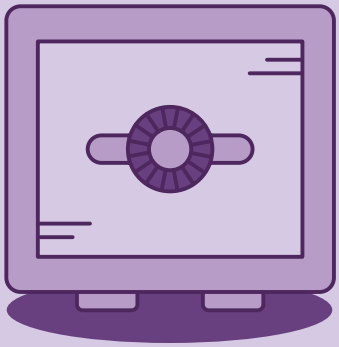
How to boost your WordPress site's security



There's no foolproof way to completely make your site secure, but there are some simple steps you can take to boost security and put up a good fight. This ebook will teach you why WordPress sites get hacked in the first place and then walk you through eight easy ways to increase security. Ready? Let's toughen up your site!

Why do sites get hacked?

To help you understand how to keep your site safe, it's important to first understand why hackers attack websites in the first place. Especially if you only run a personal blog or tiny eCommerce shop, no one should want to mess with it, right?

Not necessarily. Hackers go after websites for three main reasons:

- **They want to use your site to send spam email.**
- **They want to steal access to your data, mailing list, credit card information, etc.**
- **They want to cause your site to download malware onto your user's machines or your own machine.**

Malware, or malicious software, can be installed in a way that makes it very hard to tell it's even there. Great for the hackers, not so great for your site. Hackers will often do this to use your machine in larger scale attacks, such as a Denial of Service attack.

Why do hackers target WordPress, specifically?

The short answer – because it's popular.

Put yourself in the mindset of a hacker for just a second. If you want to take over a lot of websites for your own nefarious purposes, would you spend all of your time trying to find vulnerabilities on a platform used by 500 websites, or would you just try to break the platform with hundreds of millions of sites? Because WordPress is so widely used, it's an incredibly popular target for hackers.

The WordPress core is very secure, which makes it pretty hard to hack into. But because anyone can write additional tools for WordPress, such as themes and plugins, it's possible that not all extensions live up to the same code review standards as the WordPress core. It's possible for a very popular plugin to have security flaws that can impact thousands of WordPress sites all at once.

Don't fret; the open-source nature of the code is also what makes it strong. It is what allows white hat hackers to find exploits and report them easily so holes can be patched. It is what allows developers to help improve security over time. It is what allows third parties to create even stronger security solutions that can be installed right on top of WordPress.

> *"Dont' fret; the open-source nature of the code is also what makes it strong.*

The bottom line is that your WordPress site could get hacked at any moment (that's true for any site). But there are several things you can do to increase security and make it a little harder for hackers to mess things up.

Here's a list of some of those extra ways to enhance your site's security, starting with the most basic (and essential), working up to the more advanced options that may not be necessary or practical for everyone.

---

01 Always use strong passwords

It seems obvious, but many WordPress users overlook this vital security measure. Your password is to WordPress what locking your front door is to home security – and it doesn't matter how good your security system is if you leave the door open for anyone to walk through.

If your WordPress password is short, if it's something readable, if you use it on multiple sites, or if somebody who knows you well could potentially guess it, then chances are it should be stronger.

If you have a site with several WordPress users or allow visitors to create their own accounts, you can add the Force Strong Passwords plugin to make all users keep their passwords beefy.

02 Keep your themes and plugins updated

Like we mentioned earlier, themes and plugins can occasionally have security vulnerabilities, which are patched by the developer as soon as they're discovered. It's important to update regularly because many malicious bots specifically search for out-of-date plugins and themes with known vulnerabilities.

> *"You don't have to give up on a plugin that has a history of vulnerabilities...but it's definitely something to note.*

And when installing new plugins, be sure to check if they have any known and unfixed issues. You don't have to give up on a plugin that has a history of vulnerabilities – most of the best plugins will show a few – but it's definitely something to note when comparing options.

If your site is on Flywheel, we'll take care of WordPress core updates for you. But if you're not also updating your themes and plugins regularly, you risk leaving your site exposed to these vulnerabilities. Plus, updates often patch other bugs and enhance usability, so it's a win all around!

---

03 Uninstall inactive plugins and themes

Even deactivated plugins and themes can have vulnerabilities, and for that matter, can still take up your server's resources. It's best to simply uninstall any plugins or themes that aren't consistently active.

If this idea stresses you out, just remember: You can always reinstall themes or plugins later if you need to.

04 Move your WordPress login screen

Many WordPress hacks come from malicious bots that are programmed to crawl the web looking for WordPress sites. Once they find one, they'll add "/wp-admin" to the end of the site's URL to get to the login screen and try to force their way in.

At Flywheel, we already offer protections against this kind of behavior, but you can add an extra layer of security by making your login screen harder to find in the first place.

The Rename wp-login.php plugin allows you to change the location of your login screen from "/wp-admin" to whatever you want. You could use something like "/mysitelogin" or "/open-sesame" or anything else your heart desires! Whatever you choose, any user who tries to use the old "/wp-admin" link will just see an error message, which will help stop bots and would-be hackers in their tracks.

Note: Moving your WordPress login screen will mean that you'll have to share the new login URL with anyone who logs into WordPress on your site, or they won't be able to access the admin area.

---

05 Add an SSL certificate

SSL, or Secure Sockets Layer, is a protocol used for secure and encrypted communication between computers. It's indicated by the little green padlock in the address bar of your browser.

While this isn't necessary for all sites, it's essential for any WordPress site collecting sensitive user information. But even if that's not the case, an SSL certificate still helps to secure your site's transmissions. Plus, Google ranks secure sites higher in search engine results, so you get a little SEO boost with a secure site as well!

If you're looking for a guide to SSL, we've got just the thing for you. Check out this ebook to learn what it is, why you need it, and when to use it!

06 Add Captcha

There are several variants of Captcha out there, but the idea is the same between plugins and methods: force any site visitor who tries to fill out a form to first prove they're human. While it was once a troublesome and inconvenient option, Captcha has improved greatly in recent years. Plus it protects all kinds of forms on your site, so it does double duty by helping to stop hackers and prevent spam.

07 Avoid obvious WordPress usernames

This is less important than having a strong password, but it's still helpful. A generic WordPress username like "admin" will be one of the first things any hacker or bot will try. If somebody could guess your username just by looking at the site, it's not a bad idea to update it.

Unfortunately, WordPress doesn't allow you to change your username by default, but if you'd like, you can create a new WordPress user and then delete your old one from the 'Users' area in the WordPress admin sidebar. (You'll have to use a new email address to do this, since two WordPress users can't share the same email address, but you can always change that later, too.)

08 Use CloudFlare

This is more of an advanced option, and certainly not one that everyone needs, but CloudFlare is an external service that acts as a sort of "filter" between your servers and your users. CloudFlare offers many security and performance options, several of which are available on their free plan.

While most sites don't need to worry about DDOS attacks, CloudFlare is excellent at preventing those, since your server's IP address will be effectively masked. CloudFlare also offers a variety of other security options, including blocking IP addresses or specific regions.

Moral of the story: While WordPress is very secure, just be smart with your site and have a game-plan for the day it does get hacked – we pinky promise it'll all be OK. And if your site is on Flywheel, remember that we'll clean it up for you, for free! Just talk to the support team and they'll get it all fixed up.

Leave security to Flywheel

Having your site hacked absolutely sucks. Nobody wants to have tasteless ads show up on their homepage or spam go out from their email, so we work hard to make sure your site is always malware-free. And if it does get hacked, we'll fix it. For free.

Flywheel is a delightful platform that empowers designers, developers, and digital agencies to focus on what they do best — building beautiful, functional sites for their clients. We make it a breeze to create and develop WordPress sites, handle hosting, manage projects, and ultimately scale your business.

CONTACT SALES

sales@getflywheel.com | (888) 928-8882

Or, sign up at getflywheel.com

FLYWHEEL