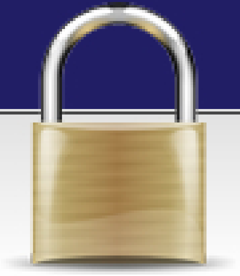
HOW TO MAKE WORDPRESS

MORE SECURE



VIDEOUSERMANUALS

Making WordPress More Secure

The worst thing that can happen to your client is to have their website hacked. If you have not had any experience with this then trust us, it is bound to happen at some point.

As a rule, we do not offer hosting to our clients, basically because we are web developers, not system administrators. We recommend our clients go with the larger hosting companies like Bluehost, Hostgator etc. However, if you read the small print or these companies you will know that they do not take responsibility for backing up sites. For example:

> *Hostgator: You are responsible for your backups and web content. We create our own weekly backups on the shared servers, and we can restore from those. However, this is NOT a procedure you should rely on to keep your content safe.*

If a site does get hacked, then it is inevitable that your client is going to contact you at some point, even if you don't host the site yourself. So what are you going to do, and how can you help prevent it from happening?

Preventative Measures

The following are some steps that we have built into our setup process, which only add about 5 minutes to the total time, but we feel are important measures to take.

If this is your first experience with WordPress security, we highly recommend you install the WP Security Scan on one of your installations, and see if the permissions for the files are set up correctly. Through experience we now know what the permissions should be set to, and we don’t actually use this plugin ourselves, but it is still worth a look.

Secure Your .htaccess / wp-config.php file

Add this to your .htaccess file in order to protect it and the wp-config.php

```
<Files .htaccess>
Order Allow,Deny
Deny from all
</Files>

<Files wp-config.php>
Order Deny,Allow
Deny from all
</Files>
```

Remove the wp-admin/install.php file

WordPress instructs you to do this, but many people forget this simple step.

Password Protect The wp-admin folder

One of the biggest causes of WordPress hacks if choosing weak passwords. You can password protect your wp-admin folder using your cpanel, and at least that way you have 2 passwords that need to be broken in order to gain access to the wp-admin.

File Permissions

It is best to lock down the file permissions as much as you can. Letting people / application to have write access to your clients files can be quite dangerous.

Files - set permission to **644**

Folders - set permission to **755**

Generate Authentication Security Keys

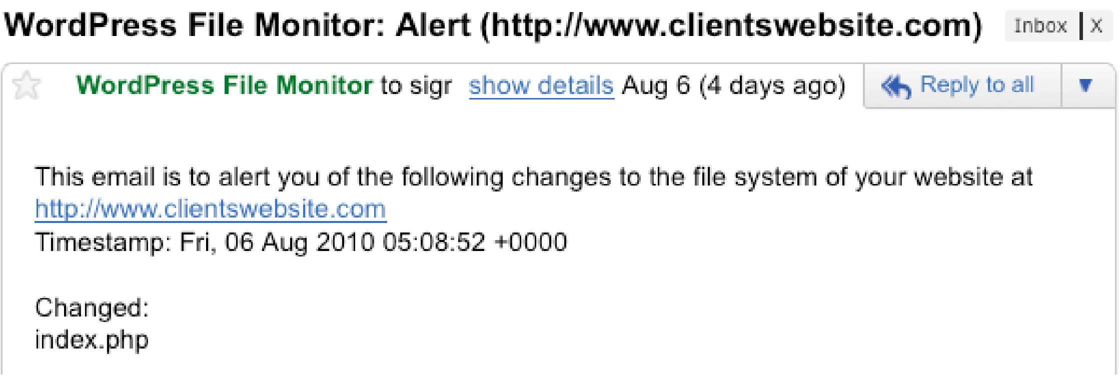
From WordPress 2.6 onwards there has been the ability to add authentication keys which were added to encrypt the information store in cookies more difficult to crack. This is a really simple step, just go here: https://api.wordpress.org/secret-key/1.1/salt/ and paste the information into your wp-config.php file.

Block Bad Queries Plugin

This plugin protects WordPress against malicious URL requests. Many WordPress sites gets attacked with extremely malicious code, fortunately Jeff Starr wrote a simple script that checks for excessively long request strings (i.e., greater than 255 characters), as well as the presence of either eval(or base64 in the request URI.

WordPress File Monitor Plugin

This plugin monitors your WordPress installation for any added/deleted/changed files. When a change is detected an email alert is sent out to you.



WordPress File Monitor: Alert (http://www.clientswebsite.com)

WordPress File Monitor to sigr show details Aug 6 (4 days ago)

This email is to alert you of the following changes to the file system of your website at http://www.clientswebsite.com
Timestamp: Fri, 06 Aug 2010 05:08:52 +0000

Changed:
index.php

The reason why this is so important is that if a site does get hacked, it will help you get to the bottom of which file caused it, which will help you prevent an attack in the future. You don't want to be left in a situation, where you have fixed the site, but don't know how it happened.

Change The User Name To Be Anything But Admin

Such a obvious step, but one that hardly anyone things about. Make this part of your setup process.

Secure Passwords For WordPress, FTP and MYSQL

This seems so obvious, but as mentioned above, weak passwords are the most common way for sites to get hacked. Try and use alphanumeric passwords. If you don't have 1Password or Roboform, then checkout http://goodpassword.com

Change Database Prefix

Most hacks target the database, so one of the most important steps you can take is to change the database prefix. We we first learnt about this we were a bit put off by the perceived complexity of doing something like this, but now we use the brilliant plugin BuddyBackup, which we will explain in more detail in the next section.

Extra Steps

These are some extra steps which our research turned up, but not steps that we actually take.

Move The wp-config.php File

WordPress 2.6 added the ability to move the wp-config.php one directory above your WordPress root.

If WordPress is located here:

public_html/wordpress/wp-config.php

You can move your wp-config.php file to:

public_html/wp-config.php

Wordpress automatically checks the parent directory if the wp-config.php file is not found in the root directory.

Remove WordPress Version From Header

If you are not using a custom theme which has already removed the WordPress version, then it is probably not a good idea to advertise to hackers that you are using a older version of WordPress.

In the header.php file remove the following line:

```
<meta name="generator" content="WordPress <?php bloginfo('version');?
>"" /><!-- leave this for stats -->
```

The wp_head function also includes the WP version in your header. To remove it, add this line of code in your functions.php

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

Limit Access To wp-admin by IP Address

Create a .htaccess file inside your wp-admin directory. Then add the following code:

```
AuthUserFile /dev/null
AuthGroupFile /dev/null
AuthName "Access Control"
AuthType Basic
order deny,allow
deny from all
#IP address to Whitelist
allow from 67.123.83.59
```

This will allow on the user with the IP 67.123.83.59 to get access to wp-admin.

More Preventative Measure Reading

You can of course go into a lot more detail and make WordPress more secure. If you are interested in learning more on about this subject we recommend the following excellent articles:

- Hardening WordPress
- WordPress Security Lockdown
- 20 Steps to a Flexible and Secure WordPress Installation

What If A Site Does Get Hacked?

The more professionally you handle the situation, the better it will reflect on your business. You really don't want to appear out of your depth here, so make sure you have at least done some background reading, so you can clearly articulate a plan for your client, if the hosting company has not already provided one.

We recommend the following articles:

- How to prevent your website from getting hacked and repair damaged sites
- How to Fix Your WordPress Site If It Gets Hacked

Backup Your Clients Sites - Simply!

If your clients site does get hacked, do you have a backup of their site to get them up and running quickly?

There really is no excuse not to, it is such an easy thing to set up.

You need to be proactive, and build a backup procedure into your development checklist.

BackupBuddy - A Simply Brilliant Plugin

We use BackupBuddy to handle the back ups for our clients sites. We came up with the following requirements, and BackupBuddy satisfied them all:

- Must be able to schedule backups.
- Must be able to automatically send file to our amazon S3 server (there is no point keeping the backups on the same server).
- Must be able to have database backups and full file backups (just incase everything gets whipped).
- The plugin must come with support.

We setup each clients site, so that there is a SQL backup at 3:00am each sunday morning, and a full site backup once a month. The backup gets forwarded onto our Amazon S3 server (because storage here costs virtually nothing).

All this can be done with a few clicks, and it gives us tremendous piece of mind to know that if the worst scenario does happen and a clients site goes down, we can get them up and running relatively quickly.

Why use BackupBuddy when there are other free plugins out there that do a similar thing? Support was important to us, but BackupBuddy has 2 features which make it pay for itself with each installation.

Migrating Your Development Sites Using BackupBuddy

One of the biggest pains in working with WordPress comes when you have to migrate your development site over to the live domain.

You have to install WordPress again and then all the plugins, themes etc. Then you have to get into phpmyadmin, export the sql file, do a search and replace on the domain name, and then import that sql etc, etc. In short, it is a real pain and can take quite a long time.

With BackupBuddy, deploying to a live site is as easy as a few clicks. It is a really simple process:

- We take a full backup of the development site - This means BackupBuddy basically zips up all the files we are using including the sql file.
- We then setup a empty database on the live site.
- Upload the zip file, and importbuddy.php to the live site, and within a few clicks everything is up a running.

A process that used to take 45 mins now only takes about 5, and we have vastly reduced the changes of making a mistake inside the SQL file. It really is a breeze!

The other reason we really like BackupBuddy is that during the installation process of a live site, it gives you the opportunity to change the database prefix, which as we point out, is a very important step in making your clients site more secure.

BackupBuddy costs $150 for a developers license. There are single licenses available, but if you are looking to run a serious business, you need the developers license which is an absolute bargain. The migration part of it makes the plugin pay for itself in the amount of time we save on each deployment.

The plugin gets updated frequently and has a good support forum.

BackupBuddy
All-In-One WordPress backup for your blog, widgets and plugins! All at once!
BACKUP BUDDY
Backup
Restore
Migration
PluginBuddy

Visit The BackupBuddy Website

WordPress Security Interview With Quintin Russ

Quintin Russ recently gave a talk about WordPress security at WordCamp New Zealand. Quintin has carved out his own niche in the New Zealand hosting industry, having spent a large proportion of the last few years becoming an expert in both building and defending systems. Quintin works at Sitehost.

SiteHost provides New Zealand web developers with professional-level hosting with Virtual Private Servers, dedicated servers and co-location.

He kindly took the time to sit down and talk to us about some of the finer points of WordPress security.

Can we start by asking what are the most common security mistakes people make?

The biggest mistake is that sites are quickly setup with the default username & password or weak passwords. Using weak passwords is a quick way of getting caught out.

There is a perception that WordPress sites are more vulnerable than other types of sites, would you agree?

No I would not agree with that. Wordpress sites that have kept up to date on their security updates are not the sites we see being compromised.

I would go as far as to say that some of the older e-commerce & content management sites. These tend to be not so well maintained and are a bigger problem these days which we certainly have seen evidence of.

In WordPress's case it is mostly weak usernames and passwords, out of date versions of software. There is also a large surface area for bugs in the wp-admin area of the site.

For example there are a small number of security bugs that I have seen that would give you admin access and these have existed in the wp-admin directory & did not require authentication to exploit.

You can protect yourself from these types of bugs by password protecting the entire wp-admin directory using basic or digest authentication for example with the very common web-server Apache. These are often configured through a .htaccess file under Apache.

Using standard, well vetted authentication mechanisms like the one apache provides via .htaccess is always a good idea. You can go a step further if you have a static IP address & know that you either only want to login from one location or a set of locations with IP addresses. By using two factor authentication, you'll further strengthen your Wordpress admin area.

What can you do to ensure you site is secure as possible ongoing?

I would recommend that every single person who is running a WordPress blog have a current copy of their files somewhere with the list of hashes for those files. If your not sure about the security of your blog, being able to go and run through the list of hashes and making sure that none of your files have changed is invaluable.

This is particularly important if you use custom plugins. You don't want to have to spend hours and hours pouring over your site just to verify its integrity or worse having to reinstall from scratch just to have the assurance that the site hasn't been compromised.

So what do you do if your site gets hacked?

When you get hacked, you want to make sure you've got backups. Make sure there’s a copy of the database and you have got everything you need to get the site back online.

You'll want to look online at support forums to see if other people are reporting similar issues & identify how the attacker got in to make those changes.

You may also want to look at Google webmaster tools. Google webmaster tools will let you know if they discover malware being hosted on your blog. [Log into webmaster tools > diagnostics > malware] if your not going to use that tool then certainly there are monitoring providers who will check the match of the content from your site, so they can check to make sure that your site has not been defaced or changed.

Monitoring is a key thing as well. Finding out as soon as possible before the attacker has time to do anything else to the system.

And is it the first thing from a developer's point of view? Do they pick up the phone and speak with their hosting company or do they try to sort it out of themselves?

Well it really depends on the level of service they are going to get from their hosting company.

And that maybe a consideration for developer's in choosing their hosting company as well as what sorts of service they can actually provide.

I think so. It will be certainly a good idea to contact them and say, "Hi, it looks like the site has been compromised?" Your provider may be seeing something more wide spread & be in a better position to offer advice on how the attacker got in. You also really need to know before signing up with them what sort of support they offer? If you are paying $10 a month for blog hosting ...

Don't expect too much from that hosting company...

Yes pretty much. It basically would have to be a widespread attack on a large number of customers before they are going to escalate it to the engineers.

So you need to do your research upfront on the hosting company?

Basically, it is up to you to understand what you think you will need from a hosting company. Most of your readers will be on shared hosting environment so making sure you have backups, talking to your hosting company and monitoring is a must.

Disclaimer

The information contained in this report contains the opinions of the author as of the date of this publication. Because the Internet moves at warp-speed, the author reserves the right to alter/update his opinion in the future.

This report has been provided for informational purposes only. While every attempt has been made to ensure it's accuracy, neither the author nor his affiliates/partners assume any responsibility for errors, inaccuracies or omissions. After all, they're only human!

We recommend you seek the advice of a professional security expert, and we can not be held responsible from any security issues you may have with your site.

The author isn't a legal professional nor does he claim to be. If you need any legal, business or accounting advice, you should seek the guidance of a professional in your area.

While the information contained in this report has been proven to

work for the author, he makes no specific guarantees in regards to the outcome you'll experience. Why, you ask? Well, solid information is great and all, but it doesn't do any good if it just stays stuck in your head. In order for this information to work, you must take action!

Your level of success will largely depend on the time you devote to the information presented, and the amount of action you take. Since these factors will vary from individual to individual, we cannot guarantee your success, nor are we responsible for any of your actions.

Any pricing mentioned in this book was determined to be accurate at the time of release. However, we have no control over the third-party websites we may have mentioned, so be sure to review their offerings if you decide to do business with them.

WordPress ® and its related trademarks are registered trademarks of Automattic, Inc.

This report is not affiliated with or sponsored by Automattic, Inc. or the WordPress ® Open Source project.

Rights Notice

This report was created for owners of the “WordPress Manual Plugin”. Owners of the plugin are hereby given the right to use this content to their own benefit or to give away the report to their customers, subscriber list or anyone they think might benefit from it. You do not, however, have the right to sell this report or make changes to it.