny from all
<Files ~ "(.xml|css|jpe?g|png|gif|js)$">
Allow from all
</Files>
```

### #3 No Directory Browsing

Because of the popularity of WordPress too many people now know the WordPress install structure and where to find the plug-ins that might give away too much information about your WordPress site. You can stop that by preventing directory browsing.

```
# directory browsing
Options All -Indexes
```

### #4 Individual File Protection

There are some files you want to make sure are protected on an individual bases rather than having to block the entire folder they reside in. The snippet example below shows you how to

prevent access to the .htaccess file and doing this will throw a 403 if anyone accesses. You can change the filename c to whatever file you want to protect:

```
# Protect the .htaccess
<files .htaccess="">
order allow,deny
deny from all
</files>
```

#### #5 Protect .htaccess

We are so busy worrying about whether we are using the correct plug-ins or whether we've installed all the updates for fixes, that we overlook that the .htaccess file is open for attack. The snippet below will stop others from seeing any file on your site that starts with "hta", so this will protect your site and make it safer.

```
<Files ~ "^.*\.([Hh][Tt][Aa])">
order allow,deny
deny from all
satisfy all
</Files>
```

This is by no means all of the ways you can improve your security with htaccess, but gives you a good start so get busy.