Resource Center

‹ Back to Resource Center

7 WordPress Security Tips and Best Practices Every Site Owner Should Know

Posted in **Security** by Britt Dreisbach

Last updated on October 10th, 2024

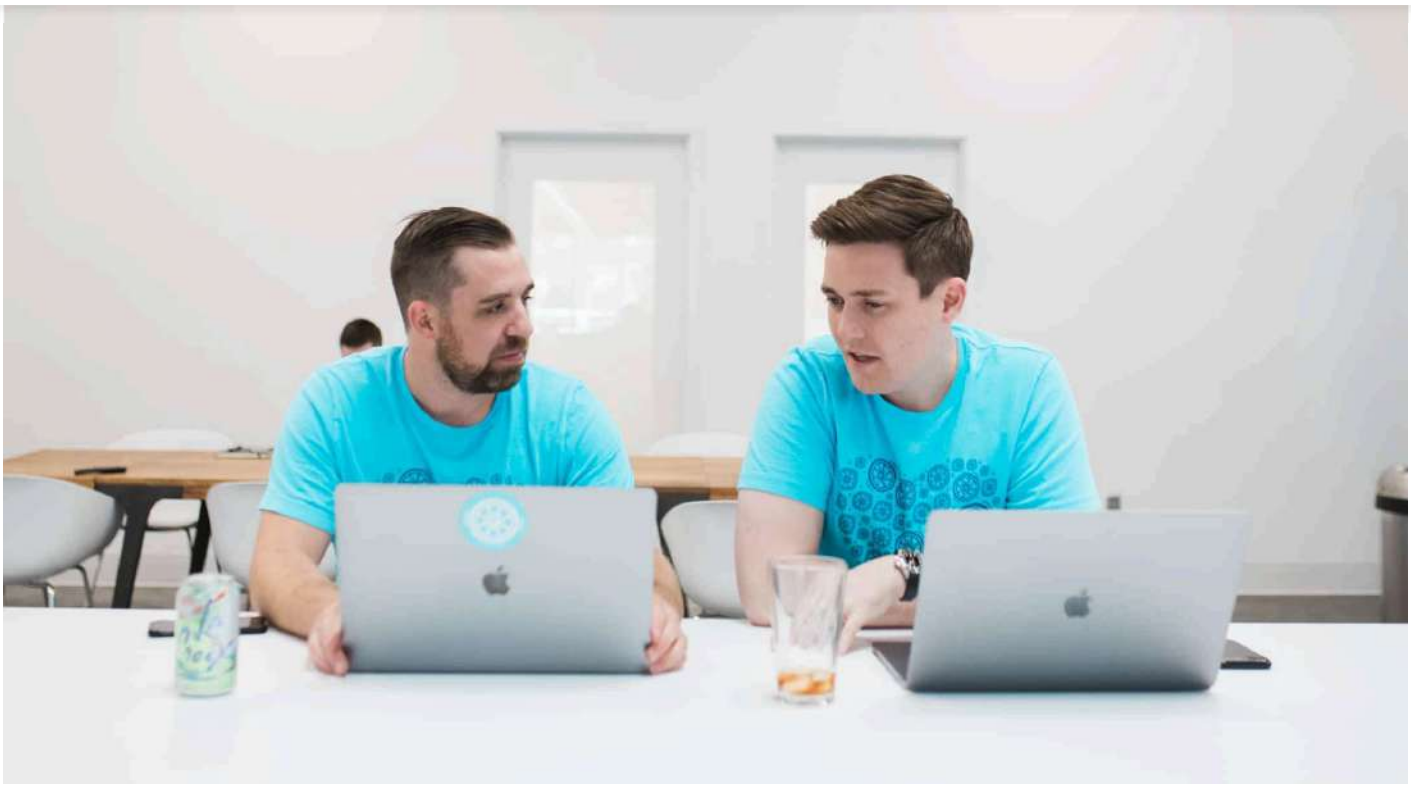
Hey there! What can we help you with today?

While there's no "one-size-fits-all" security solution for every WordPress site, there are a few security best practices that can make a big impact.

In this article, we'll explain why sites get hacked in the first place and share key security tips that are easy to implement in your workflow. Here's a quick overview.

Table of Contents

Ready to boost your WordPress site security? Let's get started!



Why do WordPress sites get hacked?

Before we jump straight into WordPress security best practices, it can be helpful to understand why websites get hacked in the first place. Generally speaking, hackers target websites for the following reasons:

- To send spam emails through your site.
- To steal your information, such as data, mailing lists, stored credit cards, etc.
- To trick your site into installing malware on your users' machines (or your own).

While a security event might feel like a personal attack, it's often part of a larger scheme, such as a **Distributed Denial of Service (DDoS) attack**. Rather than target a single site, hackers might target the infrastructure your site is operating on, affecting numerous sites at once. That's why it's important to be familiar with basic WordPress security standards, even if you're just running a personal website.

In addition to the above, WordPress may be targeted specifically simply due to its widespread popularity. Because it now **powers more than 43%** of all websites, WordPress offers a large "area

system (CMS) with a highly dedicated and involved community of **contributors**, which means there are a ton of people continuously working to improve the security of the platform.

The truth is, any website can experience a security issue at any time, and the same goes for sites built with WordPress. Luckily, there are several best practices you can implement to increase the security of your WordPress sites and make it far more difficult for hackers to mess things up.

7 WordPress security best practices

1. Keep your themes, plugins, and WordPress version up to date

One of the easiest ways to give your site an extra security boost is to keep everything updated.

If developers discover a vulnerability in their code, they'll usually push an update to fix it. The longer your site uses the outdated version, the more likely it is to be targeted by hackers.

While it might take some time, staying up to date with all plugins, themes, and WordPress core updates is a great way to limit security risks. If you're using a **managed host for your WordPress site**, WordPress version updates should be performed automatically, helping you stay on top of the latest updates to core.

When it comes to keeping your plugins updated, solutions such as **Smart Plugin Manager** automatically check your plugins for updates at a pre-scheduled time. Using machine learning and visual testing, Smart Plugin Manager also ensures your site doesn't break when updates occur.

2. Apply username and password best practices

There's nothing new about this security tip, but it's absolutely worth a reminder:

Use unique passwords. Use strong usernames. Use a password manager.

Hackers weren't born yesterday; they know all the most common passwords and will test every single one with the username "admin." So, do a quick audit.

- Are your usernames hard to guess?
- Are your passwords unique?
- Have your passwords been updated recently?

If you're feeling overwhelmed trying to remember all these login credentials, I highly recommend a password manager, such as **1Password**. Not only will it help you create and store complex credentials, it makes logging into sites a breeze (especially if you're working with a team!).

3. Limit login attempts

To limit login attempts, you can use a plugin like **Limit Login Attempts**, which will block any attempt to log into your site after three errors, putting a block on it for twenty minutes.

Sure, it might get in your own way if you forget your password, but that's what password managers are for, remember?

4. Move the WordPress login URL

One way to make your WordPress site extra secure is to **change the login page**. It's pretty common knowledge that to log into a site, you just add /wp-admin to the end of the URL. By changing the link, you effectively hide the entryway to your site, making it harder for hackers to find.

5. Use two-factor authentication

Another great way to make your credentials more secure is to **use two-factor authentication**. This security method acts as a temporary second password that updates every 30 seconds or so.

To gain access to your site, hackers would have to guess both your true password and the temporary security code within that 30 second timeframe, greatly increasing your chances of blocking them.

Two-factor authentication is great because you can use it with a variety of logins related to the sites you manage. For example, **WP Engine allows you to enable two-factor authentication** on your **WordPress hosting** account, and you can also add it to individual WordPress sites.

6. Add captcha to your forms

As you've probably gathered, locking down your site's login page is incredibly important. That isn't the only form you should focus on, however. Don't forget about blog comments, checkout pages, or any other open form on your website!

Each of these forms present opportunities for hackers to submit information to your site, such as malicious links in a comment. Even if it doesn't directly affect your site's performance, having shady links will create a confusing user experience, and may even hurt your business.

To prevent this type of activity, you can install a WordPress plugin like **Google Captcha (reCAPTCHA) by BestWebSoft**. This will prevent automated programs from posting spam or malicious links to your comments sections or open forms on your site.

7. Disable file editing

happen, and if they do, finding and fixing the error can be time consuming and potentially costly.

By limiting access to files that are vital to the form and function of your site, even users with admin privileges will be unable to alter theme or plugin files. It will also encourage the developers who work on your code to use best practices, promoting the use of secure file management and version control systems.

To disable file editing in WordPress, add the following line to your wp-config.php file:

```
define('DISALLOW_FILE_EDIT', true);
```

WordPress security is an important topic for every site owner to understand, and while it's a constantly evolving area of focus, the tips and best practices above should provide a solid baseline for keeping your WordPress sites safe and secure.

Visit **WP Engine** to learn about our secure **hosting platform for WordPress**, or **speak to a representative now** to find out more.