learnwoo

WordPress Security Essentials

Find Us on Social Media

https://twitter.com/learnwoo_com

https://www.facebook.com/learnwoo/

learnwoo

WordPress Security Essentials

We hope it has been a smooth ride for you until now with your website. However, there is another important thing that you need to pay attention to - the security of your site. As you may already know, internet is not a particularly safe place. There are numerous attackers, hackers and malware out there looking for an opportunity to attack your site and steal your data. So, as a new site owner, it is really good for you to understand the possible security vulnerabilities of your site and ways to overcome those.

In this tutorial, we will look into some of the expert guidelines on WordPress security and how you can consistently ensure the safety of your site.

Security guidelines for your WordPress Core

WordPress comes with great security precautions out of the box. However, it is better to add a few more proven strategies to add more layers to your security.

Review your Access Control strategy

Which people and what applications have access to your website is an important security criteria. As the site owner, you need to take a call on access control pretty early. It is an obvious logic to provide administrative status only to very essential people. Similarly, external applications, like plugins and themes are also accessing your site at different levels. You can minimize threats by keeping only useful themes and plugins installed. Any plugin or theme that was essential in the past, but not anymore, should be deleted.

WordPress also advises to keep separate applications connected to different hosting accounts, if you are using a large number of applications. This would minimize the damage, if a particular application's security is affected, as it will only affect that particular hosting account.

In fact, you can evade a lot of risks in this regard by focusing on a few things like strong passwords, and Two-Factor authentication.

Do not use 'admin' as username
Using the default 'admin' username is a very bad idea in terms of security. If you are still using 'admin' as username, it is better you create a new account, and transfer all the data into that. Once you have transferred all the data, you can delete the 'admin' account. Also, if you are writing blog posts on your site, it is best to not do it from an administrator account. You can always create an editor profile and post your articles. This will avoid the possibility of hackers finding your username displayed on your post. Even if they try using your username and become successful, it will still be an Editor profile, which has less capabilities.

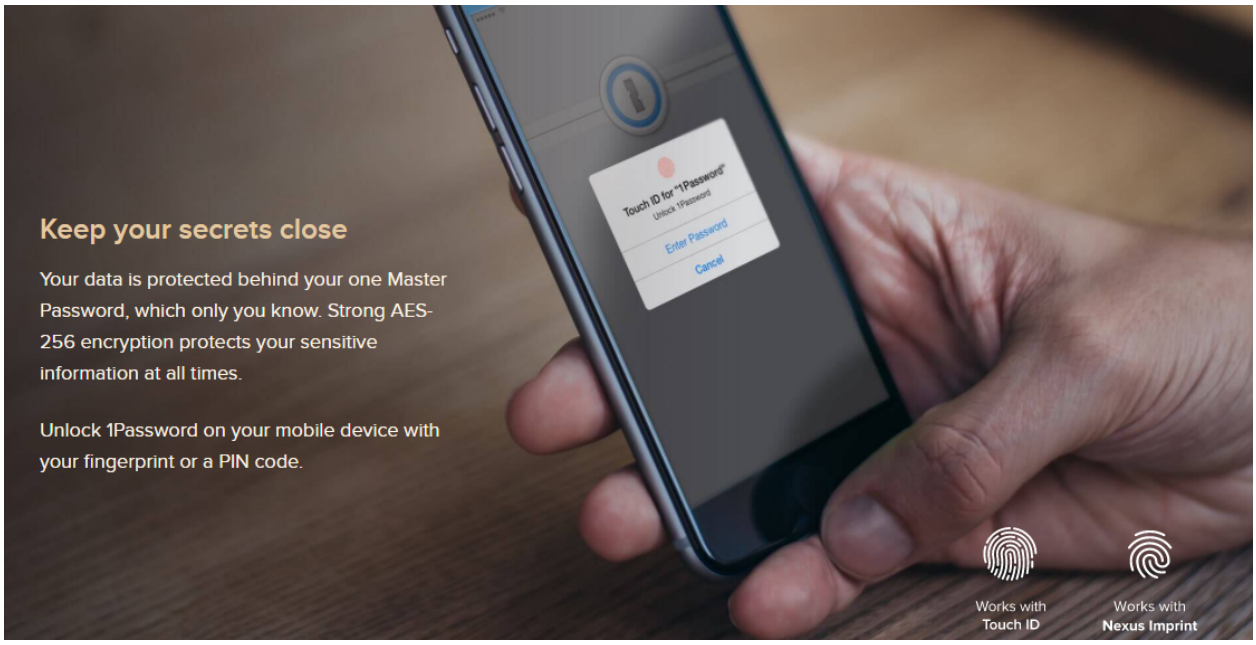
Use strong passwords
Brute force is one of the common strategies of attackers to get into your site. They will repeatedly try different combinations of usernames and passwords until they breach your defence. The best way to avoid this is by setting strong passwords. WordPress suggests using a complicated, unique and long password to log in to the backend of your WordPress site. You can simply follow the below points to make sure your password is good enough:

- Do not use your real name or a combination of your name with company name website name etc.
- It should not be a word available in a dictionary.
- It should be long enough
- Should be a combination of alphabets, numbers, and special characters.

While creating the account itself, WordPress provides a strong password by default. It is best if you use this password than accepting a weak password just because it is easy to remember.

If you are finding it tough to handle complicated passwords, get the help of a password manager plugin. Here are two good ones that you can try.

1Password
With the help of this tool, you can secure all your different passwords for different accounts in one place. Basically, you need to remember only one password, which will give you access to all your other passwords. This will relieve you from the trouble of remembering complicated passwords, and you will be able to instantly access them when required.



LastPass…
This one acts as an autopilot for all your accounts. You can save all your passwords with LastPass, and access them simply by logging in. Moreover, you can use the help of this tool while doing any other online transactions as well. It has a password generator that creates strong passwords that will protect your site against hackers.

Two-Factor Authentication
Verifying an identity on the internet is based on three principles. Something that you are (biometrics), something you have (mobile phones), and something you know (passwords). So the traditional way of identifying is by using passwords, which we have discussed above. Two-factor authentication is about using either of the other two options along with passwords. One of the common options for two step authentication is using password and smartphone together for login. You will find a few good plugins in the WordPress repository that will help you enable Two-factor authentication.

Google Authenticator - Two Factor Authentication
The plugin uses Google authenticator app to enable your smartphone to be used as an added layer of authentication to your WordPress site or blog. Basically, you can choose to enable this option only for ‘administrator’ user role, which has access to critical site functions. You can choose to allow normal password login for your other users if that seems more smooth for your site strategy. In addition to Google Authenticator, you can use several other options such as email verification, OTP over SMS, QR-code authentication, etc.