

# WP MASTER LOCK

*How To Lock Down and Secure  
Your WordPress Sites Today*



# **Introduction**

Recently, many brute force attacks on Joomla and Wordpress sites have been happening, maybe you have heard about this as well?

The odd thing is that there is even an effective online tool available that can be bought and used for these attacks.

Someone hacking into your Wordpress blog may have quite a few disastrous effects on your business. This report will give you an overview of some of them. Some of these are quite simple and can be fixed quickly – for example when you lose access to your website for a little while.

On the other hand, some could be very serious and you could end up losing your work, reputation and money!

The good news is there is always a solution, and even in this case there are things you could do to ensure that your WordPress blog will never have to deal with attacks like these. You will be able to keep your website, its content, your income, data, products and customers safe.

So let's get started protecting your WordPress site.

# **Why You Need To Protect Your Wordpress?**

If your site gets hacked for whatever reason, the best-case-scenario is that you will have temporary issues like discovering that you're locked out and can't access your site since your password has been changed. It may take an hour or two to get back in. It could also be that your site is redirected to some other site and you can fix it quickly.

What you need to be weary of though are the major problems that could occur as a result of an attack.

## **Lost Content**

It would be a much worse problem if someone hacked into your blog and deleted your content and articles. If you haven't backed it up, you could end up losing all the hard work you have done in an instant! Even if you do keep regular backups, any content you have added in between them, also comments, new user details, responses and all the rest will be gone. Sometimes your web server may be too full to make these backups and you could still end up losing your work even if you have automatic backups set up – just make sure it doesn't happen.

## **Lost Personal Data**

Sensitive information that you have stored on your website may also be copied and later used by the person hacking your blog. They may especially be targeting all the financial information, passwords, emails or other sensitive info.

It is even worse if your WordPress password is the same as your email, banking and other critical accounts, it could bring about other catastrophic problems such as identity theft and financial loss.

## **The Basics Of Wordpress Security**

So let's take a look at some of the things that can be done to make WordPress installations more secure. Every time you set up a new blog, take these steps to secure the site, and of course apply them to your current sites as well.

### **Update Your WordPress Installations**

The first thing to do is to update your WordPress often, this protects well against hackers. WordPress has security updates often, not all updates have to be about new functionality or the appearance of the dashboard or the blog.

### **Change Your Username**

See to it that you don't use a simple username to get you in your dashboard. It should not be easy to figure out and never ever use "admin" as your username! Since it's there by default, many people use it. You have to avoid it at all costs.

Your own name and variations should be off limits. Also, nothing related to the name of your blog or the niche you are in. Any variations of your email should be avoided and don't use the same username with other accounts.

## **Select A Strong Password**

Having a strong password to log in to your blog is critical, but still most people use something that's easy for them to remember as they never think about getting hacked. This could end up costing you big time. Try to include both letters (lowercase and capital) and numbers in your password, and also use 8 characters or more.

Don't use variations of your name, username, birthday, email, anniversary, mobile number or other info that the hacker could access. Common passwords that many use are also off limits.

Here is a list of some of the common passwords people use:

Password

Trustno1

Love

Iloveyou

Sex

Letmein

Money

Qwerty

God

Abc123

12345678

Don't use these or anything similar! It's a good idea to use a password generator and let it generate one for you. There are plenty of these generators available and they do give you a secure password.

### **Set A Limit To Login Attempts**

This is a simple and an excellent way to protect your blog from brute force attacks. WordPress has several plugins available that let you set a limit to unsuccessful login attempts. Another useful plugin is the one that lets you whitelist certain IP addresses so you don't end up locking yourself out.

It could be disturbing if you forget or mistype your password and are locked out of your own site. However, it is still worth that extra security you get! This can be easily avoided by using a whitelist plugin and adding all the IP addresses you usually log in from.

### **Two Step Authentication**

To keep your site especially secure, two step authorization could be used. This plugin sends a verification code to your phone by SMS and you have to submit this code to get into your site.

Barcode authentication and Google Authenticator are other two possibilities you could check out.

There are plugins available for your self hosted WordPress installations that let you set up two step logins as well.

## **Protect The “wp-login.php” File With Password**

Another easy thing that makes your site more secure and protects against brute force attacks is protecting the “wp-login.php” file with a password. This file shows the login form for accessing the dashboard of the blog.

It's not difficult to protect this file with a password. You can follow [this simple tutorial by Hostgator](#), however, other hosting providers will have their own set of instructions.

## **Changing Database Prefixes**

WordPress databases begin with “wp\_” by default. Not many users even know this or realize that it could be a problem.

Before changing database prefixes, back your WordPress database up so that nothing can go wrong. Use BackupBuddy for that or do it from your cPanel.

Now you need to open the “wp-config.php” file. This is located in your WP installation's root directory. (Use File Manager or a free FTP program such as Filezilla to locate the file.)

Find the line below:

```
$table_prefix = 'wp_';
```

Then change it to look different, for example:

```
$table_prefix = 'wp_a123456_';
```

It's a good idea to combine both numbers and letters, lowercase and uppercase to get a combination like “zyx321abv987”.

Now you need to find phpMyAdmin from your cPanel. Start it and click on “SQL” near the top. Now you will see all the databases that you have to change. You can either do it manually or click on “Query” and past the following code:

```
01  RENAME table `wp_commentmeta` TO  
    `wp_a123456_commentmeta`;
```

```
02  RENAME table `wp_comments` TO  
    `wp_a123456_comments`;
```

```
03  RENAME table `wp_links` TO  
    `wp_a123456_links`;
```

```
04  RENAME table `wp_options` TO  
    `wp_a123456_options`;
```

```
05  RENAME table `wp_postmeta` TO  
    `wp_a123456_postmeta`;
```

```
06  RENAME table `wp_posts` TO
```



```
`wp_a123456_posts`;
```

```
07 RENAME table `wp_terms` TO  
   `wp_a123456_terms`;
```

```
08 RENAME table `wp_term_relationships` TO  
   `wp_a123456_term_relationships`;
```

```
09 RENAME table `wp_term_taxonomy` TO  
   `wp_a123456_term_taxonomy`;
```

```
10 RENAME table `wp_usermeta` TO  
   `wp_a123456_usermeta`;
```

```
11 RENAME table `wp_users` TO  
   `wp_a123456_users`;
```

Now you simply run the query to change the names automatically. You are still not done. You need to check if there are more instances of “wp\_” anywhere. Again, use query for this. Open query and paste the following:

```
SELECT * FROM `wp_a123456_options` WHERE `option_name`  
LIKE'%wp_%'
```

Now you see a list of results and need to change them manually one by one.

Once this is done, search for fields that still have wp\_ in their usermeta.

Again, change all these manually. Depending on how many addons and plugins you have, there could be a lot of these to change.

After all this is done, back everything up once more (**don't overwrite** the previous backup file!) and test your site!

### **Hide The Version Of Your WordPress**

If you are running older WordPress versions and hackers realize this, it's easy for them to use the info and find security holes which have been fixed with newer versions (which you don't have). Luckily there is a way you can keep your version number hidden from hackers. Follow the two steps below.

First, add this code to your functions.php file:

```
remove_action('wp_head', 'wp_generator');
```

This hides the number of the version you are using from your blog header so nobody can check the source and find out the version.

However, it's still possible to learn the number from browsing your RSS feed! Prevent that by adding more code to your functions.php file:

```
function wpbeginner_remove_version() {  
    return "";  
}  
  
add_filter('the_generator', 'wpbeginner_remove_version');
```

Now the version of the WordPress is hidden everywhere in the blog.

### **Protect Your “wp-config.php”**

This is the most important configuration file and it's usually located in the WordPress root folder, however, this could make it easy for hackers to access and attack the site. But it could actually be moved elsewhere. You should move wp-config.php up one level. Don't worry, WordPress can still find it there.

Here is an example, if currently your wp-config.php can be found at  
/public\_html/wp-config.php

You can place it to:

/wp-config.php

### **Use CAPTCHA**

Last but not least, WordPress can be kept safer and more secure by using CAPTCHA on your login page. Special plugins have been developed for this purpose. One is called “Captcha on Login”. It will enable you to add CAPTCHA but also to change your username from “admin” to something else that's more secure.

Using CAPTCHA gives more security and helps to prevent some brute force attacks quite effectively. Now the hacker needs to enter CAPTCHA for every login attempt. Some hackers pay someone to do

it for them, however most don't want to spend the time or the money, unless they are specifically targeting your blog.

Another feature of this plugin is that it will block any IP after a certain number of attempts have been made unsuccessfully. You can configure the number. In case you already have a plugin in place for this, it's recommended that you install one.

## **Tips to securing your wordpress Sites**

- 1- Use secure webhosting- you get what you pay for, getting the cheapest is not always the best.
- 2- Keep your Wordpress sites updated with the latest versions as they usually contain patches / fixes to any problems that have occurred on previous versions.
- 3- Make sure you use strong passwords, statistics show that most hackers break in due to weak passwords.
- 4- Never use admin as your username as that is the most common username that is used which obviously makes it even easier for hackers to break in.
- 5- Hide your username from the author archive URL as wordpress shows your username.
- 6- Limit your login attempts from a single IP address, this will help deter would be attackers.
- 7- Disable the file editing by the dashboard as hackers can also get in using this method. This can be done by adding the code below to your wp-config.php file.

```
define( 'DISALLOW_FILE_EDIT', true );
```

- 8- Try to avoid using free themes as they can use out of date coding that allows spam to and malware to be inserted in.
- 9- Always make sure you backup your sites frequently as this will prove to be extremely beneficial in the case of a hack.
- 10- There are numerous security plugins out there that can be very helpful in preventing attacks to your sites. Here's a list that can be found in the wordpress.org suppository

<http://wordpress.org/plugins/better-wp-security/> – offers a wide range of security features.

<http://wordpress.org/plugins/bulletproof-security/> – protects your site via .htaccess.

<http://wordpress.org/plugins/all-in-one-wp-security-and-firewall/> – adds a firewall to your site.

<http://wordpress.org/plugins/sucuri-scanner/> – scans your site for malware etc.

<http://wordpress.org/plugins/wordfence/> – full-featured security plugin.

<http://wordpress.org/plugins/websitedefender-wordpress-security/> – comprehensive security tool.

<http://wordpress.org/plugins/exploit-scanner/> – searches your database for any suspicious code.

## **Wrapping Up**

I hope that you now truly understand how important it is to protect your site. There are many reasons why hackers may try to access your site and any of these reasons may bring a lot of trouble and harm your way.

It is not difficult to secure your blog. There are many things you can do and they will only cost a minute of your time.

Now you may be feeling confused and lost, maybe it all looks too technical for you, but do not worry!

If you want an easier way to protect your sites without doing all the technical stuff yourself, then you need to see this.

**[Click Here To Protect Your Site](#)**

(Select an affiliate product to promote here)

## Some Additional Wordpress Security Resources

**Sitelock....**

<https://www.sitelock.com/>

**Wordpress Security for Dummies...**

<http://www.dummies.com/how-to/content/wordpress-security-resources.html>

**Doteasy...**

<http://wordpress.doteasy.com/kb/hardening-wordpress-security/>

**Backup Creator**

<http://backupcreator.com>

**VIP Wordpress Security**

<http://vip.wordpress.com/security/>

**Wordpress.org**

[http://codex.wordpress.org/Hardening\\_WordPress](http://codex.wordpress.org/Hardening_WordPress)