iThemes Security

WordPress Security

★ A POCKET GUIDE ★

2019 EDITION

Contents

Common WordPress Security Questions

Is WordPress Secure?

Absolutely! WordPress is the most popular content management system in the world, and it didn't get that way by not taking security seriously.

The truth is that the biggest WordPress security vulnerability is its *users.* Most WordPress hacks on the platform can be avoided with a little effort from site owners.

How Do I Make My Website 100% Secure?

Unfortunately, there is not a 100% guaranteed solution for securing WordPress. Good security is all 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.

My Website is Small. Do I Really Need to Worry About Security?

Even if you are the owner of a tiny website with low traffic, you still need to be proactive in securing your website.

The truth is your website or business doesn't have to be big to gain the attention of a would-be attacker.

Hackers still see an opportunity to use your site as a conduit to redirect some of your visitors to malicious sites, send out spam from your mail-server, spread viruses or even to mine Bitcoin. They will take anything they can get.

5 Tips to Secure Your WordPress Website

1. Limit Failed Login Attempts

Brute force attacks refer to the trial and error method used to discover username and password combinations in order to hack into a website. The brute force attack method exploits the simplest form of gaining access to a site: by trying to guess usernames and passwords, over and over again, until they're successful.

By default, WordPress doesn't limit failed login attempts. Without this limit, WordPress can be an easy target for brute force attacks.

Install a **WordPress security plugin** to limit the number of failed login attempts. The iThemes Security plugin's *Brute Force Protection* feature gives you the power to set the number of failed login attempts before a username or IP is locked out. A lockout will temporarily disable the attacker's ability to make login attempts. Once the attackers have been locked out three times, they will be banned from even viewing the site.

2. Use Strong Passwords

You should use a strong password for your WordPress admin password.

A strong password is a minimum of 12 characters, using a combination of alphanumeric and ASCII characters.

Using only lower case letters limits the pool of possible characters to 26, so it is vital to include alphanumeric, upper-case letters and common ASCII characters to increase the pool of characters needed to crack the password to 92.

For example, here are the estimated times to crack a password using a four-core i5 processor:

- a 7-character password will take *.29 milliseconds* to crack.
- an 8-character password will take *5 hours* to crack.
- a 9-character password will take *4 months* to crack.
- a 10-character password will take *1 decade* to crack
- a 12 character password will take *2 centuries* to crack.

3. Use Two-Factor Authentication

Two-factor authentication (2FA) adds a very strong layer of security by requiring an extra code along with your WordPress admin username and password in order to log in to your website.

Three Two-Factor Authentication Categories:
Two-factor authentication includes three categories of identity verification:

1. Something You *Know*. Do you remember filling out security questions when setting up your online mortgage account? Something like 'Who is your favorite teacher?' or 'What is your mother's maiden name?' These security questions provide a form of two-factor authentication by requiring answers you would only know.

2. Something You *Have*. This category of two-factor authentication requires you to have something physically in your possession—like your phone or a Yubikey—to prove your identity. For example, some two-factor authentication methods require a time-based code sent to a specific device via a two-factor app.

3. Something You *Are*. You may not know the name, but if you have a smartphone, you have probably used biometric authentication to log into your phone. Biometric authentication requires a unique biological characteristic to authenticate your login. If your phone has a fingerprint scanner or Face ID, you are using biometric authentication every time you unlock your phone.

Different Methods of Two-Factor Authentication

1. Email: With the email method of two-factor authentication, you will be supplied the code via an email notification. You'll used the code delivered to your inbox as your secondary code to login.

2. SMS Text Message. The SMS method of two-factor authentication delivers a code via an SMS text message to your mobile device. Although SMS text is one of the most common options for two-factor authentication, it is one of the least secure. The National Institute of Standards and Technology has even recommended deprecating the SMS method of two-factor authentication.

3. Mobile App: The mobile app option for two-factor authentication delivers a time-based one-time password or TOTP code to your mobile device using a two-factor authentication mobile app such as Authy or Google Authenticator.

Use a **WordPress security plugin** to add two-factor authentication to your WordPress admin login. iThemes Security Pro supports several two-factor authentication methods, including mobile app, email and backup codes.

4. Keep Your Software Updated

Running outdated software is actually the number one reason a WordPress website or blog gets hacked. Keeping your WordPress website up to date should be at the top of your list of security checklist. WordPress core and any theme or plugin you have installed on your website should always be running the latest version.

Version updates are not just for new features or bug fixes; they can also include security patches for known exploits. Bots will scour the internet looking for WordPress sites running outdated software with known WordPress vulnerabilities.

When you leave software out of date, you are giving a would be hacker the blueprint to bypass all other security measures you have added to the site.

Create an update schedule to be sure you are keeping everything up to date. You can use a tool like iThemes Sync to **manage multiple WordPress sites** from one dashboard so you can perform updates across multiple sites with one click. iThemes Sync will also send you an email notification if updates are available for your themes, plugins or WordPress core.

5. Backup Your Website

Unfortunately, your site can be hacked even if you follow the WordPress security best practices. If an attacker successfully compromises your site, having a backup will allow you to restore your site to a clean state.

Since WordPress doesn't have a built-in backup tool, having a solid backup strategy is your disaster insurance.

Using a **WordPress backup plugin** like BackupBuddy allows you to easily backup your whole website. Set up automated backup schedules so backups run every hour, day or week. Store you backup files in a secure, remote destination so you can access them if your website ever goes down.

A Basic WordPress Security Checklist

- [ ] 1. Limit Login Attempts
- [ ] 2. Use Strong Passwords
- [ ] 3. Use Two-Factor Authentication
- [ ] 4. Keep Your Software Updated
- [ ] 5. Backup Your Website

More WordPress Security Resources & Ebooks

5 Simple Rules for WordPress Login Security

What is 2 Factor Authentication and How Can It Be Useful?

Is My WordPress Site Hacked? 7 Signs of Infection

The Top 5 WordPress Security Myths Debunked

5 iThemes Security Tips to Secure Your WordPress Website

10 Tips for Securing a WordPress Website

A Guide to Brute Force Attacks EBOOK

A Guide to WordPress Security EBOOK

iThemes Security Setup Guide EBOOK