

One of the ways a hacker will attempt to break into your WordPress site is by trying to guess your administration login username and password. Now, they'll do this by using a software program that can guess hundreds of possibilities in minutes, and if you're not using strong usernames or unguessable passwords, then your site is about to be hacked. They call this a brute force attack.

In some cases, the sheer number of guesses the hacker software is allowed to go through can put such a load on your server's resources that your hosting company might even shut your site down. Now even though this shut down might be temporary, your site is still down. And this is not a good thing. In addition to having strong usernames and passwords, you also need to be able to prevent the brute force attack from happening at all. Luckily, it's super simple and can be taken care of with the installation and activation of a free plug-in.

There are several plug-ins that will make it difficult to brute force attack your site but this one is simple and lightweight, meaning it does not suck up tons of your servers resources nor slow your site down. The name of this plug-in is Limit Login Attempts. Yup. I think the name says it all. So let's go ahead and login to our dashboard area and install this plug-in. Once you're logged in, then you come on over here to the dashboard area or actually, you want to come on down to the plug-ins area so we can install a new plug-in. Before we get things rolling, let me go in and pull in my timer here so I can show you just how fast we can do this. Go on and get the timer started. Come on over here to plug-ins, click on add new. We're going to install the Limit Login Attempts plug-in, yup, right there. And click on search plug-ins and it should be the top one that pops up here. Yup. Right there. Click on install now. Click on okay. Once it's installed, we want to activate it. Just click that link there. And once it's activated, come on down here to the settings panel, come on down to the new link that's been installed, that's the Limit Login Attempts link, click on that. And here are the settings, now then, since I've been playing with this, there's my IP address right there.

By default, there's not going to be anything there, and this is not going to show up because we'll there's nothing to reset. But the other items in here are pretty well okay just the way they are. You can adjust them, the number of allowed retries, so if somebody screws up 4 times and tries it on a fifth time, they are locked out and it will show them in a red box right above the login that you've got 19 minutes or 20 minutes before the next login attempt will be working. And if after 4 of these lockouts have happened, they're going to be logged out or locked out rather for 24 hours. Frankly myself, I would change this to like 700 somewhat hours, I don't want them back because if they are a legitimate login or legitimate user and they just simply screwed up 16 times, I mean, then something is wrong there. They're trying something fishy. So really, in my experience, if they've been unable to login for 3 or 4 times, they're going to send me an e-mail. Now, if that has not happened, then it just tells me they're probably not legitimate users. I would definitely bump this up to enough hours to where they're not going to bother me again.

And the other thing that I would adjust is right here, I would like to be notified by e-mail if after a certain number of lockouts have taken place. The e-mail that they're going to send this to is the administration e-mail that is set up in your WordPress install. Obviously with this box ticked here, the IPs of those that have failed to log in are going to show up down here. And that's basically it.

Now, if for some odd reason, you have as the administrator not remembered your password you screwed something up, let me show you what happens. Let me get this guy out of the way here. Let's go and log out, and then try to log in with something other than what's proper, and try this now. and there, you see you get this box that pops up and you've got 3 more attempts before it really messes things up so if you can't remember your administrator login credentials in 4 attempts, we'll you probably will just give up all together. But if you want to, you can go into your c-panel or FTP account and just kind of disengage that plug-in.

Come on down to file manager, look for that plug-in and just rename it. That's in the WP-content directory. Open that up, and the plug-ins directory, open that up, and right here, just rename it. I just put a number or something after the end of it like 1. Just basically change the name of it. And then come on back here, refresh, continue, and then just type in the actual username because you can see that you're not limited by the time factor anymore. But, as soon as you activate that plug-in again by renaming it back the way it should be, then the remainder of that amount of time is going to be ticking down. And that's it. That's how you can get back in if you forget your own stuff as an administrator and that's how you can block out the bad guys and gals from attempting to brute force attack your site using the simple plug-in called Limit Login Attempts.

Thanks for watching and you have a great day.