WordPress is one of the famous website designing and development platforms and frameworks, which is a frequent target for hacking. Hackers are targeting the WordPress themes, core WordPress files, plugins, and even the WordPress login pages. Here, we are going to share steps that we need to take to make it less likely to be hacked and be able to recover the website easier if it should still happen to our WordPress website. Here the steps for how to protect a WordPress website from Hackers.

How Hackers Attack WordPress Website

All website on the web is under constant attack, whether its a Custom PHP or a WordPress based website, all websites are being checked or probed by the hackers. It's not informal for a hacker to scan thousands of website pages or try to login to hundreds of Websites' login pages in a day.

And this is just about one hacker. Websites are under attack by a number of hackers at the same time that we even can't imagine.

Typically it's not a human who is trying to hack your website. Hackers employ automated software to crawl the website to pick a specific weakness in a website.

These automated software programs that crawling your whole website are called bots. We call them hacker bots in order to differentiate them from scraper bots.

How to protect a WordPress website from hackers

Protect Your WordPress Website with Firewall

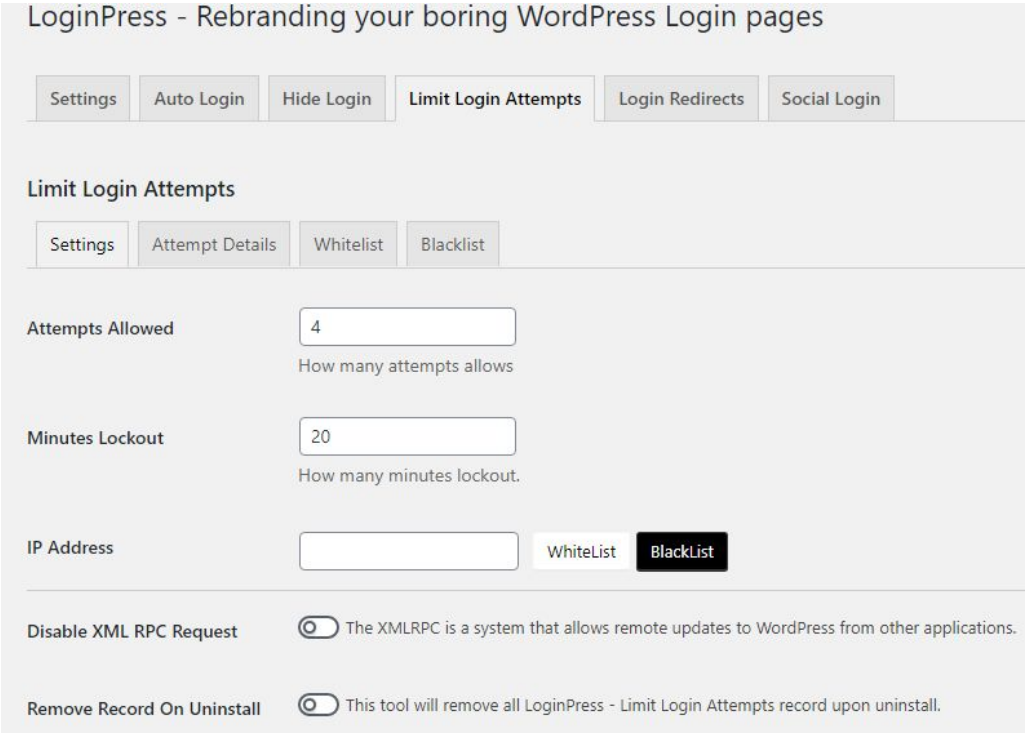
A firewall is a software program that will help you to protect your websites from hackers and block intruders. You can use a WordPress Plugin called Wordefence to activate a firewall on your WordPress website.

Wordfence checks if a website visitor's behavior matches an abusive bot. If the bot break certain reules define by the firewall, like asking for too web pages in a short amount of time, Wordfence will automatically block that bot. Wordfence also programmed to allow the search engine bots like Google and Bing.

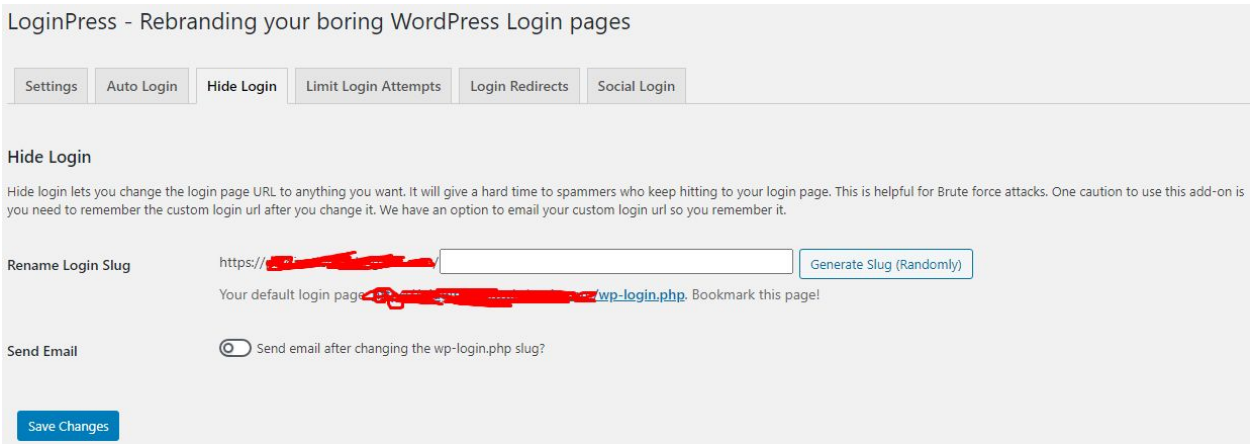
Wordfence provides the WordPress website owners, the ability to block the bots by their IP address even by a fake browser user agent that the bot is using.

Protect your WordPress website with LoginPress

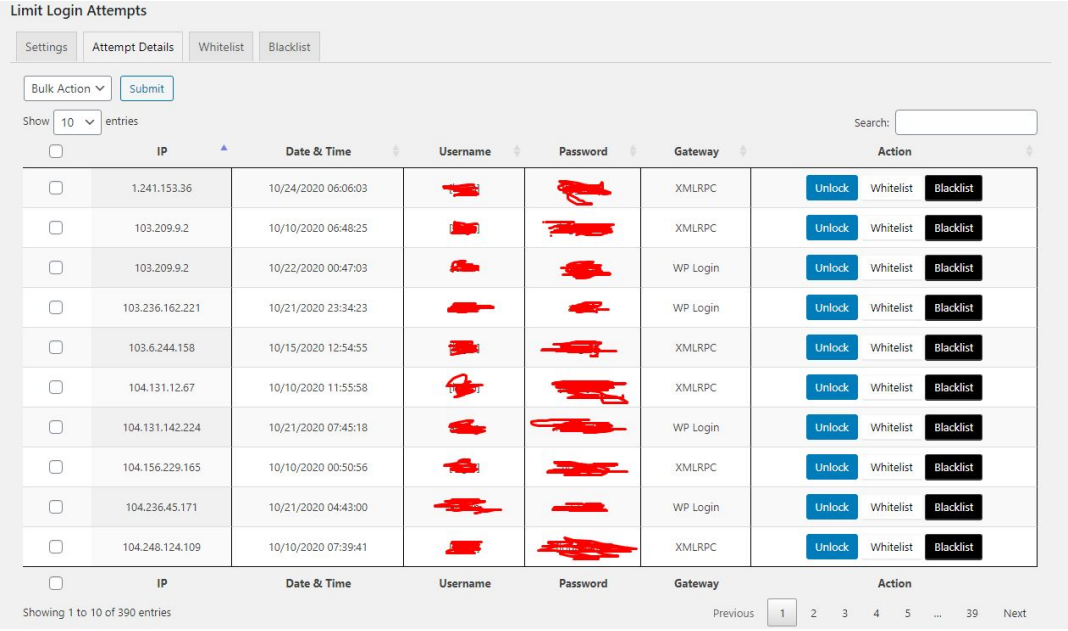
Another Plugin that you can use to protect your WordPress website from hackers called LoginPress. This plugin will help you to protect the Login page of your WordPress website from hackers.



By using **LoginPress** you can set your WordPress website login page link according to your requirements and set a limit login of your login page if someone tries to enter into your website limit login automatically will block that specific user or Bot by their IP.

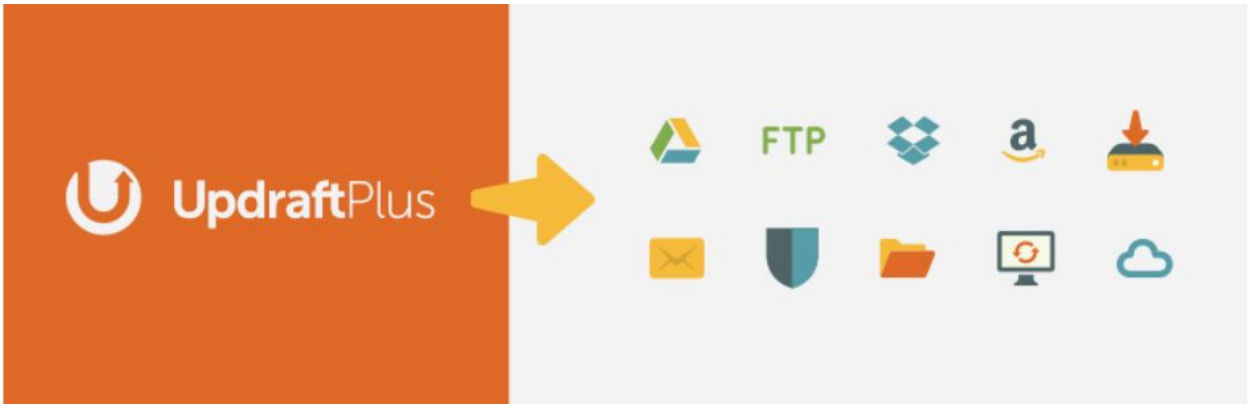


You can check these block IP in your LoginPress dashboard and add to the blacklist.



Backup Your WordPress Website

It is very important to take a backup of your WordPress website automatically on daily basis. Any issue or hacking attack that occurred on your website will take the website down and can be recovered with a proper backup of your website.



There are many backup solutions or methods that you can use to take a backup of your website on daily basis. But here is one method that you can use for your WordPress website is that you can use the UpdraftPlus WordPress plugin one of the famous WordPress backup plugins. **UpdraftPlus** WordPress Plugin is trusted by over two million-plus users and one of the best choices for taking backup of the website.

You can configure the UpdrafPlus according to your requirements that you will get your daily base backups in your email or send these backup to any cloud storage location like Gdrive, or Dropbox.

Update all Themes and Plugins

It is very important to update all WordPress themes and plugins of your website. WordPress provides a way to update the Themes and Plugins automatically, which is very convenient for website owners who don't log in to their WordPress website and update their plugin and themes.

There are many reasons not to enable the auto-update feature. For example, any updated plugin might be incompatible with other plugins.

But for other WordPress Website that doesn't change frequently, the auto-update feature is a good thing to enable for these WordPress websites.

Beware from Abandoned WordPress Plugins

The last and final step that you need to take to secure your WordPress website is to beware of abandoned WordPress plugins. Some WordPress plugins are still working after they have been abandoned by their developers many years ago. What happened to these old plugins, may contain a vulnerability and it will never get fixed.

Sometimes hackers buy these old plugins and update them with viruses and malware.

So, always check your WordPress Plugins to make sure that they are not abandoned WordPress Plugins and appear to be updated on a fairly frequent basis.

Conclusion

Here, are the steps that you need to take to secure your WordPress websites and these small steps are enough to keep the websites from getting hacked. Here, we have shared some free and Paid WordPress website plugins that will help you to secure your WordPress website from hackers, and in case of a hacking attack, you can easily recover your website.