Seven Steps to Secure Your WordPress Website

WordPress is a great way to build and manage a website. Like any online software though, there are steps you should take to secure your WordPress installation and keep it safe from hackers. Some are common sense for any website (secure website hosting and choosing a secure password) and others are specific to WordPress (such as the plugins recommended below). Here are seven steps to secure your WordPress website.

1) Pick a Good, Reliable, Secure Website Host

Where you choose to host your WordPress website can make a difference in your security. Two important things to look for are server security and backups for restore.

Choose a host who offers you php5 and runs it in suEXEC mode. With suEXEC you are able to lockdown your files more tightly. You can find more technical (very technical) details here: http://en.wikipedia.org/wiki/SuEXEC

Also look for a host who offers a reliable backup system and will restore your site for you free in the event of being hacked. Most hosts offer weekly and monthly backups at a minimum. Some hosts also do nightly backups and incremental hourly backups. I'm hosted on a server with monthly, weekly, nightly, and incremental backups. This means that if my site were to be hacked I could easily roll back to what it looked like 3 or 4 hours ago. I wouldn't loose much, if any, of my content or other files.

2) Use Fantastico to Install Your Blog (or Change Your Admin Username)

If you install yourself with FTP and cPanel, you'll have a default username of "admin" which is very easy to guess. By using Fantastico, you will be given the choice to pick a username and password that are unique. Plus, it's easier than an install with FTP and cPanel.

Either way, don't use "admin" for the admin username. And don't EVER use "password" for your password.

3) Use a Secure Password

Hackers and bad people are constantly attempting to crack into our online accounts and access everything from our email to our online banking records. How can you stop them from easily accessing your accounts? One important step is to use SECURE passwords that aren't easily guessed or cracked by their software.

Here are tips on how to create secure passwords:

- Don't use names, dates, phone numbers, or addresses
- Don't use common words from the dictionary
- Mix up letters and numbers
- Make it at least 8 characters long (longer is better)
- Change it often (for online banking or hosting accounts, try every 3 months)

You may also want to use an online random password generator like this free one: http://www.random.org/strings

4) Stay on Top of WordPress News

Subscribe to the udpates here so you'll know immediately when the developers release an update or patch for any security issues: http://wordpress.org/download/

5) Keep Your WordPress Installation Up to Date

It's critical to your security to keep WordPress up to date. The new versions of the script make that very easy and you can update in just a couple of clicks. It's under "Tools" then "Upgrade" on the menu on the left of your admin pages.

For more detailed info on updates: http://codex.wordpress.org/Upgrading_WordPress

6) Keep Your Plugins Up to Date

Anytime a plugin is updated, be sure to update the version on your site. You'll know an update is available because when you login to your admin area, there will be a number in bright orange-red circle next to the "Plugins" link on the left. Click "Plugins" and it will show you which have an update available. You can follow the steps to automatically upgrade your plugin(s) as needed.

7) Install Security Plugins

Here are two security plugins I run on my WordPress websites and recommend installing:

- WP Security Scan: http://wordpress.org/extend/plugins/wp-security-scan/
- Secure WordPress: http://wordpress.org/extend/plugins/secure-wordpress/

With these seven steps you'll have a more secure installation of WordPress.