

# **12 Ways to Protect Your WordPress Blog from Being Hacked**

# Table of Contents

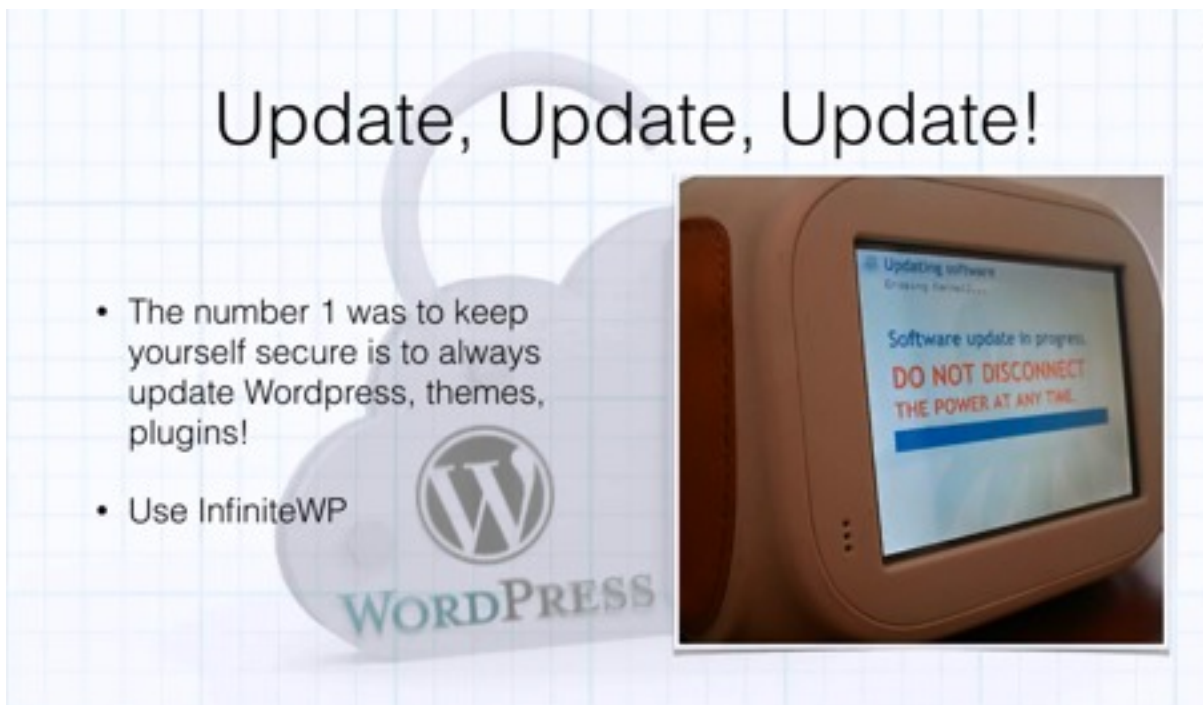
Introduction .....	3
Update, Update, Update! .....	4
Secure Passwords .....	9
Better WP Security .....	12
Brute-Force Attacks .....	15
Protect Against Malware .....	18
Spring Cleaning.....	21
Delete Your Backup Files Too! .....	23
Deleting the Default Admin User .....	25
Acunetix WP Security .....	27
Creating Backups.....	30
WP Security - Advanced Tactics Pt. 1 .....	33
WP Security – Advanced Tactics Pt. 2 .....	38

## Introduction



In this lesson you are going to learn how to keep your WordPress site safe. First of all, please take note that WordPress is a very secure platform in and of itself. However, it is open to vulnerabilities just like every other popular platform out there. So, you need to know how to keep your WordPress site secure yet accessible.

## Update, Update, Update!



One of the most important things that you can do is keep all your WordPress themes and plugins up to date. WordPress is very good about issuing new updates and keeping their installations up to date. This can make it difficult for you to keep everything up to date though. When they issue a new update, you'll need to install that update as soon as possible in order to close up any possible vulnerability.

A plug-in that will make things easier is InfiniteWP. Actually, this isn't really a plug-in because InfiniteWP runs on your server, not on your WordPress installation. InfiniteWP allows you to manage multiple sites, back them up, and keep them all up to date. The former is probably the best feature of InfiniteWP. When you use it, you'll be notified by email when one of your themes needs an update or when WordPress itself needs an update. InfiniteWP also has add-ons. One of the best add-ons available is the automatic backup feature. This will allow the program to automatically backup your site at whatever interval you prefer.

The last thing you want to see whenever you log into WordPress is a yellow bar up at the top telling you that you are out of date. Now, this isn't that big of a problem if you are only managing one site and you're checking on it every day. However, if you are managing multiple sites, these updates can take up a lot of your sites. InfiniteWP takes care of nearly everything for you, and it is completely free.

You can always sign up to receive email notifications from WordPress. Of course, you would have to sign up to get notifications from all of your plug-ins and themes too, and not every one of these is going to have a service like that available. That's another reason why it makes things easier to use InfiniteWP. Plus, it cuts down on the amount of emails that you have to review on a constant basis.

As previously mentioned, InfiniteWP does not run within WordPress. It is installed within a folder on your server and it runs inside its own database. Now, it does require a database to be set up on your site. If you're not comfortable with that, InfiniteWP will install everything for you for \$39, which is money well spent if you don't know what you are doing when it comes to running databases such as this. However, a tutorial is available that will walk you through every step of the process.

In order to download the program, you will need to visit InfiniteWP.com. When you get to the site, all you have to do is submit your email address and you will receive a download link via email which will allow you to download the program. The program will be delivered in the form of a zip file. You'll need to install this via FTP Client and into some folder. You may want to create a folder specifically for it beforehand.



Once you upload the program, you are going to be brought to the page shown above and you are going to be walked through the process of setting up the InfiniteWP Admin Panel. To begin, just click on the 'Agree & Install' button at the bottom of this page. The program is going to check and make sure that everything it requires is enabled. If you get all green checkmark symbols and no red checkmarks, you are good to go and you can click on the 'Continue' button to move forward.

Next, you are going to be directed to a page which will allow you to enter in your database and login details. The login details that you are going to enter in are going to be for InfiniteWP itself. For this, you'll just need to provide an email address and a password, and then you will need to confirm that password. The database details will need to be set up inside the cPanel of your hosting site. Setting this up is very easy, but again, if you don't feel comfortable doing so, you can have this done for you by requesting that it be done through the website.

If you log into your cPanel, you will find the option to run a 'MySQL Database Wizard'. Click on it and the setup wizard will open up. The first thing that you will be asked to do is name the database that you're trying to set up. After that, click 'Next Step' and you will be asked to set up a username and password for this database. For this, it is recommended that you use a randomly generated password.

Most cPanels will provide a password generator for you. In any case, your password should consist of uppercase, lowercase, and numerical characters. Be sure that you take note of what your password is because you will have to enter this password into the InfiniteWP panel and other places later on. Again, you'll want this password to be very secure because this password will give people access to your site. You definitely don't want to have any vulnerability there.

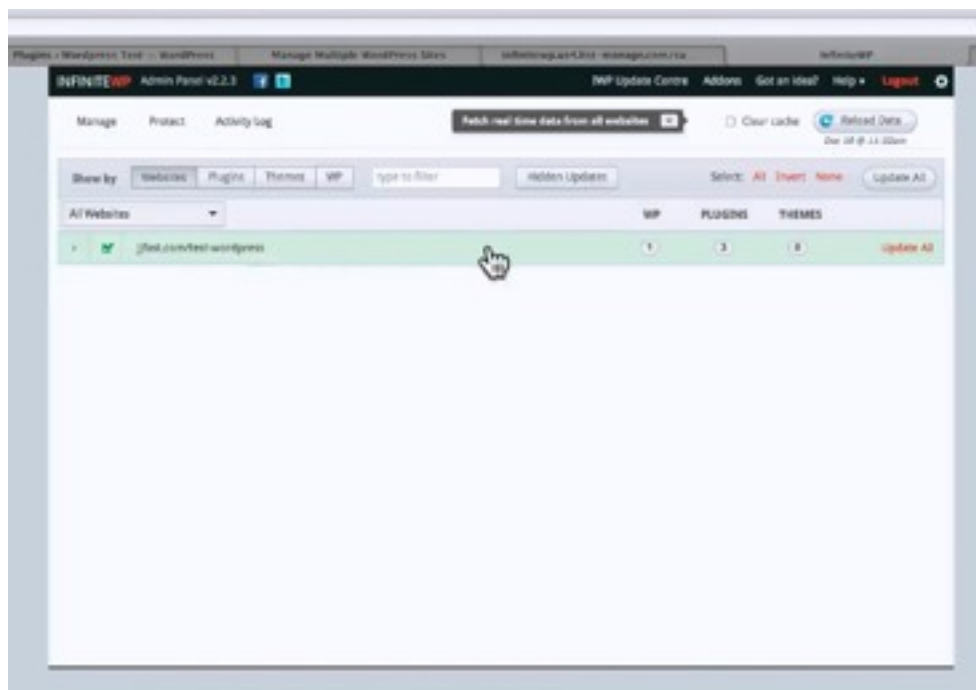
Next you will be given to the option to allow access to your database. This is what will allow InfiniteWP to have access, so you'll want to choose 'All Privileges' and then click 'Next Step'. Then, the final page should say that your setup is complete. So, now you can head back over to your InfiniteWP setup page in order to enter in your database details there. You'll need to enter this information into the following fields:

- DB Host
- DB Port
- DB Name
- DB Username
- DB Password

You will also be asked to enter in the 'DB Table Name Prefix'. You don't really need this information, so you can just leave this field blank. After you finish filling out all of these fields, simply click on the 'Install' button and the program will be installed. At this point, you could go ahead and click the login link at the bottom of the page. However, you also want to take note of the note at the bottom of the page that says 'For added security, delete or rename the 'Install' folder'. It is recommended that you do so. You're not going to need the installation folder again, and even if you do, you can always just download it again.

When you first get inside of your InfiniteWP panel, you are going to be asked whether or not you would like to take a tour. It is a smart idea to take this tour so that you know a little bit more about the program and how to get things done. Anyway, when you're finished with the tour, the next thing you are going to want to do is click on the 'Add Website' button. There are a couple of different ways to add your website. The easiest way to do so is to simply head over to your WordPress dashboard, click on 'Plugins', and then choose 'Add New'. The InfiniteWP plug-in is actually inside WordPress' plug-in database. So if you search for it, the 'InfiniteWP Client' will appear and you can install it.

Once you have it installed and activated, a yellow box will appear at the top of your dashboard. This box will contain all of the information that you need to enter into your InfiniteWP Admin Panel. So, return to your Admin Panel, enter this information in, and click 'Add Site' at the bottom of the 'Add a WordPress Site' window. The site that you add will then be listed within your admin panel and along with it you will see all of the aspects up your site that needs to be updated.



You can see in the picture above that this person's WordPress site is out of date, and he/she needs to update three plug-ins, but none of the themes for this site are out of date. Now, if this were your site you could update each of these individually, although there is the option to update everything all at once as well. You can do so by clicking on the 'Update All' button.

If you remember, you can also allow the program to send you email notification. You can set this up by clicking on the 'Account Settings' tab at the top of the screen. Now, you're going to have to set up a 'Cron Job' up on your website server as well. This is super-easy to do, and

there are a lot of tutorials out there on how to do this. YouTube is one of the best sites to look for one. Again, if you want InfiniteWP to set all this up for you, it costs \$39. Your hosting support can help you set this up as well.


This is the first recommended step for keeping your WordPress site secure. Whether or not you choose to use InfiniteWP is up to you. Surely you can see why it is recommended. It makes your life easier when it comes to the important process of keeping your site(s) up to date. The important thing is that you do so; otherwise you are leaving your site vulnerable. You can always do so the old-fashioned way, but the program being recommended here is free, so why not give it a try? Plus, InfiniteWP has a lot of other feature that haven't been touched upon yet like the backup features mentioned earlier in the lesson.



## Secure Passwords

S3CUR3 PA22W0RD2!

- Make sure all of your admin (and any other) passwords are secure
- They need a combination of uppercase letters, lowercase letters, numbers, and special characters (!\$#\*&-)



WORDPRESS

The easiest way a person can gain access to your WordPress site is through any of the passwords associated with that site. If you're using simple passwords like 'Password', your site is very, very vulnerable. If a person were to get access to a password related to your site, whether it is your FTP password, your admin panel password, or even your database password, then you are in trouble. Your WordPress site could be manipulated or completely gone.

Obviously, if you don't want this to happen to your site, you'll need to secure your passwords. There are a couple of different ways that you can do this. The first and most basic way to do this is to make up your own password. The problem is that when people do this, they use some kind of word or a combination of characters that we recognize. For example, if brownies are your favorite dessert, you might always use 'Brownies21' as your password. First of all, it's a big risk to use the same passwords over and over again. Secondly, in most attacks a computer is trying to guess your password, so if your password is in the dictionary, the likelihood that it will be guessed is a lot higher.

A secure password will consist of a combination of uppercased letters, lowercased letters, numbers, and special characters. The following symbols represent special characters: !\$#\*&-. It is always best to use a randomly generated password. A really secure password is going to be at least eight characters in length. Some people use passwords that are 15, 21, or even 46

characters long. In most cases you can have as long of a password as you like, so it really just depends on how secure you want your site to be.

A randomly generated password isn't going to make sense to you at all at first because it's just going to be a random mixture of numbers, letters, and symbols. So, it might be hard for you to memorize, but it's also very hard to hack. That's why you want to use a password like this.



One of the best places online to find a password generator is [StrongPasswordGenerator.com](http://StrongPasswordGenerator.com). When you get to the site, all you have to do is choose a 'Password Length' from the dropdown menu at the top of the screen. A minimum of 15 is recommended by the site. You'll also want to check the box next to the word 'Punctuation' so that special characters will be included. Then simply click on the button labeled 'Generate strong password' and almost instantly a randomly generated password will appear beneath.

By the way, there are forms that don't allow you to use special character. If this is true for the site you intend on using the password on, simply uncheck the box next to 'Punctuation'. Most, if not all, of WordPress' forms are going to allow for special characters though. Either way, a randomly generated password would be extremely difficult to figure out whether you're a human or a computer.

The problem with passwords like this is that they are hard to memorize. So a lot of people who use these kinds of passwords also use a password manager. Password manager will not only generate passwords for you, they will also store them. There are a whole bunch of different password managers out there to choose from.

Most of password manager have an auto-fill feature, which means that when you go to a site, the password manager will automatically fill in the password for you. So, you really never have to know what your passwords are and you never really have to try to remember them. All you really have to do is remember the password to the password manager itself. Of course, you'll

want to make that password very secure; so you'll want to use a randomly generated password for your password program as well.

One great password manager you may want to use is 1Password. This program runs on a Mac and on Windows as well as iPhone, iPad, and Android devices. It also syncs your passwords to each one of these devices so that you always have your password wherever you go. It either does this via Dropbox, which is very secure, or it will sync via iCloud. You do have to have one or the other installed in order to use 1Password.

Another option you have is LastPass. This is a very popular password manager tool. It allows you to do the same thing as 1Password. The only real difference is that LastPass only syncs to its own servers. This doesn't make it any more or less secure; it just works a little differently.

RoboForm is another very popular option. This actually began as a form-filler. In other words, it would remember all of the information that you would typically fill out in forms online such as your name, address, and credit card information and then automatically fill out the majority the fields on future forms for you. Anyway, this is how RoboForm started and now it also stores and generates passwords.

There are a bunch of different option out there, but these are the three most popular. You are encouraged to try them out. Now, keep in mind that LastPass and 1Password are paid programs but Roboform is free. Well, for the most part it is free. There are some additional features that you can purchase, but it's completely up to you whether you do or not.

Now you have three different options for automatically generating and storing passwords. They also all have auto-fill features which will remember these passwords and insert them into the fields for you as well. Keep in mind that this can pose a problem if you ever forget the password for the service that you're using. So, you take some risk in not being able to access that service. That means that you have to figure out what your comfortable with as far as security goes because the longer your password is, the harder it is to access services.

A lot of services like Gmail, Dropbox, Evernote, and Facebook now have a two-step authentication process where they allow you to enter in your secure password, and they text you another password if it was entered into a computer that you have not used previously. There are a couple of services which run on WordPress and do the same thing. You will learn more about these further on in this training. No matter what you end up using, your first line of defense is securing your password.

# Better WP Security



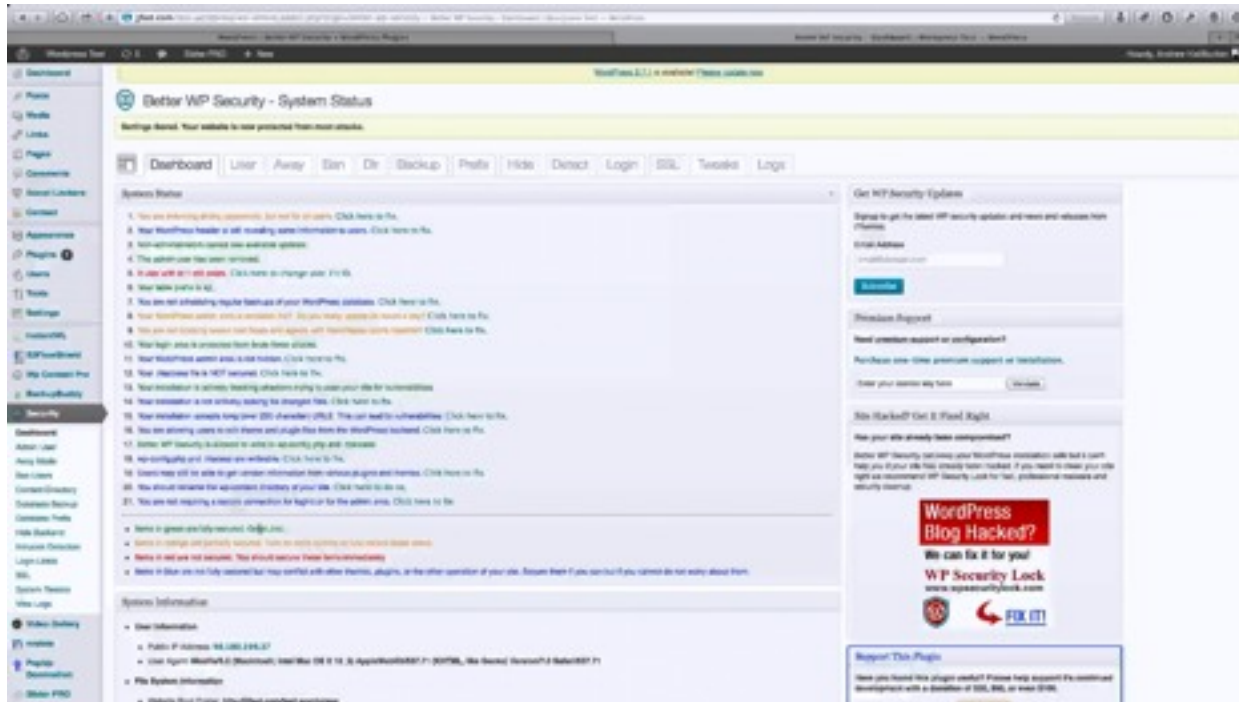
There is a really cool plug-in that you may want to try. It's called Better WP Security, and it has been called the 'Swiss Army Knife of WP Security'. It does a lot of things, but what's really killer about it is that it scans your entire WordPress and checks for vulnerabilities. It checks for weak passwords, it checks for hacking, and scanning on your site. It will also track 404 errors, which is a common way people can get access to your WordPress data.

This plug-in is absolutely free, and it's made by iThemes. You can get it inside the WordPress plug-in repository. By looking at the page above, you can see that it's currently the #1 WordPress security plug-in. This page provides an outline of all of its features.

Once you install the plug-in, you'll be directed to a 'Welcome' page. The first thing that you'll be asked to do is to create a database backup. There are other database backup options that you'll learn about later on in this series. However, you can use this backup as well. After the backup has been completed you will receive an email in the administrative email that you have set up.

This plug-in takes care of just about everything that you need taken care of. The next button that you will see will say 'Secure My Site From Basic Attacks'. So, it's going to run a basic check on all your plug-ins and all of your themes and make sure that all of the compatibility is there so that your site doesn't end up broken. Of course, this doesn't always work perfectly and that is why having a backup is always nice. When this scan is finished, the plug-in will provide you a

list of things concerning your site that need to be taken care of. This list is color coded that it is easy to tell which items are 'fully secured', 'partially secured', and 'not secured' as well as those that are 'not secured because they may interfere with other themes'.



Above you can see a status report for a test site. One item is showing in red, which means it's not secured. It says 'A user with id 1 still exists.' You see, when you install your WordPress database, you have an Admin User ID and a User ID of one. If you delete or rename that Admin User ID, that makes your site much more secure because the hacker has to guess the username and password to gain access to your site. The same thing goes for the regular User ID.

You may notice that there is also a 'Click Here' link that you can use to fix the problem. If you were to click on this link, you would be led to a page that would allow you to change the User ID. There is a button on this page that you can click and quickly fix the problem.

Another problem that this list shows is 'Enforcing strong passwords but not for all users'. That's because on this site strong passwords are only set up for administrators. So, the subscriber, the editor, and people like that currently don't have to have strong passwords. You can require this, but this is an example of where the security you set up can offset the usability of your site. Remember, most users don't use a strong password. Now, that's changing as more security issues are coming up in the news and other forms of media. However, you don't want to isolate people from visiting your site because they can't remember their password.

It is recommended that you require strong passwords of your administrators and your editors at least. You'll usually want to require this of your editors because they have the ability to edit

content, and you always want to require this of your administrators because they have complete access to your WordPress backend. That means that they can create new users, they can delete users, they can delete any content, and they can add new content. They could even take your entire site down if they wanted to. That's why you need to require your administrators to have strong passwords as well.

Not all of the items marked with orange have to be changed, but the ones in red need to. Another item that came up red was 'Your installation is not actively looking for changed files'. Once again there is a link to click to fix it. When you click on this link, there is a box that you can check which will 'Enable File Change Detection'. If you check this, you will be notified of any changes that may not be authorized.

Hopefully you can tell how helpful this is and how easy it is to set up. Plus, it catches all of these potential problems but it allows you to fix it because you may not want every option turned on. If you start to notice an attack, this program will help you to figure out what's going on as well.

Now you can click on each of the tabs within the page above and really bump up the security, but this would slow the site down big-time and that effects the usability of your site as well. So, if you find something that's a security risk, you can turn it on, but 99% of the time the biggest risks are going to be found under the 'Dashboard' tab.

## Brute-Force Attacks

In this portion of the lesson you are going to learn how to protect yourself from brute-force attacks. The term 'brute-force attack' refers to a scenario where a hacker uses a computer in an attempt to guess your password. The computer usually uses some kind of dictionary. So, it pulls in all of the words in the English language or other languages and tries each in one form or another until it gets in. This type of attack is pretty easy to prevent. All you really need is a secure password, but if you're not using one, the results can be pretty detrimental.

A randomly generated password is going to hold up to a brute-force attack a lot better than a regular password. However, just about every password can be hacked if enough time is given. So, if you really want to ensure control, it is best to use some kind of secondary means of protection.

One secondary step that you can take is to limit the number of times a person can attempt to log into your site. There is a WordPress plug-in that will do this. You can find it at <http://wordpress.org/plugins/limit-login-attempts>. This works pretty much the same way as a phone password does. If you were to enter the wrong password into your phone ten times in a row, it's going to lock you out. That's what the 'limit-login-attempts' plug-in does for your site. If you attempt to log into your site too many times, you are no longer going to be able to log in from that IP address for a certain amount of time. This protects your site from brute-force attacks because they only get 10 attempts to break your password before they get locked out.

Another option that you have is to use a captcha. You've probably seen these on websites before. A captcha is a graphic that contains letters, numbers, and sometimes even special characters. The point of a captcha is to prove that you are a human. As a human, you can see the graphic and type in the characters. A computer can't do that. A captcha usually is found below the username and password fields on a login page.

The cool thing about a captcha is that you can use it for a number of different things such as to prevent spam. For example, if you use a captcha on the contact form on your site, you increase the likelihood that a human is typing in that contact form, so you don't end up with a whole bunch of messages that have been sent from a computer. There is a captcha plug-in as well by visiting <http://wordpress.org/plugins/captcha>.



Both of these are very simple plug-ins. They each do one thing, but they do that one thing very well. In the screenshot above, you can see some of the features of the ‘limit login attempts’ plug-in. According to this page the plug-in does the following:

- Limits the number of retry attempts
- Limits the numbers of attempts to log in using auth cookies
- Informs the user about remaining retries or lockout time
- Optional logging and optional email notification
- Handles server behind reverse proxy
- Optionally whitelist IPs using filter

You can see that the primary feature of this plug-in is to limit the number of attempts for each IP address. You can customize how many times a user can try to login before they are locked out. You will also be able to receive an email when someone is locked out. So, let’s say that just a few people are managing your site and someone is continually trying to access the site. You will receive an email informing you of this. So, if someone is just having trouble accessing the site, this feature allows you to reach out to them.

You can also whitelist an IP address such as the IP address that you work from at your house. However, it is not recommended that you do so because people can either spoof your IP



address or they can get on your local network and gain access to your account. This isn't very likely, but it's a risk that you could be taking.

If you are using this plug-in and people fail to use the right username or password, the site will tell them how many login attempts they have left. This message doesn't inform the user of whether it was their username or password that was incorrect. After a person has used up all of the allowed attempts, the site will inform them of how long they have to wait before attempting to login again. So, if a user has just forgotten or lost their password, then they can try again after a certain amount of time has elapsed.

There is also a 'Lost your password' link at the bottom of the page that will help them to reset their password if they cannot remember it. Of course, a hacker would have to have access to this person's email address to reset their password. So, unless the person hacking the site has a great deal of information about the account's holder, it would be nearly impossible to get into their account. In this sort of case, a hacker is just going to give up because there are a lot of other sites that are much easier to hack into.

When you set this plug-in up, there are a number of settings that you can adjust and customize. On the 'Limit Login Attempts Settings' page, you can limit the allowed number of retries and the amount of time before they can attempt to login again. If they are locked out numerous times, you can set the user to be locked out for a number of hours. Again, this plug-in only really does one thing, but it will keep your site extremely more secure.

You can use the captcha plugin as well. Again, you can not only use this to increase security but to decrease spam as well. This particular captcha requires the user to answer a simple math question, which is a little bit different than most. However, it still ensures that it is a computer answering this question. The captcha will also be used on password reset pages and contact forms as well. Again, this ensures that the person contacting you is indeed human.

This is a simple plug-in to install. It has a couple of configurable features. The arithmetic capture feature is really cool. It's something that is not seen a lot, but it is very, very effective. In fact, it is often more effective and easier to use than the image captcha because a lot of times the image is obscured in some way which prevents a user from being able to read it.

Now you know a few ways to protect your site from a brute-force attack. The first step, as always, is to use a secure password. However, if your site will be much more secure if you limit your login attempts and use a captcha. You don't have to use all three of these techniques, but if you do you are that much more secure. These are 'set and forget' types of plug-ins, meaning that once you install them, they will continue working on their own and all you have to do is keep them updated.

## Protect Against Malware

Malware can be very damaging to a site just like it is to a computer. Any sort of malware can take your entire site down and you can lose all of your information. However, in a lot of cases malware affecting a site can be much more damaging because it can cost you to lose sales and cause your Google ranking to plummet.

There are a couple of different ways that your site can be affected by malware. Most of the time people get malware on their site by selling a host with someone else. For instance, let's say that you were on a VPS shared hosting plan. This is usually a cheaper option, but if one of the other sites gets hacked, malware can find its way onto your site. There are other ways too. For instance, your site could get hacked or you can download a plug-in that isn't what it says that it is. The same thing goes with themes and other downloadable items.

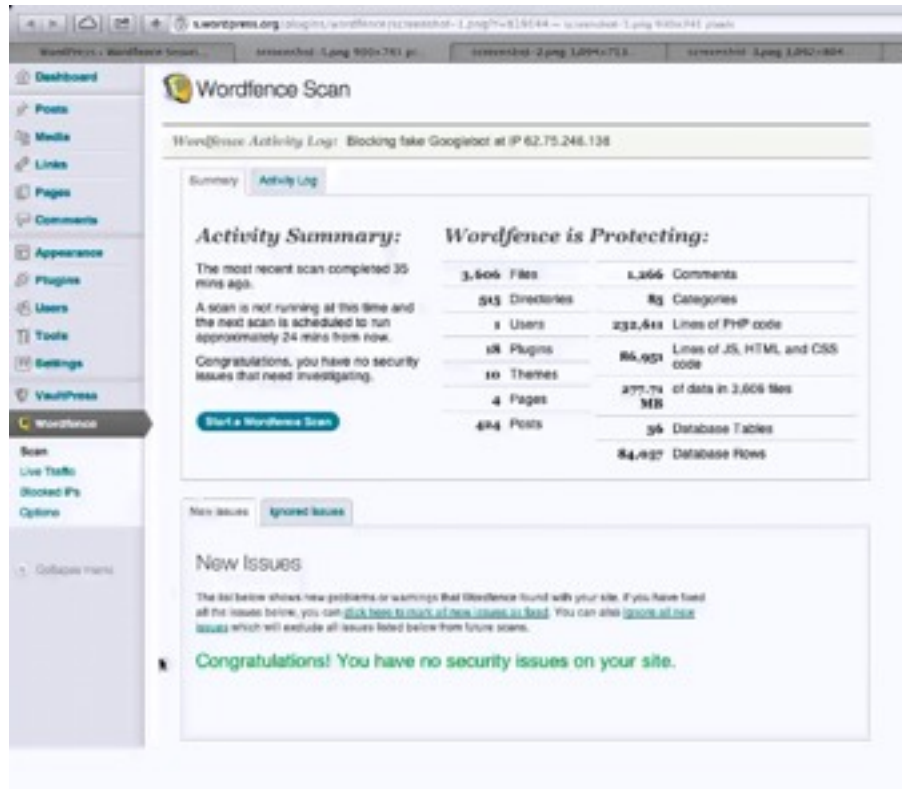
Again, the malware cannot only take your entire site down; it can also spread to all of the other sites using the same host. There are a couple of different ways that you can prevent malware. The first all, all the security options that are covered within this training series will help you prevent malware. However, there are even more proactive choices out there.

Just like running virus protection software on your computer, you need to run some sort of malware protection on your site. The best malware protection currently out there for a WordPress site is Wordfence Security. This is a free plug-in that will actively scanning every bit of traffic that goes into your site identifying any potential threats. It also even uses a two-step authorization process to help protect your site.

Wordfence also gives you the option to fix the problems that it finds on your website. Hopefully, you never have any problems with Malware, and you really shouldn't if you follow the steps being provided herein. If you ever do, this feature is super-valuable.

Wordfence can be found within the WordPress repository just like all of the other plug-ins provided herein. Before downloading it you can review its features, and you will see that on its most basic level it works as a firewall and an anti-virus program no different than one that you would use on your computer at home. It also allows you to implement a two-step identification process. Plus, it scans your live traffic for malicious URLs and bad crawlers. Then, as stated above, it allows you to easily fix any problems that it finds.

Once you download this plug-in and apply it, it will ask you to perform a full Wordfence scan. After you click the button to do so, it will begin to scan every file and folder related to your site. From that point on, it continuously scans the live traffic and everything else that comes through your site, just like a virus protection program on your computer would.



One of the coolest features of this plug-in is that it shows live activity. In the screenshot above, for example, it shows that the program is showing that it is blocking a fake Googlebot. It even shows you the IP address. Below this the live traffic on the site is also shown, whether human or otherwise. If you run across potential problems, the program also allows you to block certain IP address, and it will block some for you automatically as well. Plus, it even throttles certain crawlers if they access the site too frequently. In addition to making your site safer, this will prevent those crawlers from taking up your site's bandwidth.

In addition to everything else, you can set this program up to notify you of any issues via email. If this is something that you like, but you are worried about receiving too many emails, don't worry. You can customize the settings as to which types of alerts you would like to receive so that you are not overrun with emails. Other things that you can customize through your admin panel include:

- Live Traffic View
- Scans to Include
- Firewall Rules
- Login Security Options
- Other Options

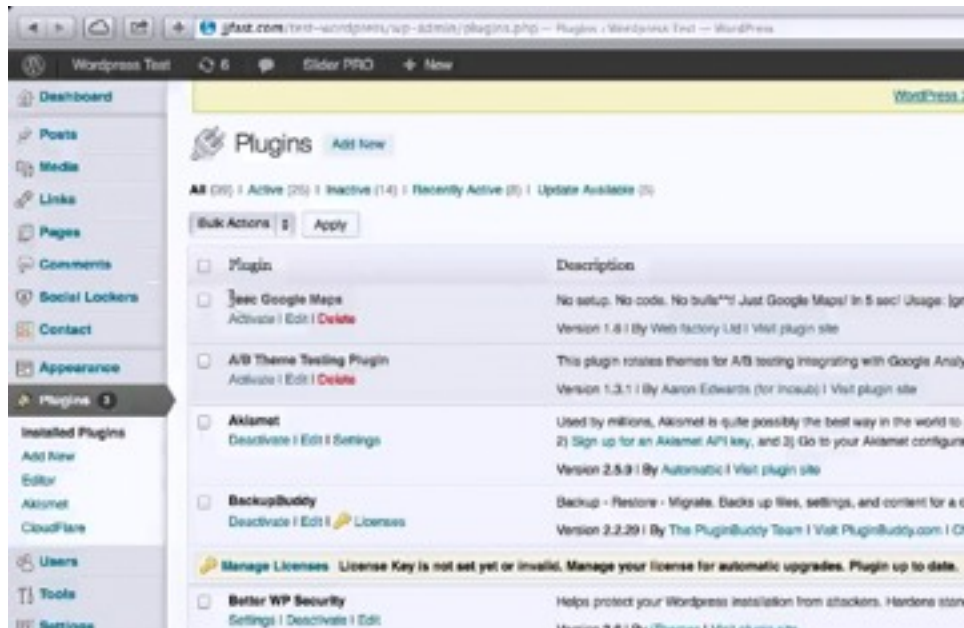
You are likely to be impressed by the 'Firewall Rules' to be found here. For example, if anyone's requests exceed 960 pages per minute the attempt will be throttled. Also, if a human's page view exceeds 120 page views per minute, then this IP will be blocked because, obviously, no one can view pages per second. Whether the tool should 'block' or 'throttle' these users can be manually set as well.

Another option that you have is to set up an extra security step to your page by allowing it to send a text message to a user with a special password if they are attempting to login from a different computer than usual. This is yet another option that you can use to make your site even safer. So, take a little time to explore these options when you are setting this up.

This is one of those programs that continuously learning and sourcing information from different sites. So, if the program detects a new sort of attack on one of the sites that is protecting, it applies that new-found knowledge to each site that it provides in order to block future attacks. This is honestly one of the best security programs out there.

Again, malware is a very real threat, and you can experience huge problems if your site is infected. That's why it's always a good idea to back everything up and install some sort of malware protection software. The Wordfence program is going to do this for you automatically and often live. Go ahead and check the repository for it and check out its features. You are likely to be pleased; currently the majority of its users are.

## Spring Cleaning



Logic says that if you have less stuff on your site then you will have less security holes as well. So, every once and a while you are going to want to go through your sites and simplify them as much as possible. This, of course, applies to your WordPress database as well.

Many people install a lot of different themes, plug-ins, pictures, and other types of files whenever they set up a site, but once they get everything nailed down, they never really delete any of it. It's important that every once in a while you go through this spring cleaning process and get rid of everything that isn't necessary and things that are never used.

There are options for deleting various plug-ins and themes inside your WordPress dashboard. You can see a list of various plug-ins within the screenshot above. You can get to this page by clicking on 'Plugins' and then 'Installed Plugins'. Under each of the plug-ins, there is a link that either says 'Activate' or 'Deactivate'. You have to 'Deactivate' a plug-in before you can delete it. If you click on a 'Deactivate' link, the option will appear to 'Delete' it. When you click on the 'Delete' link, you will be redirected to a new page where you can click a button to delete the chosen plug-in.

Go through this list attentively and search for any plug-ins that you and your site's users could possibly live without. When you find one, deactivate it and delete it. This will help your site to be much easier to handle, and therefore, a lot safer. It is recommended that you make a backup for your site before going through and deleting anything because there may be a plug-in that you don't realize that you use and things like that.

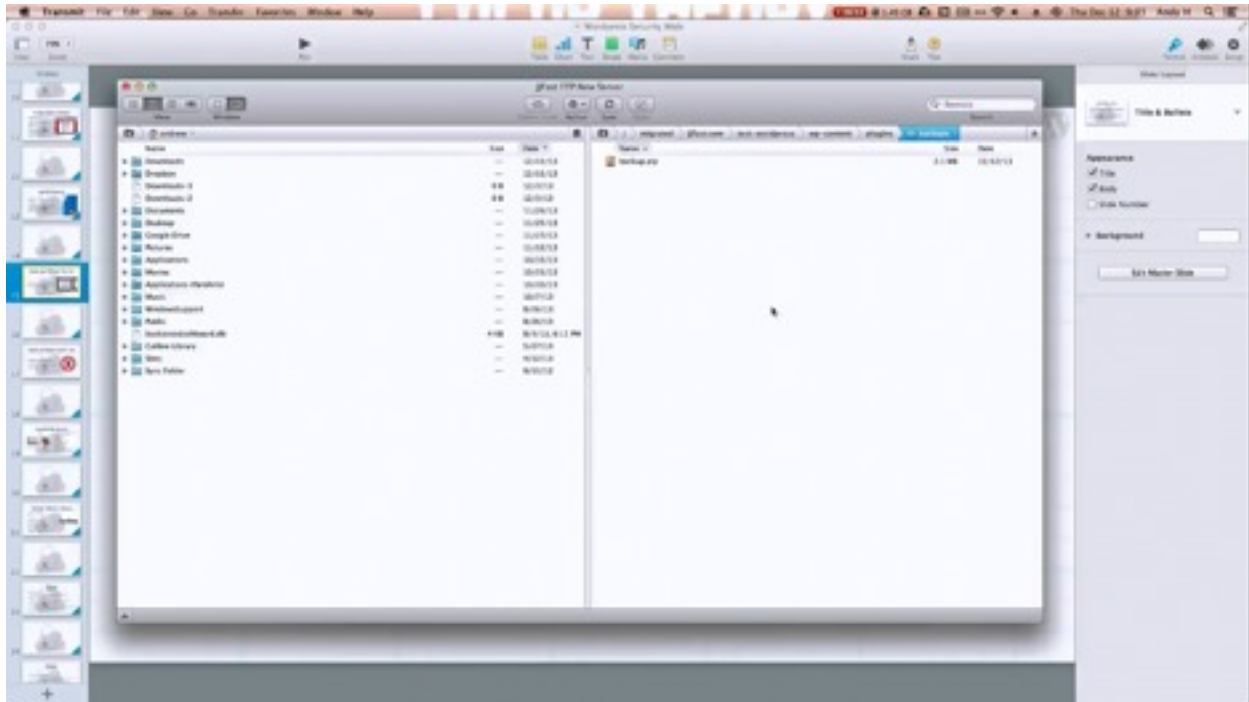
If you want to be super-safe, you can also make a backup every time you delete a plug-in or a theme. As you delete various themes and plug-ins from your site, you also want to test it. The themes can be deleted in the exact same way as the plug-ins are by the way. You will find a list of themes being used by your site when you click on 'Appearance' followed by 'Themes'. Simply click the link to deactivate them and then to delete them.

After you are done sifting through and deleting your themes and plug-ins, click on 'Media' and you will find a list of videos and pictures. You may want to start at the oldest pictures and work your way back since those are the most likely to be chosen for deletion. Another thing that you might want to do is click the 'Unattached' link at the top of the page. This will bring up images that are uploaded but not actually attached to any page. Getting rid of these excess files is also going to make your site run much faster.

You should go through and delete your old pages and posts as well. You can find a list of these by clicking on 'Page' and/or 'Posts' within the side panel of your dashboard. When you do a list of them will appear. If you want to delete one, simply hover over it and click on the 'Trash' button that appears. Don't forget that you will need to click on the 'Trash' link at the top of the page in order to delete these items permanently.

Again, this process is very important. Each file on a site can potentially be compromised, so the less files you include, the less of a risk you take. This will also make your site cleaner and more attractive visually, and it will make your site run a little faster.

## Delete Your Backup Files Too!



Deleting your backup files is an important part of keeping your site cleaner and more manageable, but it's something that a lot of people often overlook. However, did you know that keeping those backup files is a huge security risk? If you do need to keep a backup file, then you should keep it in Dropbox, Amazon S3, or another separate server. That way, if your site gets hacked, your backup files are isolated separately.

There are a couple of different ways that you can go about deleting these files if you choose to do so. One way is to use an FTP client to get into your server and delete the files that way. Another thing that you can do is use an automated backup system and they can delete the backup for you.

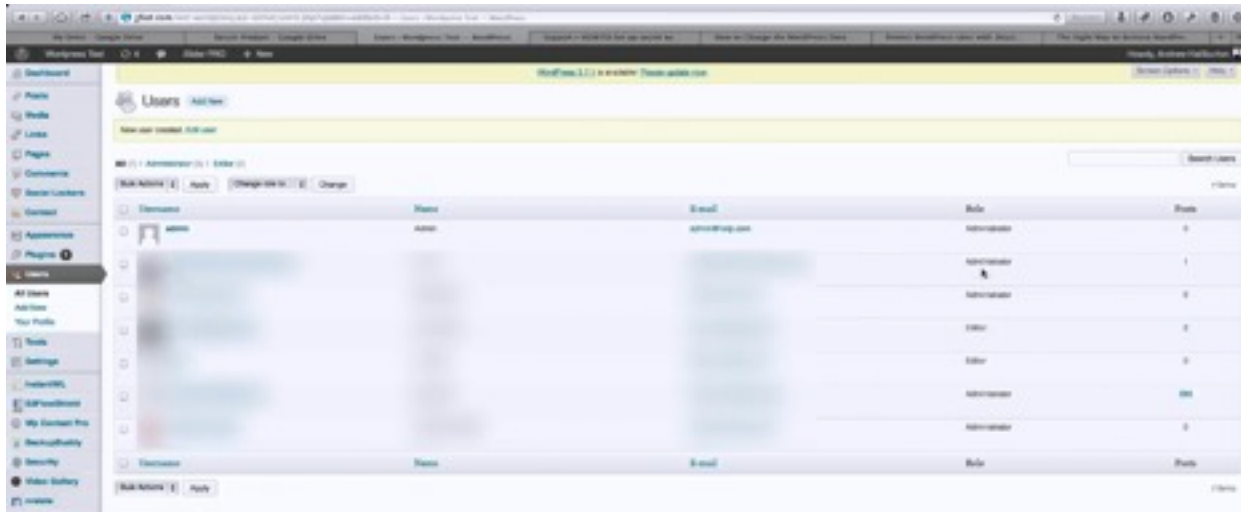
Above, you can see a screenshot of the inside of an FTP server. This server is called Transmit, but you can use any sort of FTP client; there are a lot of different ones to choose from. If you're looking for a free option, Filezilla is a good choice. It runs on both Mac and Windows. Cyberduck also runs on both Mac and Windows, and it's free as well.

Anyway, in Transmit all you have to do is select your backup file and hit the 'Delete' key on your keyboard or right-click on the file and choose 'Delete'. The same should be the same stand for most other programs. Again, it is best that you have these files stored on a separate server prior to deleting them. After all, you never know what you may need in the future. You can

always store it on a secure hard drive of your own or you can upload it to a server such as Google Drive or Dropbox.



## Deleting the Default Admin User



In order to make your site more secure, you should delete the default 'Admin' user or at least change it. You can change it to your email address or your name. If you want to go the extra mile, you can change it to something that no one would be able to guess by using a mixture of numbers, digits, etc. Of course, if you do delete the default admin account, you'll want to do this after you have created a new admin user. In other words, don't delete your admin account without creating a new one.

You should also take the time to delete all of the users that don't need access to your site anymore. Let's say that you hired someone to code a theme, for instance, and they needed admin access to perform the task. Once the job is done this person isn't going to need admin access anymore, so you can go ahead and delete them.

A lot of people don't delete accounts such as these because they think that the person they have hired might need access to the site in the future. In cases like this you can simply change the password so that they can't get in, and if they ever need to again, they can just ask you to grant them access again.

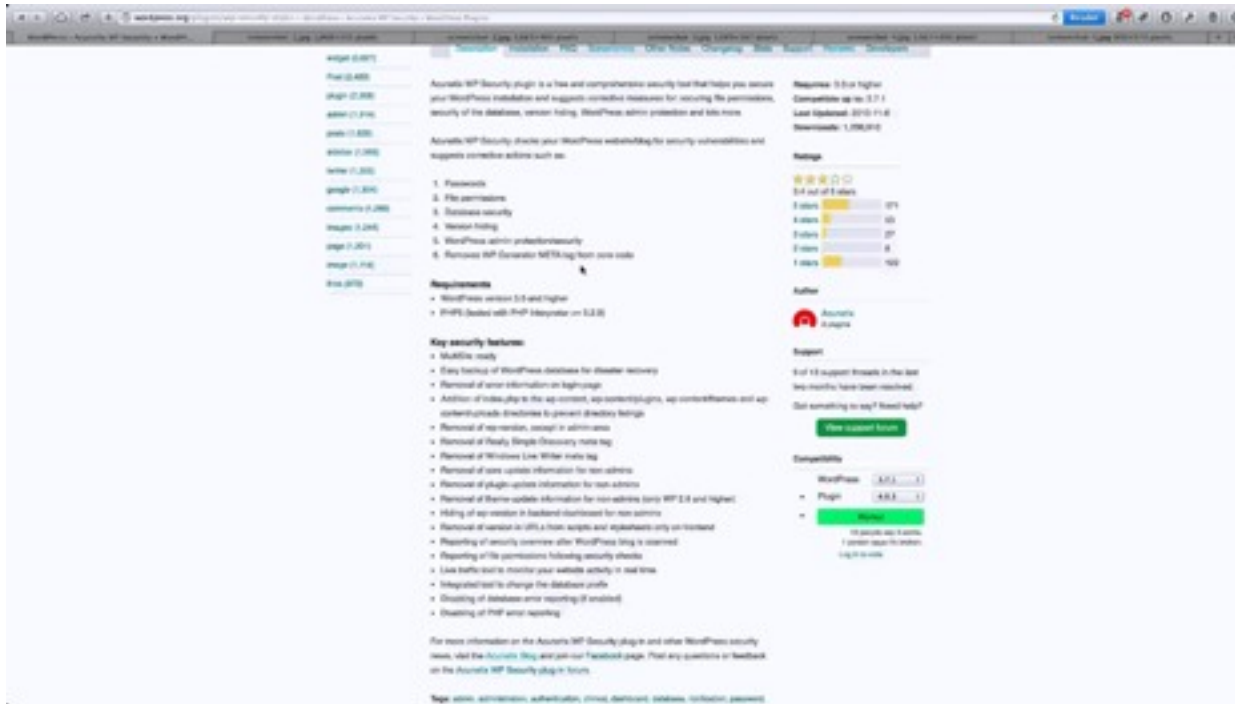
It is actually pretty easy to delete an admin account from your WordPress dashboard. To do so, simply click on 'Users' and the page above will be shown. On this page, all of the administrators will be listed as well as others who have access to the site. Simply hover over the account that you want to delete and a 'Delete' link will appear beneath.

You can also click 'Edit' to change the email address that's used to log in. The only problem is that you can never change the username. So, it's usually easier just to create a new user and then delete the old one. If there are any posts within the original account, the site will ask you which site to direct these to, and you can just choose the new account.

If you want to create a new user, simply click on the 'Add New' link at the top of the page. When you do, the page will redirect and you will have a number of fields to fill out. Again, when you set this up you will want to make sure and use a strong and secure password. Once you have this new admin account created, you can simply go back to the 'Users' screen and click on the 'Delete' link beneath the previous account. The site will then ask you where you want the posts for this account to go from here on out. Make your selection and then click the 'Confirm Deletion' button below.

After you have replaced the default admin account with another one, your site will be much more secure because now a hacker would have to guess your username as well as your password. They can no longer use the normal admin username. As you can probably tell, this isn't something that is very hard to do. It will make your site much more secure though.

# Acunetix WP Security



Acunetix WP Security is yet another plug-in that you can find in the WordPress plug-in directory. This plug-in is very similar to the Wordfence plug-in earlier discussed, but there are some major differences between the two. For example, Acunetix scans for weak passwords, incorrect file permissions, and poor database security. This plug-in will also hide your version as well as protect and hide your admin area. This plug-in allows you to hide certain things from certain types of users as well. For the most part, however, this plug-in protects a site from malware in much the same way that Wordfence does. This one just takes things a little bit further.

In other words, this plug-in protects your admin panel from certain people who have access to your site. So, let's say that you were giving out site credentials to freelance workers who are doing something for you. This is a great plug-in to have in that scenario because it's going to allow you to protect the backend of your site as well as the frontend.

Acunetix WP Security is also going to make sure that all of your passwords are strong and things like that. Several of the other plug-ins introduced in this lesson let you do that but this one will also correct file permissions. This is a great way to find out if someone has access to your site who shouldn't. Also, it will prevent people who shouldn't have access from gaining it.

If you would like to download this plug-in, it is located at <http://wordpress.org/plugins/wp-security-scan>. A screenshot of this page is provided above. As you can see, tons of features are

listed within this page. Obviously, WordFence had some that Acunetix doesn't. It really all comes down to what interface and features you prefer.

This program will allow you to remove an incorrect password or username from a login page. It will also have an 'Index.php' to prevent directory listings, which hides the fact that you're using WordPress if someone gets FTP access to your site. So, that's yet another level of protection. It also allows you to hide the version of WordPress that you're using, which will hide vulnerabilities as well. You see versions of WordPress that are not up to date carry vulnerabilities. So, if people know what version you are using, then they know how to attack your site. This plug-in focuses a little more on protecting the admin panel than the previous one did. However, like the other plug-in, Acunetix does scan your live traffic to identify and prevent real time threats.

Again, this program will provide you with a 'File Scan Report'. A screenshot of this report is provided below. This particular report will tell you what the current permissions are and provide you with suggested permissions. For instance, your root directory may need '0755' permissions instead of the '0777' permissions that you currently have. If you don't know what that is, your host can help you to reset these.



The features that this program offers are all customizable. As you choose which ones to implement, keep in mind that you need to balance the site's security with its usability. For instance, this tool will allow you to turn your RSS feed off in order to make your site more secure. However, this RSS feed may be the major reason why people visit your site. So, by turning the feed off, you may have been able to make your site more secure but now you have fewer visitors. On the other hand, if you're selling things on your site that you only want members to have access to, then disabling RSS data may be vital.

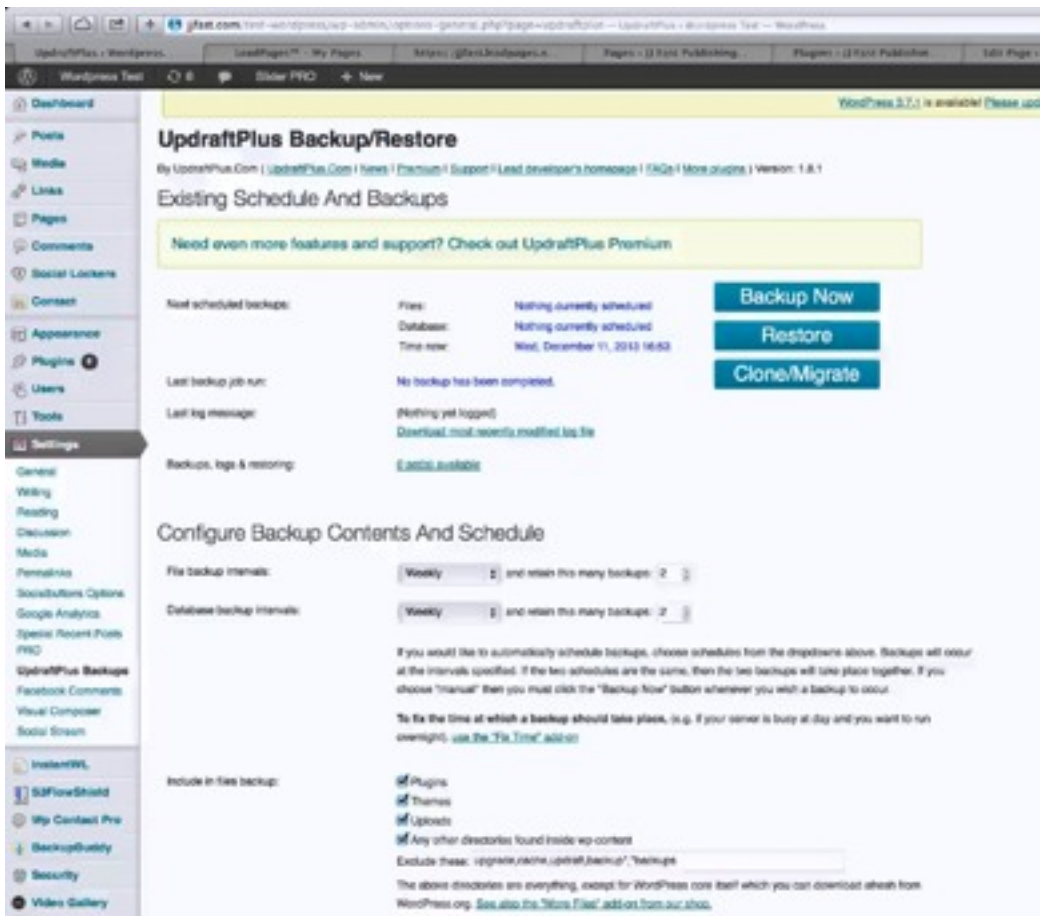
Another feature that this plug-in has in common with Wordfence is its ability to monitor live activity. It will also block any activity that could potentially cause problems. This program will

inform you of the different types of alerts, the status of all your files, and suggest solutions on how you can fix some of your site's security risks.

In addition to these automatic scans, you can perform a manual site scan to see if any changes have been made to your WordPress core files within a time span that you have specified. If you don't often edit your theme files or plug-in files, but you see that changes have been made, then you will know that your site has been compromised. You see, a lot of hackers will input things into your themes or your plug-ins that monitor your site and things like that. So, it's important to know if any modifications have been made, and this manual scan will let you know that.

To reiterate, Acunetix WP Security is very similar to WordFence. However, they each kind of take two different approaches to providing security. Acunetix protect against both external and internal users, and it allows you to scan for weak passwords, provides database security, and things like that. WordFence, on the other hand, does a really good job of monitoring your live traffic. They also provide that secondary identification step and crowd-sourced security, both of which Acunetix does not do.

## Creating Backups



We've already looked at a number of different options for backing up your site. It was previously stated that Infinite WP helps you to keep your site updated and allows you to control those updates, but it also helps you to backup your files. Then, you can download those and save them on your hard drive or store them to Dropbox, Amazon S3, etc. We have also looked at two security plug-ins, both of which allow you to back up your files as well. However, there are also plug-ins specifically designed to help you backup your files. One of the best plug-ins out there for this is 'UpdraftPlus'.

If you like to back up your files using sites like Dropbox or Amazon S3, then this plug-in would be great for you because it allows you to do so quickly and easily. This plug-in automatically generates backups and automatically uploads them to the server of your choice. You can also use an FTP account and even email if the backup is small enough. Again, it's a security risk to have your backups stored on your own server. So, it's super powerful to have those backups sent to a secure location automatically.

This is a 'set and forget' type of plug-in. You simply specify how often you want it to backup your files, and it's done. You will even receive an email if there's ever an issue, and you can also set this plug-in up to inform you every time a backup is created.

Above you can see the setup page for this plug-in. Once of the things that you may notice first are the three buttons at the top-right of the page. As you can see, this plug-in allows you to backup, restore, and even clone/migrate your site. Underneath these basic settings are the settings to configure the contents of your backup and schedule your backups. You can set this plug-in to automatically backup your site at different intervals or you can do so manually yourself.

It is recommended that you backup most of your files each month, especially if you don't create a lot of content-driven sites that aren't updated on a daily basis. If your sites are updated on a daily basis, you might want to have your databases and/or files updated on a daily basis. The 'File backup' option backs up your entire WordPress database. So, it backs up all of your media files, themes, plug-ins, etc. The 'Database backup', however, just backs up the data portions of WordPress; so, it backs up the text in your pages and things like that.

This page also allows you to set the number of backups that you want to retain. When you use services like Dropbox and Amazon S3, you have to pay for the amount of storage that you use. Therefore, you may want to limit the number of backups that you retain, especially the full backups. It is recommended that you only retain two of the file backups and four or five of database backups.

You are also given the option of which types of files to include in these backups. You should keep all of these options checked, and check the backup intervals so that they occur less frequently if you don't update your site a lot. You want to keep a backup of everything on your site. That way, if the worst-case scenario does occur and everything on your site disappears, you always have a backup somewhere else and you can easily restore your site. This is also very helpful if you need to clone your site or migrate it to a new hosting provider.

In the 'Reporting' section of this page, there is a box that you can check in order to receive a basic report about your backups sent to your site admin email address. This report will tell you how many successful backups have been made and inform you of any problems. This plug-in does a very good job of not bombarding you with a ton of information.

Next, you will see the settings which allow you to automatically copy your backups to a remote storage system such as Amazon S3, Google Drive, or Dropbox. You can choose the 'None' option, and the files will be uploaded to your own server. However, it really is much more secure for you to use one of these separate highly-secure servers. Of course, it is possible for you to even choose 'Email' if your back up files are small enough. If you do, be sure to use a very secure password for your email address.

If you don't have one of these secure services set up with, go ahead and set one up and then return to this page because there are a number of different access keys and things like that which you'll need before you can begin setting up your plug-in. All of these different options are going to have different configuration requirements. So, go ahead and choose the one that you think you would like to use in order to see what you need before heading over to the other site to create and account.

This is a very simple type of plug-in. It pretty much automates everything so that you don't really have to think about these types of things that often, yet it keeps you updated enough to keep you on top of things. If you would like to check out this plug-in for yourself, you can do so by visiting <http://wordpress.org/plugins/updraftplus>.



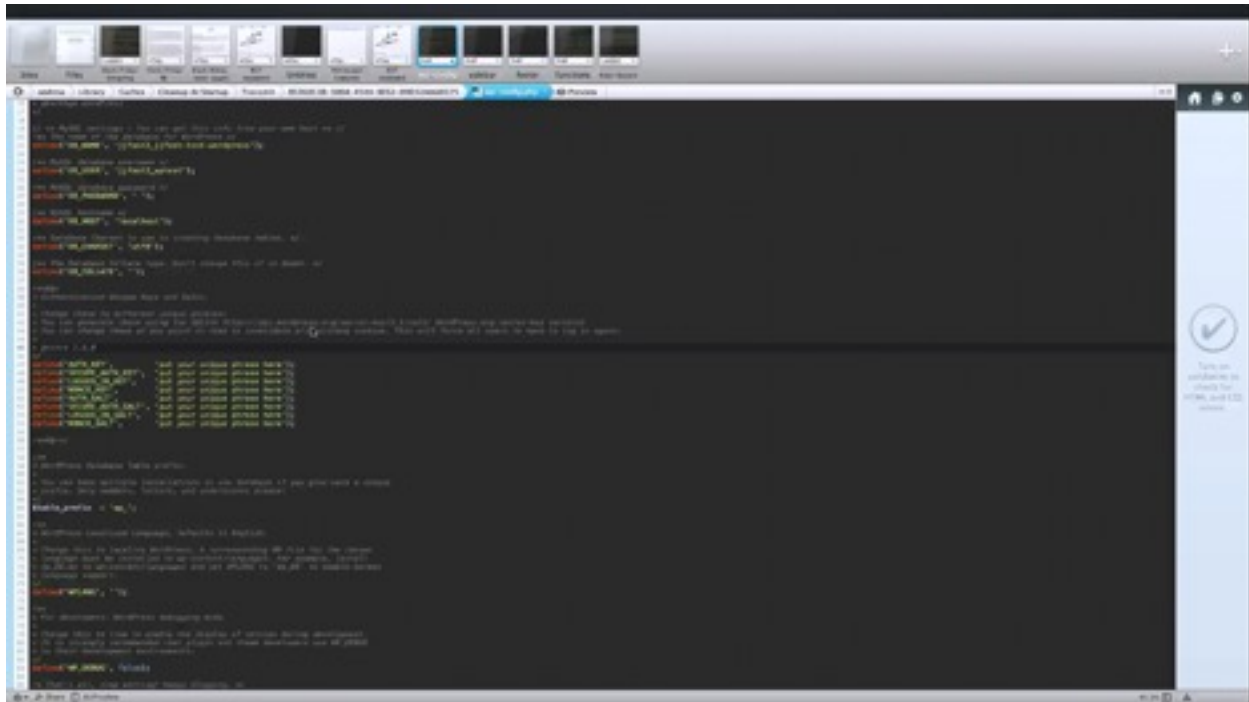
## WP Security - Advanced Tactics Pt. 1

In this portion of the lesson and the portion to follow, you are going to have the chance to learn about some very powerful advanced tactics that you can use for securing your WordPress site. If you feel comfortable editing your own database files, this section is for you. These tactics will allow you to secure your site without the need for added plug-ins.

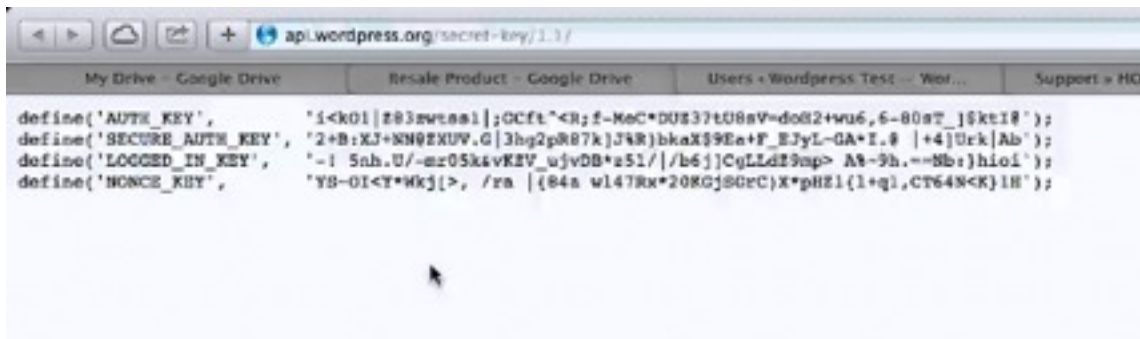
If you don't feel comfortable doing these sorts of things, then it's recommended that you shy away from this portion of the training. There are plenty of plug-ins that you can implement to keep your site secure. These are advanced tactics, so proceed at your own risk. You are going to learn how to edit theme files. Therefore, you want to make sure that you have a backup of everything before you begin.

One thing that you can do to help secure your WordPress site is to create secret keys for your 'WP-Config.php' file. This secures your cookies, essentially, making them harder for a hacker to reproduce them and gain access to your site. To do this, you will need to create four random phrases. Each should consist of about 60 characters or so, and they should consist of a mixture of uppercase, lowercase, and special characters. You can find more information about this process by visiting <http://wordpress.org/support/topic/set-up-a-secret-key-in-wordpress-25>. WordPress also has a 'Secret Key Generator' that you can use. You can access this at <http://api.wordpress.org/secret-key/1.1>.

To begin the process of generating these secret keys, go into your database and open up your installation folder. Within this folder, you will find a file titled 'WP-Config.php'. You'll want to download this file. In many cases you can edit this live on your server, but it is recommended that you still go ahead and download the file. That way, if you break something while making your changes, you can re-upload it and overwrite the changes that you've made.



Above you can see a screenshot showing what this file looks like opened up. It's going to look like a bunch of gibberish at first, but if you look at it a little more closely, you will find the database name as well as the username and password that are associated with it. In the center of the screenshot there is an orange and yellow block of text. This is where you secret keys are going to go. So you are going to paste a secret key at the end of each line where it says 'put your unique phrase here'. Again, it is recommended that each of these phrases is at least 60 characters long.



When you click to access the secret key generator, you will be brought to an empty page that has nothing more on it than a block of text on it. You can see this demonstrated above. These are the keys that have been generated for you. Simply copy and paste these four into the lines of code referred to above. You'll want to have four more, of course. You can simply retrieve more by refreshing the page.

As you can see, it's pretty easy to edit these custom keys and set that up to make your site more secure. However, feel free to skip over all of these steps if you don't feel comfortable messing with these codes. If you have never done this before but aren't afraid to try that's fine too, just be sure that you have backed your files up beforehand.

Another thing that you can do is change the 'database prefix'. Now, there are several different plug-ins that will do this for you. All you have to do is perform a Google search on the keywords 'change the database prefix' to find them. It only takes a moment to run the plug-in and make the change and you're done. It's really just as easy to make this change manually though.

```
/*
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/}
 * You can change these at any point in time to invalidate all existing cookies. This
 * will force all users to log in again, which is a good security measure.
 */
define( 'AUTH_KEY',         'put your unique phrase here' );
define( 'SECURE_AUTH_KEY', 'put your unique phrase here' );
define( 'LOGGED_IN_KEY',   'put your unique phrase here' );
define( 'NONCE_KEY',       'put your unique phrase here' );
define( 'AUTH_SALT',       'put your unique phrase here' );
define( 'SECURE_AUTH_SALT', 'put your unique phrase here' );
define( 'LOGGED_IN_SALT',  'put your unique phrase here' );
define( 'NONCE_SALT',      'put your unique phrase here' );

/*
 * WordPress Database Table prefix.
 *
 * You can have multiple installations in one database if you give each a unique
 * prefix. Only numbers, letters, and underscores please!
 */
$table_prefix = 'ap_';

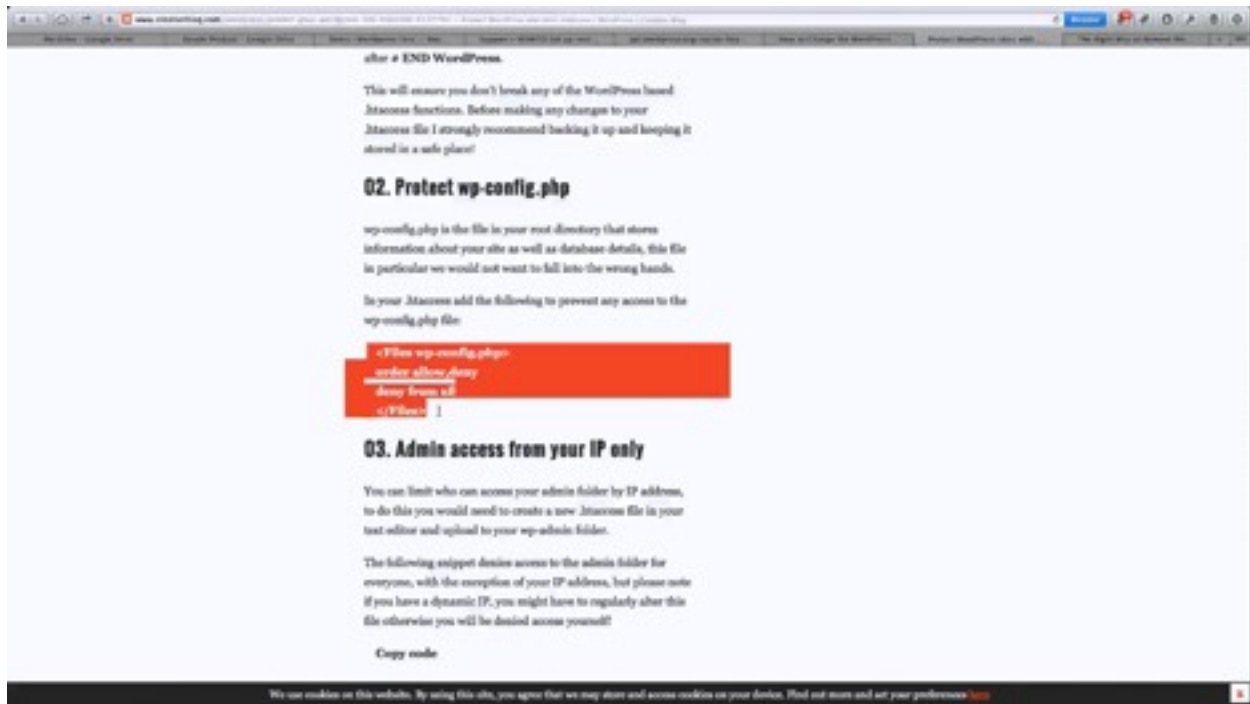
/*
 * WordPress Localized Language, defaults to English.
 *
 * Change this to localize WordPress. A corresponding MO file for the chosen
 * language must be installed to wp-content/languages. For example, install
 * de_DE.mo to wp-content/languages and set WPLANG to 'de_DE' to enable German
 * language support.
 */
define( 'WPLANG', '' );
```

You can make this change through your WP-Config file as well. If you look at the picture above, you can see that this accounts database prefix is currently set to 'ap\_'. Someone has already changed this database prefix to make his/her site more secure. You can change your prefix to anything you want, but take note that the instructions here ask that you use letters, numbers, and underscores only. It is also recommended that you always have an underscore at the end of the prefix. That just makes it a little bit easier to read if you ever need to.

There are other settings that can be changed but should not be changed inside of this WP-Config file. One thing that you can do is protect your WP-Config file through what's called an '.htaccess file'. If you don't have one of these files on your server then you're going to want to ask your host to put one on there. There are also a lot of tutorials on the web that will walk you through the process of setting up one of these files. It will probably take you about 30 minutes

or so to research that and get that file created, but again, you can also ask your host for help. Now, not all hosts support this but most do.

There are a whole lot of different security settings that you can set up through your .htaccess file. You can find some information on the various things that you can do by visiting <http://www.creativeblog.com/wordpress/protect-your-wordpress-site-htaccess-4122793>. The most important thing for you to protect is your WP-Config file, and there are instructions on how to do so on the webpage as well.



These instructions are shown in the screenshot above, and in the middle of this page you'll see a section of code. You just want to copy this code and paste it into your .htaccess file, and this will deny access to anyone that is trying to get into your WP-Config file. After doing this, you'll have to change your .htaccess file in order to access your WP-Config file to make any changes. So, essentially you are just adding another lock to your WP-Config file.

One of the other things that this page tells you how to do is allow admin access from your IP only. This one is kind of dangerous to implement though. That's because at times an ISP will change your IP address without your knowledge, but you can set this up if you want to. This page also provides instructions on how to ban bad users, and you can also add no directory browsing, which means that no one can see your FTP folder. There are a number of different ways that you can use this .htaccess files to make your site more secure, so check out the site above to learn more about them.

Finally, you can move your WP-Config to the main directory. This protects the file because it is no longer in the location that it would normally be found in. Just moving this file up one directory is going to make it much more difficult for anyone who gains access to your FTP folder to locate your file. At the very least it would take a hacker a little longer to try to find it.

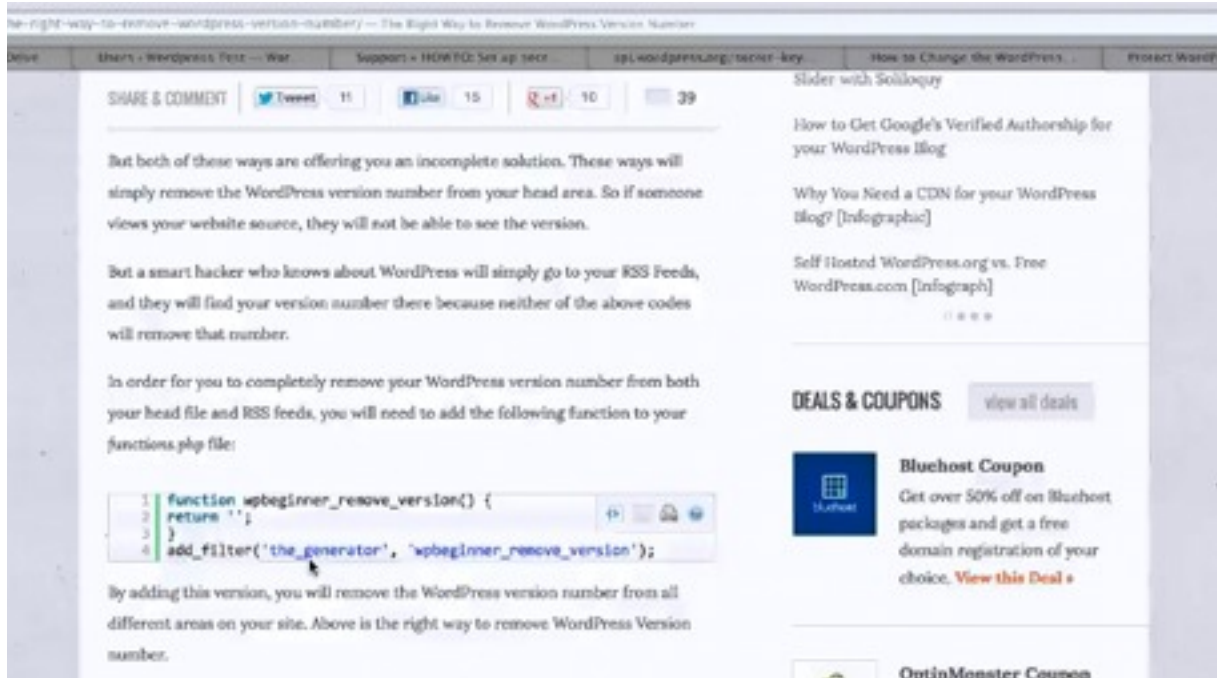
## WP Security – Advanced Tactics Pt. 2

In this portion of the lesson you are going to learn how to edit the 'Functions.php' file. Again, if you don't feel comfortable editing this file, then it's recommended that you shy away from doing so. There are other ways to go about this and other types of security options.

The first thing that you may want to do is hide your WordPress version. The only reason that this would be necessary is if you are not keeping WordPress updated. For instance, you may be using a theme or a plug-in that requires an older version of WordPress so this keeps you from updating it. When you use an older version like this, your site will have security loopholes.

Really it is a best to try and keep your WordPress updated so that you don't have these kinds of problems. You can usually find an updated version of a plug-in or a different plug-in that is newer and does the same thing. If you are using an old theme or plug-in that doesn't have an updated version, then it's likely that it has been abandoned and you probably shouldn't be using it anyway. In other words, if the makers of a plug-in are not updating their plug-in, then they almost certainly aren't catching security risks inside of their plug-in.

Again, it is recommended that you keep your WordPress and all of its plug-ins up to date. However, if you need to hide your WordPress version then you can begin the process by visiting <http://www.wpbeginner.com/wp-tutorials/the-right-way-to-remove-wordpress-version-number>. You will find a couple of different tactics on this page on how to do so, but most of them are incomplete. So, it is recommended that you only follow the instructions that pertain to editing your Functions.php file.



Basically, all you're going to do is copy the block of code that is demonstrated in the screenshot above. Then you will need to go into your FTP folder and open up 'WP-Content' folder followed by your 'themes' folder. After that, you open up the folder for whatever theme you are using at the moment; this is where you will find the 'Functions.php file that you're looking for.

You can actually do all of this inside of WordPress if you don't want to mess with the Functions file. If you know how to do this through the Functions file it can be a little easier, but as always, you want to make sure that you have a backup anytime you're working with code in case something doesn't come out right. Anyway, you can see a screenshot of a WordPress Functions file that is opened up. Down at the very bottom of the file, there's a custom section that you can insert the section of code into. After you do this and save the file, your WordPress version will then become hidden.

Again, it is best that you always keep your WordPress version updated. Even if you use this security tactic to hide that you are using an old version, there are many different ways that hackers can find out what version you are using. For instance, sometimes they can log into an account and find your WordPress version.

Usually the biggest risk that you face is going to be through VPS shared hosting. You see, when you use cheaper sites, a lot of times you are not paying for your own hard drive computer from your host; you are actually sharing it with other people. Now, think about it. If you were to get a virus in one folder on the hard drive of your home computer, then it could spread to other folders on that hard drive. Well, the same thing can happen when you share hosting with

others. This scenario poses the highest threat to your site when it comes to it becoming infected with viruses, malware, and the like.

It is highly recommended that you talk to your host about security and see what options they can offer. Also, try to gain an understanding about how they generally handle security. Most of the good hosts out there are going to offer built-in protection against spam and they are going to constantly be monitoring for it. They will also generally provide support when it comes to fixing a site when the problem has been caused by another site on your shared hosting plan.

If you have a site that is very important, such as one that is making you money, then it's a very good idea for you to take it off of a shared hosting plan if it's on one. That way your files will be contained on their own hard drive. Doing so will also speed up your site. Just think, if you have less files on your hard drive, then your computer will run faster, right? So, it makes sense that if you are no longer sharing a hosting hard drive with other, your website will run faster.

You should take the time to talk to your host about the different options that you have. It's a lot more expensive to have your own hosting plan, but there are some scenarios where the extra cost is worth it. In most cases, however, it's okay to use shared hosting if you implement the security tactics that have been described in this lesson.