

HOW TO PROTECT YOUR WORDPRESS ADMIN LOGIN





If you own a WordPress site, it is your responsibility to ensure that the login area remains safe from malicious attackers. For WordPress users, the login is often the most important part of your website's security. By logging in, you have access to all of your website's assets and data.

This article discusses the most important security steps a website owner can take to keep their WordPress website and data safe from malicious attackers.

The Importance of Protecting Your WordPress Admin Area

Your WordPress login area is the first and most important access point to your website. Your login area is the doorway to accessing all of your website data, including private information from your customers.

It's important to protect your login as you are required to provide confidentiality and protect the data of your customers and web visitors.

A data breach caused by poor security in your admin login area can sever your business reputation and land you in legal problems.

Many hacker-attacks primarily target the WordPress admin area. They include brute force attacks where bots attempt to access your website using common usernames and password combinations.

Ways of Protecting Your WordPress Admin Area

There are a few easy steps that you can take to protect your WordPress admin login area.

Change the Default Admin Username

This is the first and most important step to take in securing your WordPress login area.

The username is set to admin by default, and many people never change it. This makes it easy for hackers to access your website as they already know your username.

It's recommended that you change the default username for your WordPress site to a username that is only specific to you.

To change the username, go to "Users" on your dashboard and create a unique username and password.

Remember to set the user role to administrator and delete the previous default admin user profile.

When creating a password, use random passwords such as the one generated by the inbuilt WordPress password generators.



Random passwords are hard to guess. You can also use a password manager if you are concerned about losing your login credentials.

Limit Login Attempts

Bots access your website by trying multiple combinations of usernames and passwords. Often, these bots will attempt these combinations multiple times before they can break in.

You can significantly reduce the chances of bots breaking into your website by limiting the number of login attempts made from the same IP address.

To limit login attempts, you can install a plugin that will lock out any IP address from your WordPress site if there are more than x number of failed login attempts.

You can also use the built-in security features that come with WordPress, such as Captcha and Challenge Questions. Some website hosts may also have built-in features that limit login attempts.

Change Login URL

By default, all WordPress websites use the same login URL, your website's main URL followed by wp-login.php or wp-admin.

You can change the default login URL on your website by adding a string to the end of it. This will make it impossible for bots to break into your website by guessing the URL.



For example, you can change it to "yourdomainname" .com/login instead of "yourdomainname" .com/wp-login.PHP.

Tools such as Protect WP-Admin can help you create new login URLs and block the default login URLs so that they redirect to the homepage. Here's a [helpful article on how to find and change your WordPress login URL](#).

Add SSL To Your Website

An SSL certificate is a type of security protocol that protects your website by encrypting data sent between the user's browser and server.

SSL certificates verify the identity of the user to the website, as well as assure confidentiality between a visitor's browser and the website.

Once you set up SSL/ HTTPS, only the user's browser can decipher data sent from a server as the data is already encrypted.

Two Factor Authentication

Two Factor Authentication involves adding a second layer of security to help protect your WordPress login from being hacked.

It involves generating a code on a trusted device that acts as a second password. Upon logging in on your WordPress with your username and password, the login page prompts for the code.



There are free and premium plugins available for two-factor authentication on your WordPress.

Password Protect Your WordPress Directory

The WordPress directory includes all the files that make up your website. It's an important feature of a WordPress site, so you should protect it.

To do this, you should install Apache or Nginx .htaccess files. These are codes that will stop anyone without permission from accessing your site.

While this may be relatively complex to implement compared to other methods, you create an extra security layer for your WordPress.

To wrap it up, it's necessary to learn about securing your WordPress login area as you are fully responsible for protecting your website.

The methods listed above are simple, but they can keep your website from getting hacked and losing your user data.

You can also look for security tools and plugins that can help to protect your WordPress admin area.

References

<https://www.wpbeginner.com/wp-tutorials/11-vital-tips-and-hacks-to-protect-your-wordpress-admin-area/>



<https://managewp.com/blog/protect-wordpress-admin-area>

<https://www.wpexplorer.com/protect-wordpress-login-page/>