# WP Security Ninja II

By

**Paul Okeeffe**
**Global Marketing Ninja**

## Usage Rights

## Disclaimer

All the material contained in this book is provided for educational and informational purposes only. No responsibility can be taken for any results or outcomes resulting from the use of this material.
While every attempt has been made to provide information that is both accurate and effective, the author does not assume any responsibility for the accuracy or use/misuse of this information.

# - Table of Contents -

# Top Simple WordPress Security Tips

So you're using WordPress and you want to keep your site safe from hackers, malware, spam and other threats… where do you begin?

While WordPress does have some security risks, most of these are relatively simple to plug as long as you know where to look. This article will provide some easy and straightforward tips to help you fortify your site and to avoid common mistakes.

### Consider Your Host

WordPress security isn't all about WordPress! Another weakness can often lie in your hosting account, so make sure you research the security of your hosting provider thoroughly before choosing one. Look for hosts that are willing to discuss security concerns and offer the most recent stable updates to server software.

### And Your Computer!

Likewise, another alternative 'way in' for hackers is through your computer. If you have malware on your system, this can do things like record your keystrokes in order to isolate passwords. Make sure your security software is up-to-date and that you do regular scans.

### Keep Updated

Many vulnerabilities exist in WordPress itself and the plugins that you install, but as long as no one finds them, you're safe. The problem is, people *do* find them and when that happens you can be briefly vulnerable.

In the vast majority of cases, the developers of WordPress or the plugins will identify the flaws in their security very shortly after they come to light. They will then issue an update to fix them. This is why it's *so* important that you update not only WordPress but also all of your plugins every time a new update is issued. If you don't, then you might be leaving well-publicized flaws in your security for hackers to take advantage of!

### Avoid Unnecessary Plugins

Every plugin you add to your site presents new potential security flaws in your code. Having too many then will unnecessarily leave you susceptible to a number of possible attacks and can also slow down your site. Don't use more plugins than you need and make sure you research the quality of any that you *do* decide to use.

### Install Security Plugins

Some plugins that *are* useful are those specifically designed to provide additional security to your WordPress site. This is a very easy way to upgrade your sites fortifications that takes minutes – so do it!

### Choose a Smart Password

This is a simple and easy one but it’s too often ignored. Make sure that you use a strong password *and* username combo for your admin login.

# The Top WordPress Captcha Plugins

Captcha software is software designed to stop spam and brute force attacks. Its main goal is to make the user 'prove they are human' in order to prevent computer scripts from automatically entering thousands of username and password combinations, or automatically submitting comments.

Captcha often works by getting the user to type out the letters of an obscure image, which is difficult for software to discern even using optical character recognition. This is a smart and largely effective system but unfortunately it can sometimes be overly challenging and frustrating for the user.

Here, we will look at some of the best plugins available for WordPress that allow you to increase your security in a way that is less annoying – or even *fun* – for the user.

**Google Captcha**

Also called 'reCAPTCHA', Google's Captcha plugin challenges users to identify things like house numbers from Google Maps or skewed words from their book-uploading projects.

It's clever sure, but how does that benefit you or your users? Well, the simple fact is that reCAPTCHA is reliable and common. People are familiar with it and it does the job it sets out to do well.

**Fun Captcha WP Plugin**

'Fun Captcha' is a plugin that turns captcha into a game. There are four different modes for you to choose from, which should bring a smile to your visitors' faces.

**Sweet Captcha Revolutionary Plugin**

That's quite the name! This plugin attempts to live up to the 'revolutionary' moniker by using cutesy interactive images rather than boring text to keep spam out. Tasks involve dragging guitarists onto guitars for instance, which is both amusing and a little more effective than some other anti-spam measures.

**Free Math Captcha WordPress Plugin**

As the name suggests, this one works using math problems to filter out spam. It works quite well too, as the problems are very quick to solve. It could be a smart choice for a blog on brain training or learning too!

**Key CAPTCHA**

This popular choice actually gives you the option to *monetize* your CAPTCHA by using ads. It works with login, comments, forms and more.

So there you go, a big selection to get started with! Of course there are many more, so keep looking around if none of these appeal. The key thing here is that you implement *some* form of spam protection, as bots can sometimes be much more than merely a ‘pest’.

# The Top Plugins for Protecting Your WordPress Site

One of the very best things about WordPress is the huge community supporting its development and consistently submitting new plugins and themes for developers, bloggers and businesses to take advantage of.

With millions of free plugins available, it's possible for you to add a wide variety of features to your site with just the touch of a button.

And one of the most important places to start is with your security. Here are some of the best themes/plugins you can add to help protect your site from a myriad of threats.

**iThemes Security**

iThemes Security was previously known as 'Better WP Security' and is a plugin that promises to help protect your WordPress site in over 30 different ways. It protects automated attacks, fixed common security flaws, adds a two factor authentication process, password expiration and malware scanning among other things. It has good reviews and is a very comprehensive approach to your security.

**Backup WordPress**

In the worst case scenario there is still one option – burn it all down and start again! Only, you probably won't want to do that if it involves losing many years of work and taking your site entirely back to the drawing board. Backup WordPress is a plugin that does what it says on the tin – backs up WordPress and all the hard work you've put in.

**All in One WP Security & Firewall**

This is another plugin designed to check and fix vulnerabilities in your WordPress site. It protects against brute force attacks, sends email notifications when someone gets locked out of your site and includes a 'security scanner' to track files that are changed to look for malicious or suspicious code.

**Key CAPTCHA**

CAPTCHA helps to block both spam and brute force attacks by providing a test to prove that you're human. Key CAPTCHA is a popular and effective example of this that has lots of options and lets you protect login, comments, forms and more for comprehensive coverage.

**Optimize Database**

Optimize Database should keep your WordPress site running smoothly by keeping your database clean and preventing errors.

All these and many more plugins can all help you to keep your WordPress site safe and secure – but remember that too many plugins can present a risk in themselves. Try not to overdo it – choose a security plugin and CAPTCHA that works for you and then just use common sense to protect against the rest!

# The Security Benefits and Weaknesses of Using WordPress

There are hundreds of very good reasons to use WordPress. WordPress is a tried and tested platform that has helped many users achieve *significant* success online. The platform is simple and easy to use with tons of customization options and it has become something of the industry standard these days for blogs and more. It's free, there's a huge community… it's great.

But just because WordPress is amazing, that doesn't mean it's perfect – and it's crucial to remember this as a webmaster or blogger in order to avoid down time and other problems. This is particularly true when it comes to security. Here we will look at why WordPress is a *boon* for security, as well as why it is a risk…

**The Security Benefits of WordPress**

The big benefit of WordPress when it comes to security is the huge community surrounding it. Millions of people use WordPress which is an open source platform that anyone can contribute to. This is great news because it means there are *thousands* of people looking after security at any given time. If one user spots a security flaw in the system, then they will likely report it and a fix will be uploaded in no time at all. What's more, plugins designed to enhance security are being added all the time.

Another big advantage of WordPress is that it is such a big and powerful CMS (content management system). It's been around for a long time, it was coded by absolute experts in their fields and most IT support companies and web developers know how to work with it. This means that you don't need to try and build your own website – with security – yourself and means you don't need to hire a company you've never heard of to do it. It *also* means that when something does go wrong, most people you contact will be able to help you fix it quickly without having to learn the way around your code.

**The Drawbacks of WordPress**

Unfortunately though, the very things that make WordPress secure can also be drawbacks in some senses.

For instance, the fact that anyone can provide themes and plugins means that you will often be trusting complete strangers with your security. Add a plugin from an unknown source and you might be opening yourself up to new vulnerabilities.

At the same time, the fact that so many big sites are on WordPress means that it's a very appealing target for potential hackers. If they can hack *one* WordPress site, they can probably hack them all – which is why we need to be ever vigilant against people trying to bypass our security and work as a community to defend what we've built.

# The Psychology of Security for Bloggers and Online Businesses

When it comes to security, the biggest flaw of *all* is most often the wetware – the human element. You can have the best security software in the world but if your password is 'password' then you're likely going to be caught out.

The problem here is that many bloggers aren't tech savvy enough to understand the basics of how hacking works. They fail to recognize the methods and motivations of their enemy and as such, they waste time on unnecessary security methods, or miss the most important ones.

**You Are Not a Target**

One commonly held belief for many bloggers and small online businesses for instance, is that they are likely to be 'targeted' by hackers. The belief here is that someone is sitting at home, plotting to hack into their site.

This is *highly* unlikely to be true though, unless you have hundreds of thousands of visitors a day, or you look after lots of bank account details. In all likelihood, you aren't going to be worth the time of a hacker to target you directly. And anyway, with billions of websites on the net, the probability *alone* makes it unlikely.

This is why it's not *terribly* useful to move your login URL to another address, or to choose a password that a *human* wouldn't guess.

**Hackers Work on Scale**

Does this mean that your website is completely safe from attack? Not at all. And the reason for this is that hackers actually tend to work *on scale*. What this means, is that they write scripts, send out phishing e-mails and generally try a 'blanket approach' to see who they can hack into. Scripts for instance will work by entering millions of username and password combinations into a log-in form.

Alternatively, hackers might focus on zero hour vulnerabilities – flaws in the software *underlying* lots of websites, rather than any specific website in particular.

Understanding this changes the game. It means you aren't one person defending yourself against one person – you are part of a community defending against software flaws and malicious ‘scripts’. To keep yourself safe, you need to be vigilant in applying updates, you need to stay relatively ‘under the radar’ and you need to avoid being predictable from the perspective of a machine.

And consider this: as long as your site is *less vulnerable* than the majority of others, the malicious software will likely move on and look for easier targets. Just like camping with your friend when a lion enters the tent – you don’t need to run faster than the lion, you just need to run faster than your friend…