WORDPRESS Security Guard

GUARD YOUR WORDPRESS SITE 24/7!

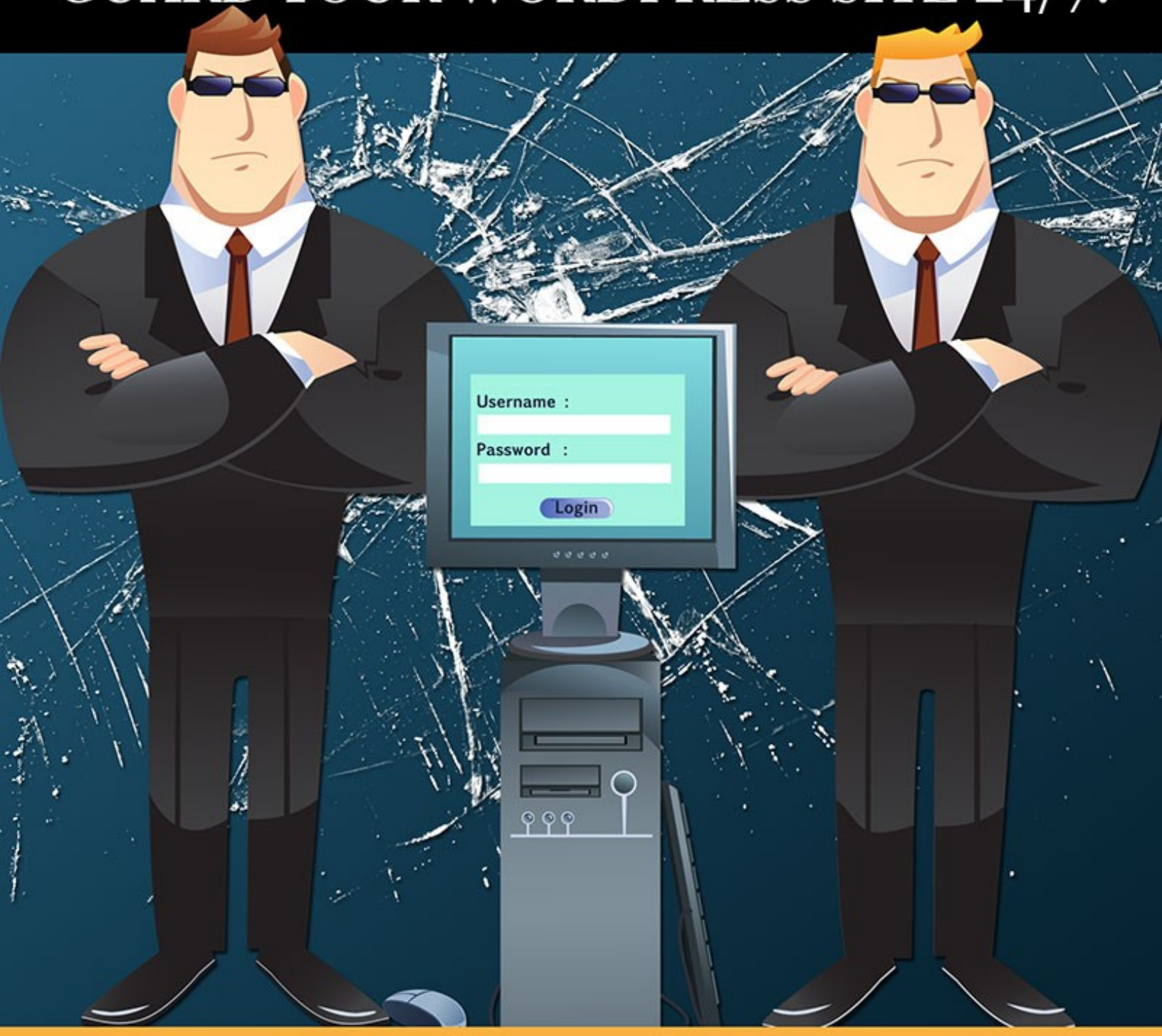

Table of Contents

The information contained herein has been obtained from sources believed to be reliable at the time of publication. The opinions expressed herein are subject to change without notice.
The publisher disclaims all warranties as to the accuracy, completeness, or adequacy of such information.

The publisher assumes no liability for errors, omissions, or inadequacies in the information contained herein or from the interpretations thereof. The publisher specifically disclaims any liability from the use or application of the information contained herein or from the interpretations thereof.

Introduction to WordPress Security Guard

You may have heard about the recent brute force attacks on Wordpress blogs and Joomla sites. There's even a commercially available web-based tool that is currently being used to launch brute force attacks, and it's quite effective.

There can be many disastrous repercussions from having your Wordpress blog hacked. Some of these will be discussed in this report. They could be simple and easily fixable, like simply losing access to your site for a few hours. Or they could be as disastrous as losing money, work or reputation!

Fortunately, there are a few things you can do to secure your Wordpress site against such attacks, and keep your site, your content, your products, your income, your data and your customer's safe!

First, you're going to learn about some of the biggest reasons why it's absolutely vital that you secure your Wordpress installations immediately. Then you'll learn a few things you can do right away to start protecting your site from hackers and other malicious attacks. Finally, you'll find out how to get more help securing Wordpress when you're ready.

So let's get started.

Why Protect Wordpress?

There are a lot of things that can go wrong with a Wordpress blog, and some of those things could be absolutely disastrous to your business.

Temporary Issues

If you're lucky (and by lucky, I'm referring to the best-case-scenario if you are hacked), you will only experience minor, temporary issues due to the hacking. These issues can still lead to big problems if you don't notice them in time, but as far as hacking goes, this is about as benign as it gets.

Temporary issues are simple things such as having your password changed and being locked out of your blog for a few hours until you can get help getting back into it, or having your blog temporarily redirected to another site until you get in and fix it.

Losing Content

Much worse than having temporary issues, you could have a hacker log into your account and delete all of your articles. If you don't have a backup, that could mean countless hours of hard work would be gone! Even if you back up regularly, you could still lose content added in between backups, along with comments, responses, new user information, and more. You could even lose a backup because your web server is too full to perform the backup, and you might not realize this until it's too late!

Losing Product

If you store virtual products on your server like videos, eBooks, graphics, or other content you are selling, those products could be stolen. Not only that, but

hackers could then distribute that content widely, costing you potentially thousands of dollars in lost revenue!

Don't think it matters when your content is distributed? Well, think about this. Many people have admitted that when they find a digital product they want badly, they will first check pirate sites to see if that product is available for free. If, and only if, it is not, then they will buy the product.

If you're selling physical products, the damage could be even worse. A hacker could log into your site and create an order, making it look as though the order has been paid for, and you could unwittingly ship the items before you realize the money isn't in your account.

Losing Money

If a hacker takes your site down for a significant period of time, you could lose a significant amount of money in lost revenue. If your site makes, for example, $2,400 per day, being down for 12 hours would potentially cost you $1,200. Being down for 10 days could cost you $24,000!

Of course, the temporary monetary hit could lead to a larger one. Imagine if a few of your regular customers came by to order that day and saw the site was down. They might assume you've gone out of business and never return. That could mean a very significant loss over what would have been the lives of those customers.

In the event people have already bought and paid for merchandise, they may ask for refunds or even seek chargebacks through their credit card companies. This can negatively affect your standing with your merchant account!

Losing Personal Data

If you store any sensitive personal information on your server, that information could be stolen and used by hackers. Emails, passwords, financial information, and other sensitive information could all be targeted.

Additionally, if your Wordpress password happens to be the same as your email passwords, banking passwords, or other critical passwords, you could be facing financial loss, identity theft, or other catastrophic events.

Losing Reputation

Your reputation is everything in business. Once it's damaged, it can take years to repair. In fact, it may never recover to its former status.

You may be wondering how your reputation could be damaged so badly by something so seemingly benign. Well, there are many ways, such as:

1. If your site is down, people may think you've disappeared, or your company is fly-by-night. This is especially true if they've placed and paid for an order that has not yet been delivered.
2. If your site is defaced, it could seem as though you did it. Hackers could lace your site with pornographic content or malicious software that could harm visitors' computers or steal their data. It may be hard to convince people you had nothing to do with it, especially if your reputation isn't yet well established in your industry.
3. User data could be stolen. If you have people register to post on your site, or if you store their financial information on your site after purchases, hackers could steal and use that information. This could be extremely detrimental to your reputation.

These are just a few of the ways you could be negatively impacted in the event of a hacking attempt. There are many more!

Why Hackers Hack

You may be wondering why people even bother to go through the trouble of hacking Wordpress blogs, especially a smaller blog that doesn't have a lot of traffic. There are a number of different reasons why hackers do what they do.

Here are a few:

1. Many hackers do it out of curiosity, boredom, or bragging rights. They aren't malicious. They just want to practice their skills or brag to their friends they got in. The worst this type of hacker is likely to do is deface your site with a calling card to prove to their friends they did it.
2. Some do it to be mean, often because they think it's funny. These hackers have one purpose, and that is to harm you or piss you off. They are likely to delete content, lock you out by changing your password, redirect to pornographic websites to hurt your reputation, or something similar.
3. Some do it for financial gain. They may redirect your blog to an affiliate link, to their own website, or they may steal financial information you may have stored on your blog. This type of hacker is likely to take sensitive information and use or sell it, or to install malicious software that installs on visitors computers and infects their system with adware.
4. You may even be targeted by competitors who hack you in an attempt to make you lose your search engine rankings, lose traffic, or hurt your reputation.

There are many other reasons someone might want to hack a Wordpress blog, but these are some of the most common.

Basic Wordpress Security

This section is going to focus on some very basic things you can do to secure your Wordpress installations. You should be taking these steps on every single blog you set up, and you should be doing it **without fail!**

Update Wordpress

The easiest thing you can do to protect your blog from hackers is to update your Wordpress installation often. Wordpress issues critical security updates from time-to-time, so don't become complacent and think all updates are purely cosmetic or offering new functionality. Those security updates are absolutely vital, and they can stop some really nasty stuff dead in its tracks!

Choose a Good Username

Be careful not to choose an easy username for logging into your Wordpress admin area. Make sure it is not easy to guess, and whatever you do, **do not use the username *admin***! Nearly everyone uses it, because it's default upon install, so avoid it like the plague!

Also, don't use your name or any variation of it. Don't use anything having to do with your blog's name or niche. Don't use any variation of your email address or any other usernames you may have.

Use a Strong Password

A strong password is absolutely critical, yet most people choose something easy to remember thinking they'll never get hacked. This could be a big mistake! Your password should contain, at the very least, both numbers and letters (both capital and lowercase) and consist of at least 8 characters minimum.

Never use any variation on your username, name, email, birthday, anniversary, phone number or any other information a hacker may have access to. And never use common passwords or even include them in yours.

Some of the most common passwords include:

- Password
- Love
- Sex
- Money
- God
- 12345678
- Abc123
- Qwerty
- Letmein
- Iloveyou
- Trustno1

Avoid using anything even close to these passwords! In fact, you may want to use a password generator and then keep your password secure using a password manager. There are many of these on the market, and will keep your password secure without allowing you to forget it.

Vary Login Information Across Multiple Blogs

Another mistake people commonly make is using the same login information for multiple blogs. If you have several different blogs, be sure to use different usernames and passwords for each so if one is compromised, your others can't easily be attacked.

Remember, there are websites that will allow someone to see all of the other domains hosted on your server, so if your Wordpress installations all reside on the same hosting account, it's easy for hackers to find your other blogs in order to target them.

Don't Use Usernames or Passwords from Other Sites

If you are a member of a forum, social network, etc., never, ever use one of those usernames or passwords as your blog username or password! If the forum or website gets hacked and user data stolen, your blog could be compromised! Use something different for **every** site you register with, including your own!

Limit Login Attempts

One very simple thing you can do to thwart brute force attacks is to limit login attempts. There are plugins available on the Wordpress website that will let you limit login attempts. Additionally, you can get the Whitelist IP plugin that will let you add your own IP addresses to a whitelist to ensure you don't accidentally lock yourself out.

You may experience some minor frustration if you accidentally lock yourself out if you forget your password, but the extra security is worth the potential of frustration! If you use the whitelist plugin and add any IP addresses you might log in from, this isn't likely to happen.

Two Factor Authentication

If you want to make sure your site is extra secure, you can use a two-step authorization that sends a secret verification code that cannot be guessed to your mobile phone. You must then enter this code onto your blog.

There are also other types of two factor authentication such as Google Authenticator and barcode authentication.

You can read more about two factor authentication here:

>> http://en.support.wordpress.com/security/two-step-authentication/

You can get plugins for your own hosted Wordpress installations that will let you use two step authentication.

Type your text

Password Protect wp-login.php

One easy way to make it harder to brute force attacks to get through is to password protect the file wp-login.php. This is the file that shows you the form to log into your blog.

It's relatively simple to password protect this file. Hostgator has a simple tutorial you can follow, although this may or may not work on other hosting accounts:

>> http://support.hostgator.com/articles/specialized-help/technical/wordpress/wordpress-login-brute-force-attack

Change Database Prefixes

By default, the databases used by Wordpress begin with the prefix wp_. Most people don't even realize this, or if they do they don't understand why it is a problem.

Before you attempt this, backup your Wordpress database in case something goes wrong. You can use a plugin like BackupBuddy to do this easily.

Next, open your wp-config.php file. You will find this in the root directory of your installation. (You can use an FTP program like Filezilla, which is free, to find the file on your server.)

Locate the line that looks like this:

$table_prefix = ‘wp_’;

And change it to something like this:

$table_prefix = ‘wp_zyx321abc987_’;

You can use any combination of letters, number and underscores, including both uppercase and lowercase letters in place of “zyx321abv987”.

Next, log into your hosting account cPanel and search for phpMyAdmin. Enter this and click the “SQL” tab at the top. This will show you the different databases that must be changed. You can change these manually, or click the Query tab and paste this:

```
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`;
```

Then run the query and it should change the names for you.

You're not quite done. Now you must search to see if there are any other wp_ lurking about in the options table. You can use another query to do this. Go back to query and enter this:

```
SELECT * FROM `wp_ zyx321abv987_options` WHERE `option_name`
LIKE'%wp_%'
```

Go through all the results and change them one at a time.

The next step is to search for any fields still using wp_ in the usermeta. Here is the query for that:

Change these manually. If you have a lot of plugins and addons, there may be several to change.

Finally, create a new backup (**do not** overwrite the old one!) and test the site!

Hide Wordpress' Version Number

If you aren't running the latest version of Wordpress and hackers find out, they can exploit this by using security holes that newer versions have plugged up. Fortunately, you can hide the version number from hackers using a simple two-step process.

First, open functions.php and add this simple line of code:

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

This is enough to get rid of the version number in your blog's head area so people can't view the source of the page and learn your version number.

However, hackers can still access the version number through your RSS feeds! To thwart that, add the following line of code to functions,php:

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

This will keep the version number hidden from all areas of your blog.

Protect wp-config.php

The configuration file for Wordpress is typically found on the root Wordpress folder, making it a simple way for hackers to attack your site. However, it doesn't have to be there. Instead, you can move it up one level. Wordpress will still find the file.

For example, if your wp-config.php file is located here:

/public_html/wp-config.php

Move it to:

/wp-config.php

CAPTCHA

A final method for securing your Wordpress site is through the use of a CAPTCHA form on the login page. There are plugins that will allow you to do this. One such plugin is known as "Captcha on Login". This plugin will also allow you to change the default "admin" username to something more secure if you already have blogs that use it.

Using CAPTCHA on your login page will help prevent brute force attacks, because it adds an extra layer of protection. Hackers will have to spend time entering the CAPTCHA, or paying someone to do so, for every login attempt. Most hackers will not be willing to do this unless your blog is a prime target for some reason.

Additionally, the “Captcha on Login” plugin will block IPs after a specific number of failed attempts, which you can configure. So if you’re not already using another plugin to do this, it will add that additional layer of protection.

Final Words

Hopefully you now fully understand the gravity of the situation. Hackers may hack your blog for a variety of different reasons, and many of those reasons could end up causing you serious harm.

Fortunately, securing your blog isn't difficult. You can take a few of these simple steps right now, and they'll only take you a few minutes to put into place.

Don't forget, there are many other elements of Wordpress security to keep in mind that can't fit in a simple report. Those include elements such as:

1. Hotlink Protection
2. Video Protection
3. Folder Protection
4. Indexing
5. PDF Security
6. Piracy Protection
7. And More

If you're feeling a bit lost and confused, or like all of this is too technical for you to wrap your head around, don't worry! Help is on the way. Check the next page of this document to find out how to get more help security your Wordpress installation even if you feel like you have no idea what you're doing! You'll learn how to protect practically **every** aspect of your blog for true lockdown security!