WordPress Security

* A POCKET GUIDE *

* * * * * * * * * * *

WordPress Security

A POCKET GUIDE

Brought to you by iThemes
Your one-stop shop for WordPress themes,
plugins & training

PUBLISHED BY

iThemes Media
1720 South Kelly Avenue
Edmond, OK 73013

iThemes.com

WordPress is a registered trademark of Automattic Inc. This ebook and its author are not affiliated with or sponsored by Automattic or the WordPress open source project.

Sign Up for WordPress Security Updates

Get WordPress security updates sent straight to your inbox by signing up for our WordPress Security Newsletter.

Subscribe

About iThemes

iThemes was founded in 2008 by Cory Miller, a former newspaper journalist and public relations/ communication practitioner, turned freelance moonlighting web designer, turned full-time entrepreneur. Miller founded iThemes in his home, fulfilling a lifelong dream of running his own company. Since then, iThemes has grown into a full enterprise providing professional, premium themes, plugins and professional WordPress web design and developer training at WebDesign.com.

Contents

Security is a big tech topic these days. Sites have been hacked and people are worried. But there's plenty you can do to secure your site.

We're going to talk briefly about security and WordPress, covering some big picture concepts to help you keep your site safe, including:

- Preliminary Ideas
- 3 Kinds of Security Your Site Needs
- 4 Best Security Practices
- More Security Help

The easiest thing you can do to keep your site secure is install a plugin such as iThemes Security (formerly Better WP Security). We actually hired the developer of that plugin, Chris Wiegman, and brought him on our team to update the plugin and make it a part of the iThemes family.

Security plugins such as iThemes Security can take care of a lot of the practical matters. But here we're just going to cover some of the conceptual ideas about security.

First Things First

Let’s talk about some preliminary ideas first:

1. There’s Always a Risk

Your website can never be 100% secure. Hackers are always trying new things and discovering new vulnerabilities to exploit. The online world changes quickly and the same is true of security. Good security is about minimizing risk. If anybody tries to sell you a 100% secure solution, they’re scamming you. You’ll never be completely safe, but there’s a lot you can do to minimize your risk.

2. Don’t Blame WordPress

The haters like to say that WordPress isn’t secure. That’s not necessarily true—it depends on how you set up and use WordPress. If you’re not keeping it updated or following bad practices, then no, it’s not secure. The reality is that 17% of the world’s websites are using WordPress, which makes it a huge target. So you need to be smart. You need to keep things updated and follow the best practices to lock your site down.

Many security issues have little to do with WordPress and more to do with server vulnerabilities, cross-contamination and poor passwords. Bad decisions can undermine your site, and that’s true whether you’re using WordPress or any other solution. So don’t blame your security woes on WordPress.

3. Security vs. Usability

There’s a fine balance between security and usability. Sometimes locking down your site makes it secure, but it’s hard to use. Sometimes making your site easier to use makes it less secure. You’ll have to find the balance.

3 Kinds of Security Your Site Needs

There are three phases to security: protection, detection and restoration. If you truly want to protect your site, you need to do all three.

1. Protection

First and foremost you need to lock down your site and keep it safe. You've got to raise the drawbridge, lower the gate, ignite the flammable moat and do whatever else you can to stop attacks before they start. This is the obvious first step and kind of hard to ignore: protect your site.

2. Detection

No matter how good your protection is the bad guys might find a way to hurt your site. And you need to know when an attack is happening.

The attack won't always be a full frontal assault that makes it painfully obvious your site has been hacked. Sometimes they're sneaky and bots will put a bunch of hidden code into your site. It's no good to have all kinds of protection but then not know when some malicious virus found a weak spot and broke through. Malicious bots and hackers may have already infiltrated your site. You'll never know without detection.

3. Recovery

Finally, you need a plan to get your site up and running again after it's been knocked down. These things happen. The best protection and detection strategies can still be foiled and you need to be prepared. Why worry about the worst-case scenario when a little preparation will have you covered? Plus, a good backup is important for other reasons besides security. We recommend backing up your site with BackupBuddy (which also handles restoring your site if something happens) so you're prepared for anything.

4 Best Security Practices

1. Keep It Current

One of the biggest security vulnerabilities in WordPress is old software. WordPress is updated fairly often and whenever there's a new security issue they roll out an update immediately. But that doesn't do you any good if you're not keeping your installation up to date. You also need to keep your themes and plugins up to date—they can have security issues as well.

Sometimes people put off updates for fear of breaking their site, but you'd rather break your site with an update than risk a break-in.

Also, just because a plugin is deactivated doesn't mean it's not a threat. You need to delete the plugin entirely.

2. Strong Passwords

Your security is only as good as your password. If you've got a simple password, you've got a simple site to hack. You need to use strong passwords. Your password should have numbers, capitals, special characters (@, #, *, etc.) and be long and unique. Your WordPress password can even include spaces and be a passphrase.

Don't use the same password in multiple places. Yes, remembering different passwords for different sites is tough, but a hacked site is worse.

3. Manage Users

Your own strong password is useless if another admin has a weak one. You need to manage your users. Not everybody needs admin access. The more people with admin access, the more chances to hack your site. Make sure you're only giving admin access to the people who truly need it. And make sure those few admins are following good security practices.

Remember to update or remove users when you have staff transitions.

4. Back It Up

If anything ever goes wrong with your site, you want to be able to get it back up quickly. That means you need a backup plan. In order for backup to work, it needs to be complete and automatic. Backing up your database isn't enough. That will save your content, but you'll still have to rebuild your entire site, including theme tweaks and plugin settings. And if your backup isn't automatic, you'll forget about it.

Get a powerful backup tool, such as BackupBuddy, to keep your site safely backed up and ready to be restored.

More Security Help

This should give you a good overview of security, but it's just a start. Security is a big deal and you need to take the right precautions.

That's why we've rolled out a new security plugin, iThemes Security, built by Chris Wiegman on top of his Better WP Security plugin that's had nearly 1.7 million downloads to date.

Learn more by watching the Introduction to WordPress Security webinar with Chris. He offers an overview of the Better WP Security plugin and what you can expect when we take over the plugin and roll out the new iThemes version.

Sign Up for WordPress Security Updates

Get WordPress security updates sent straight to your inbox by signing up for our WordPress Security Newsletter.

Subscribe