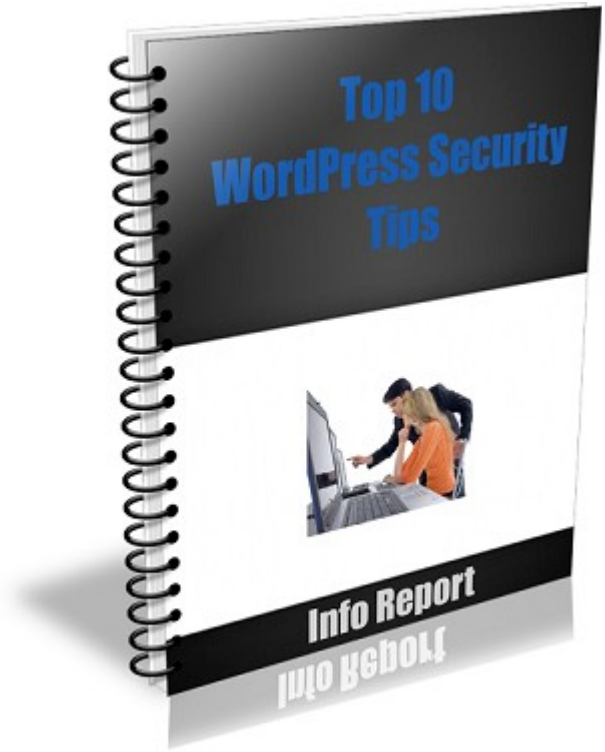


Top 10 WordPress Security Tips

Brought to You By [PLR-MRR-Products.com]

You may give away this report.

It may not be sold or modified on any manner.

Disclaimer

Reasonable care has been taken to ensure that the information presented in this book is accurate. However, the reader should understand that the information provided does not constitute legal, medical or professional advice of any kind. No Liability: this product is supplied “as is” and without warranties. All warranties, express or implied, are hereby disclaimed. Use of this product constitutes acceptance of the“No Liability” policy. If you do not agree with this policy, you are not permitted to use or distribute this product. Neither the author, the publisher nor the distributor of this material shall be liable for any losses or damages whatsoever (including, without limitation, consequential loss or damage) directly or indirectly arising from the use of this product. Use at your own risk.

Top 10 WordPress Security Tips

It would be hard to overstate the popularity of WordPress as a web publishing platform. Between the fully hosted blogs at WordPress.com and the self hosted blog software that's available for download WordPress.org, there are hundreds of millions of sites running on the WordPress platform. This makes WordPress a great resource for individuals and businesses looking to create their first websites.

But it also makes WordPress websites a popular target for hackers. Since having your website hacked can be devastating to your business, it's important to make sure you're doing everything you can to stay secure.

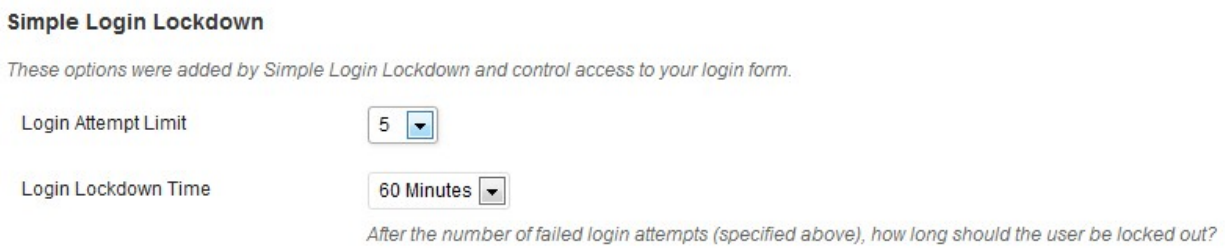
Here are the top 10 WordPress security tips you should consider. (Note that some of these tips will apply only if you host your own WordPress installation, but not if you use the services at WordPress.com.)

1. **Keep Your WordPress Install Up To Date**. Sometimes the strongest security tips are also the easiest to implement. Every time you login to your WordPress dashboard, check the top of the screen to see if a new version of WordPress is available. Because security fixes to the underlying WordPress code are distributed through these updates, it's important to make sure you're always running the current version of the software. You should also make sure all your WordPress plugins are also up to date.

2. **Make Backups**. Having backups of your WordPress site not only provides protection in case your site is compromised, it also acts as an insurance policy in case something happens with your web host. It's certainly possible to manage the backup process manually, but there are plugins you can use to make the process much easier, including UpdraftPlus Backup and Simple Backup. Make sure to keep those backup files in a secure location as well.

3. **Don't Use "Admin" or Your Email Address For Your Username**. Not all hacking consists of high-level computer manipulation; quite often WordPress sites are compromised by someone guessing the site administrator's username and password. Unfortunately, if you use "admin" or your e-mail address for your username, then a hacker is already halfway towards reaching their goal. It's much more secure if you make your username something that would be as difficult to guess as a strong password.

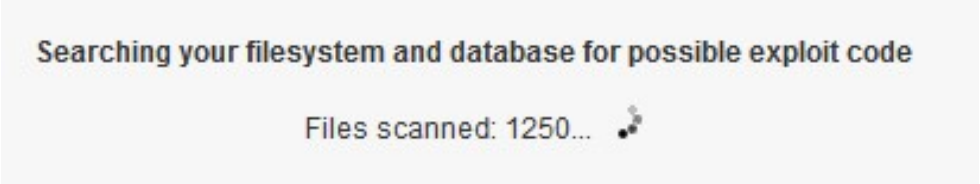
4. **Limit The Number of Failed of Login Attempts**. A persistent hacker may not be sufficiently dissuaded from attacking your site if they can simply use a "brute force" attack to try to guess your username and password. You can use a plugin like Simple Login Lockdown to detect failed logins from a particular IP address and significantly reduce the threat of these brute force attacks. This plugin will block an IP address from accessing your login page for one hour when there are five successive failed attempts -- although the lockout time and number of attempts can be changed.



5. **Make Sure Your Themes are Secure**. Hackers should not be your only security concern. Given the seemingly endless number of sources for WordPress themes, you need to be confident that you're not using a theme with any malicious code. You can use a plugin such as Theme Authenticity Checker to identify any potential he problematic code that may have been added to an otherwise valid theme.

6. **Additional Login Authentication.** The Login Dongle plugin provides an additional layer of login protection. This plugin installs a bookmarklet in your browser, and asks you to create a secret challenge and response text. When you go to your login page, after entering your standard username and password, you then click the bookmark and fill in the proper response code before you can log in. This creates an additional level of authentication security for your blog.

7. **Do a Security Scan**. Unfortunately, it won't always be clear to you when you've been hacked. Sometimes hackers want to use your server space for activities that may not be apparent simply by viewing your site. You can use a plugin such as Exploit Scanner to automatically search through the files on your site for anything potentially suspicious.



8. **Consider a Multi-Tiered Security Manager**. Wordfence Security is a multi-pronged security plugin that adds a firewall to your website, as well as virus scanning, real-time traffic analysis, the ability to see any changes to your core WordPress files, and many other functions.

9. **Secure Your wp-config.php File**. Your wp-config.php file contains very important information about your WordPress site, including details on the databases that contain all of your posts and comments. You can keep this file more secure by following the tutorial here.

Don't give a hacker access to your private information in this file:

10. **Protect Your WordPress Directories**. Finally, you can protect your underlying WordPress directories by adding the code "Options –indexes" to the very beginning of your .htaccess file. If you've never worked with a particular file before, then this is another one that you may wish to contact your web host or Webmaster for help on. You can also consult this tutorial.

WordPress provides you with the ability to make a powerful and professional website without spending a penny on software. Make sure to get the most out of your site by keeping it secure.

Wordpress Info Products

The Wordpress Classroom - High Value Training That Teaches How To Set Up And Build A Business Using Wordpress. New Videos And Plugins Added Often.

Wordpress User Manual Plugin - A Comprehensive Video And Online Manual Wordpress Plugin That Developers Can Give To Their Clients. It Has Over 30 High Quality Video Tutorials. An Online Manual With Over 100 Pages. It Automatically Updates With Each New Version Of Wordpress.

Auto Content Cash - Wordpress Auto Blog System,The Wickedly Effective Wordpress Auto Blog System Is Now Revealed.

SwiftWebDesigner.com – Web design with the Power of Wordpress