7 Quick and Easy Tips for Better WordPress Security

Written *by* Jim Wright

Nothing strikes terror in the hearts of website owners and webmasters like the words: “Your site’s been hacked!”

And, unfortunately, having your WordPress website hacked is a common — and not unfounded — concern.

Although keeping up with the hackers can be complicated, there are a number of easy things you can do to keep your site reasonably secure.

Hackers tend to look for sites that are easy to break into … the low-hanging fruit, if you will.

Since none of us wants to be their easy target, here are seven quick and easy tips to keep WordPress sites more secure …

1. Keep Your Site Up-To-Date, Part 1

One of the easiest and simplest ways to keep your site secure is to keep it up-to-date.

The main reason for this is that what gets “fixed” in many updates are security issues and vulnerabilities. Ensuring that your site is up-to-date means that any known security issues have been dealt with and the security holes have been patched up.

Keeping your site up-to-date is important, but it’s not just your site that needs to be up-to-date; all of your WordPress themes and plugins should also be kept up-to-date, and for the same reason.

A word of caution: If you have a complicated site with many different theme options, plugins, and widgets, there is always the possibility that they won’t all play nice once the updates have been completed.

Although I’ve never had any issues, I’m aware of those who’ve had compatibility issues, and it’s not fun!

Check with your theme and plugin providers to make sure that upgrading won’t cause any compatibility issues.

2. Keep Your Site Up-To-Date, Part 2

Another way of keeping your site up-to-date is to audit your site for unused themes, plugins, and user accounts.

Unused and outdated themes, plugins, and user accounts are all potential security risks.

Simply go through your site and delete any unused themes and plugins, and remove any unused user accounts.

3. Remove the Admin Account

One of the things that WordPress hackers count on is that most WordPress installations will have the default username “admin.”

You can change this in one of two ways:

1. When installing WordPress, the default admin username will be “admin.” Just make sure you specify your own admin username instead.
2. If WordPress is already installed, just create another user with administrator privileges, and then remove the admin account.

Note: If you delete the admin account, you will have the choice to delete any posts attributed to the admin account, or to reassign them to another user.

4. Use Strong Passwords

You knew this one was coming, right?

It’s estimated that 10% of WordPress breaches occur as a result of weak passwords.

What makes it worse is that lists of common passwords are easily available; just Google “worst passwords,” and you’ll see them all.

Here’s a partial list of often-used passwords:

1. 123456
2. password
3. 12345678
4. qwerty
5. abc123
6. 111111
7. iloveyou
8. admin
9. 123123
10. letmein
11. monkey

Someone trying to hack a WordPress site armed with the username “admin” and that list, could potentially do a lot of damage!

(Hopefully you didn’t see your password on that list!)

5. Beware of Free Themes and Plugins

The problem with free themes and plugins is that they are not all created equal.

If you're using a free theme or plugin, it's definitely worth checking out the ratings, and version numbers (to make sure they're updated on a regular basis) to try and get an idea of the popularity of the plugin.

Another tip is to watch for plugins that also offer a pro version — these are written by professional programmers, and chances are the quality of the plugin will be much higher.

Although I don't use a free theme, I do use many free plugins, but I stick to ones that have a track record, and of course, I keep them up-to-date!

6. Get Better Hosting

Sometimes, things are cheap for a reason.

Many years ago, the hosting company I was using was sold, and the company that bought them out didn't give the impression that quality was very important to them. This led to one of the sites I was looking after being hacked due to issues with the (in)security of their web servers.

I changed to a more reputable hosting company, and haven't had any further problems.

Again, it's worth checking out your web hosting company and looking at their track record and reputation, not just price.

7. Consider a WordPress Security Plugin

Why is this tip at the bottom of the list instead of the top?

By their nature, WordPress security plugins tend to get their tentacles pretty deeply into your site — and on existing sites, the plugin can go in and change things like accounts, links, directories, and many other parameters. If you don't know exactly what you're doing, there is always the possibility that your site can be rendered unusable.

Also, many of the functions of these plugins have been covered in the previous six tips (enforcing strong passwords, removing admin account, etc.).

If you're considering adopting a security plugin, it's important to do your research. As for options, iThemes Security (formerly Better WP Security) and Wordfence are two of the most popular.

Keep a Backup

Although not a security tip per se, it's always a good idea to have a regular backup of your site, just in case something does happens.

It's just a good idea! Implement these seven security tips, and enjoy some extra peace of mind.