WordPromise
Expert Website Maintenance & Support™

A Pocket Guide
by WordPromise...

WordPress Security

Table of Contents

Common WordPress Security Questions 2

Tips to Secure Your WordPress Website 4

5 common Myths related to WordPress Security ... 10

Common WordPress Security Questions

Is WordPress Secure?

Absolutely! WordPress is the most popular content management system in the world, and it became so widespread by incorporating many features, and security is seriously one of them.

As a matter of fact, the biggest WordPress security vulnerability is its users. Most WordPress hacks on the platform can be avoided with a little effort and awareness from site owners.

How Do I Make My Website 100% Secure?

Unfortunately, there is not a 100% guaranteed solution for securing WordPress. Due to ever-changing technologies, it's impossible for anyone to guarantee 100% that your website will never be compromised in the future but it can definitely be secured from all known holes and leaks.

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 potential 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.

What if you lose my website data in case of something goes wrong during the audit?

We make a backup before any work is performed. So, your website data is always safe with us in case there is anything wrong during the audits.

Tips to Secure Your WordPress Website

1. Limit Failed Login Attempts

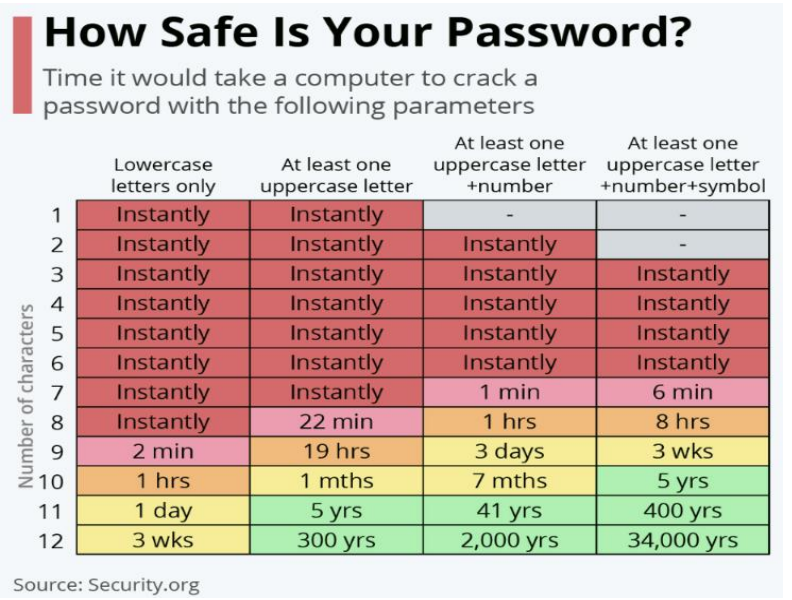
Brute force attacks refer to the trial-and-error method used to discover username and password combinations to hack into a website.

The brute force attack method exploits the simplest form of gaining access to a site: by trying to guess usernames and passwords, repeatedly, 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.

> *Protect your site against attackers that try to randomly guess login details to your site by using best suitable Security Plugins. Setup Brute Force Protection so that after several failed login attempts, a username or IP can be 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 can be banned from even viewing the site.*

2. Use Strong Passwords

You should always 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 special characters to increase the pool of characters needed to crack the password to 92. To make a password truly secure, even more characters or more than one uppercase letter, number or symbol can be added. A twelve-character password with one uppercase letter, one number and one symbol is almost unbreakable, taking a computer 34,000 years to crack.



3. Use Two-Factor Authentication

With WordPress Two-factor authentication (2FA), users are required to enter both a password AND a secondary code sent to a mobile device such as a smartphone or tablet. Both the password and the code are required to successfully log in to a user account.

Two-factor authentication adds an extra layer of WordPress security to verify it's you are logging in.

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.
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. Many security plugins support two-factor authentication methods, including mobile app, email, and backup codes.*

4. Keep Your Software Updated

Running outdated software is 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.

5. Backup Your Website

When it comes to security, we should be prepared for the worst. In worst scenario, 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. Your website backups can be scheduled and saved on at a secure storage. We can either save them on your server or any chosen cloud. In case a restoration is required, a backup will always be available to get restored.*

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

5 common Myths related to WordPress Security

Myth 1: You Should Hide Your /wp-admin or /wp-login URL (Also Known As Hide Backend)

The idea behind hiding the wp-admin is that hackers can't hack what they can't find. The truth is that most Hide Backend features are simply security through obscurity, which isn't a bullet-proof security strategy. While hiding your backend wp-admin URL can help to mitigate some of the attacks on your login, this approach won't stop all of them.

What expert recommends

Ultimately, the Hide Backend approach gives people a false sense of security, Instead, use more solid security measures like WordPress two-factor authentication and refuse compromised passwords.

Myth 2: You Should Hide your Theme Name and WordPress Version Number

The theory behind hiding your theme name and WP version is that if attackers have this information they will have the blueprint to break into your site. The problem with this myth is that there isn't an actual guy behind a keyboard looking for the perfect combination of theme and WordPress version number to attack. However, there are mindless bots that scour the internet looking for known vulnerabilities in the actual code running on your website, so hiding your theme name and WP version number won't protect you.

What expert recommends

Instead of worrying about hiding the theme or version number, keep your WordPress software up to date to ensure you have the latest security patches.

Myth 3: You Should Rename Your wp-content Directory

The wp-content directory contains your plugins, themes, and media uploads folder. That is a ton of good stuff and executable code all in one directory, so it's

understandable that people want to be proactive and secure this folder.

Unfortunately, it's a myth that changing the wp-content name will add an extra layer of security to the site. It won't.

Changing the name of the directory will not add any security to your site, but it can cause conflicts for plugins that have hardcoded /wp-content/ directory path.

What expert recommends

The only reason to be concerned about the content directory is if it contains a plugin or theme with a vulnerability. Again, keeping your themes and plugins up to date is the best way to know you are running secure software.

Myth 4: My Site Isn't Big Enough to Get Attention from Hackers

This WordPress security myth leaves a lot of sites vulnerable to attack. The truth is your site 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.

What expert recommends

Take active security measures to protect your website. For example, keep your themes, plugins & WordPress updated, install a trusted WordPress security plugin, use quality WordPress hosting and active WordPress two-factor authentication.

Myth 5: WordPress is an Insecure Platform

The most damaging WordPress security myth is that WordPress itself is insecure. This is simply not true. WordPress is the most popular content management systems 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 the site owners.

When a hacker uses a security hole it isn't a WordPress flaw, it is a user flaw.

WordPromise
Expert Website Maintenance & Support™

All-In-One
WordPress Maintenance Service
with 24/7 support

WordPress Security, Speed, Support and Maintenance Plan for Website Owners and agencies. WordPromise is much more than just a WordPress auditing service. It's the most powerful solution to maintain your website overall.

Get Started Now!

www.wordpromise.com