Do you host your site on WordPress? Many millions of people

and organizations do, because it's really easy to use, open source (read: free, heavily supported and well-documented) and can be customized to look pretty much any way you want.

But for a hacker with just a bit of skill, it's not too difficult to worm their way into an unprotected WordPress site and cause all kinds of trouble! I just spent most of my Thanksgiving weekend cleaning up a site that was hacked about 3 weeks ago. I thought it was all cleaned out…but it wasn't, and the database was totally corrupted and malicious scripts were putting out phishing information on the site (like asking for peoples' credit card numbers, paypal logins, etc.). This is a HUGE problem!

Of course, all sites–no matter how they are built–are vulnerable in some ways. Just like our homes. But we can do simple things to protect our homes, like install a burglar alarm, lock our doors and windows, and not leave a key under the mat.

We can do simple things to protect our WordPress sites, too. And luckily there are SOME programmers out there who are using their powers for good instead of evil, and they've written some great (free) WordPress plugins that you can use to protect your Internet real estate.

Take a few minutes and install these plugins on your site, activate them and go through the steps they outline. It will take 20 minutes or so, and will save you a world of hurt if your site is ever hacked.

One really important tip that this doesn't cover–Make SURE that in WordPress, you NEVER use the "admin" login. In fact, just delete it (make sure you have some other account with administrative privileges created first, of course!). What hackers use to break into your site is a program that repeatedly guesses random combinations of letters and numbers until they lock onto your password. So if you are using "admin" as your user name–the default WordPress user name–then they already know half the combination to access your site!

It goes without saying to make sure your password is as complex as possible–more than 8 characters, containing letters, numbers and symbols, as well as capital and lower-case letters.

So here is that list of a few critical steps you should take to protect your WordPress site. ***(caveat: this only works on a self-hosted wordpress site. if your site is hosted on wordpress.com (if your URL is something like yoursite.wordpress.com) then you can't install these plugins.)***

Create a new administrator user with a new login name. Delete the default "admin" user.

Use random gibberish passwords of at least 12 characters. Here's a helpful random gibberish password generator .

Install and activate the Login Lockdown plugin .

Install, activate, and run the Secure WordPress plugin .

Install, activate, and run the WP Security Scan plugin . Run its File Permissions check, and change your folder permissions accordingly.

If you are creating a new website, install, activate, and run the Maintenance Mode plugin to create a landing page and "cloak" the work in progress.

Also, be sure to keep your WordPress install and your plugins updated to their most recent version at all times. Usually the updates to the system and to plugins are to address new security vulnerabilities. Hackers are always developing new ways to attack, so the WordPress developers must respond with enhanced security.

I assure you that now you don't scare about WordPress security, now sleep much and think your site is more secured and protected.