WARNING

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 11 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 only used by 500 websites, or would you 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 though; 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.

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.

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

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 Use smart usernames and passwords

It seems obvious, but many WordPress users overlook this vital security measure. Your username and 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.

As for the username, steer clear from picking something typical like "admin" or the name of your site. Those will be the first thing a hacker tries to guess. The same rule of thumb goes for the password; don't pick anything obvious. If your WordPress password is really short, something readable, used on multiple sites, or even just something someone could guess, chances are it should be stronger. If you have trouble remembering a random password (or you want to be extra secure) you could always try using a tool such as 1Password or LastPass.

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 themes, plugins, and WordPress updated

Updates can be a pain to keep up with, especially if you have lots of plugins installed on your WordPress site. But it's critical that you try. 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. Plus, updates often patch other bugs and enhance usability, so it's a win all around!

> "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.

Aside from updating your themes and plugins regularly, staying on top of WordPress core updates is crucial. In fact, wordpress.org recommends it for security protection. If there's an update ready, you'll see a notification in the WordPress dashboard. Or if you're on a managed WordPress host like Flywheel, we'll actually take care of WordPress core updates for you – you don't have to worry about them at all!

Worried about updates?

Test updates in a staging environment first!

With Flywheel's free Staging feature, you can safely test theme, plugin, and WordPress updates before performing them on the production site! It's a great way to see exactly what changes will happen and make sure things work as expected. Then when you're ready, just push changes into production with a single click!

LEARN MORE

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 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.

---

05 Limit the amount of login attempts

A tactic for some hackers is to continuously try to guess your username and password to get through your site's front door, also known as brute-force attacks. There are various plugins out there that will help prevent this by blocking an internet address from making further attempts after a specified limit on retries is reached. This is highly effective at making a brute-force attack difficult or even impossible to perform.

If your site is on Flywheel, you don't have to worry about this step – all Flywheel sites have one of these plugins installed for free (Limit Login Attempts).

06 Add an SSL certificate

SSL, or Secure Sockets Layer, is a protocol used to secure and encrypt communication between computers. In other words, it helps keep sensitive information on your site incredibly secure. This includes things like passwords, credit card information, banking credentials... basically any information your site stores that you (and your users) would want to remain safe. It's visually indicated by the little green padlock in the address bar of your browser.

While this isn't technically necessary for all sites, it's incredibly beneficial (and essentially required) 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 and builds trust with your users.

Another big reason for adding an SSL certificate to your WordPress site is SEO. Google has announced that they will flag sites that store passwords or credit card information without SSL as insecure, as part of a long-term plan to mark all sites, whether they collect information or not, as insecure. In other words, if your site doesn't have an SSL certificate installed, it could seriously hurt your traffic and conversions.

Get free SSL certificates!

They're included with every Flywheel plan

We've partnered with Let's Encrypt to provide all of our users the opportunity to install SSL on their sites for the low, low cost of zero cents. No need to bounce back and forth between your hosting company and a third party provider — now, you can get world-class WordPress management and encryption all under one roof. Learn more!

LEARN MORE

07 Add two-factor authentication

Another way to prevent brute-force login attempts is by setting up two-factor authentication. This method requires two verifications – a password and an authorization code sent to your phone or email – to log in.

While it takes a little more time for people you trust to log in, it also makes it a whole lot harder for people you don't trust to gain access to your site. You can add two-factor authentication to your WordPress site login, and some hosts (like Flywheel!) offer it for your hosting account as well.

Two-factor authentication takes a little time to get used to it, but it's definitely worth it in the long-run!

---

08 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.

09 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.

---

10 Back up your site regularly

Backing up your site, routinely, is a safety precaution that will make your life easier if hackers do find their way into your site. By having a recent copy of your site, you'll be able to easily restore your content before it was compromised and won't be stuck in the position of trying to figure out what to do next.

Sites on Flywheel are automatically backed up every single night and stored for 30 days – all for free! And if catastrophe does strike, you can easily restore at any time. Learn all about it here!

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 (AKA backups!) We pinky promise it'll all be OK.

Let Flywheel take care of security for you

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 our team of WordPress experts work hard to make sure your site is always malware-free. And if it does get hacked, we'll fix it. For free!

In addition to our suite of security features, Flywheel offers you a professional managed WordPress hosting platform that's packed with sleek workflow tools. The result is a completely unique, next-level platform that allows you to quickly and easily build, launch, manage, and ultimately scale any (and all!) of your WordPress sites.

See how Flywheel can help boost your WordPress security and overall workflow today!

CONTACT SALES

sales@getflywheel.com | (402) 223-6105

Or sign up at getflywheel.com

FLYWHEEL