ITHEMES PRESENTS

A GUIDE TO WORDPRESS WEBSITE SECURITY

10 THINGS YOU NEED TO KNOW

Is WordPress *really* secure?

The answer to the question “is WordPress secure?” is *it depends*. WordPress itself is very secure as long as WordPress security best practices are followed.

On average, 30,000 new websites are hacked each day. WordPress websites can be an easy target for attacks because of plugin vulnerabilities, weak passwords and obsolete software.

Thanks to an active community and open-source development, WordPress continues to be an excellent choice for a wide variety of websites because of its ease of use, flexibility and continued development.

And by following a few simple WordPress security best practices, you can greatly reduce your vulnerability to attack.

What you'll learn in this guide:

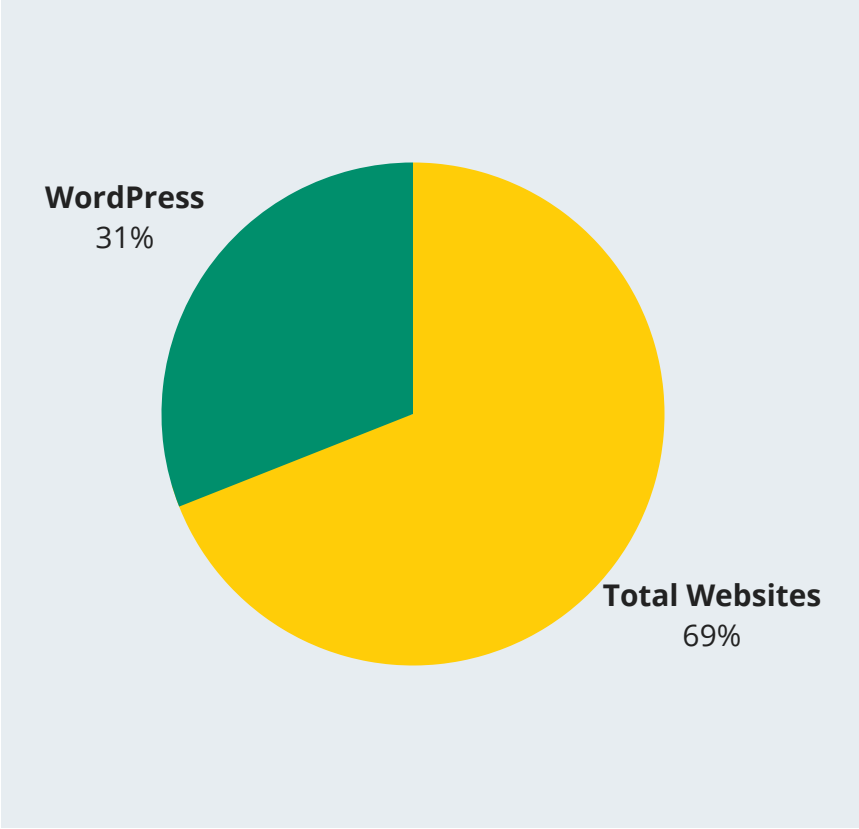
- The different types of WordPress security vulnerabilities
- Mistakes users and admins make
- WordPress security best practices
- Actions you can take today to reduce your risk of a hack or breach

1. Yes, WordPress websites are a target for hackers.

WordPress currently powers over 31% of all active websites on the internet, so it has become a target for hackers with malicious intent.

Why? If a hacker can find a way into one of the 75 million WordPress websites on the web, they can scan for other websites that are running similar insecure setups and hack those, too.

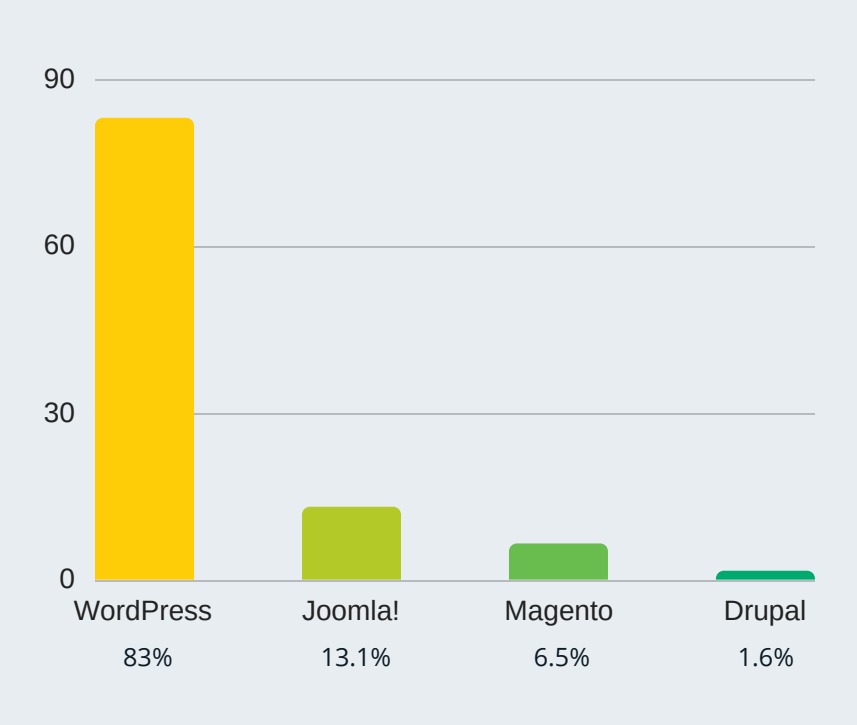
Unfortunately, vulnerabilities are inevitable because not all website owners and users are careful, thorough or conscious about their online security.



WordPress Usage Across the Internet
Source: W3TECHS, 2018

A recent report by Sucuri analyzed 34,371 infected websites to highlight hacking trends in compromised websites.

According to the report, WordPress infections rose from 74% in 2016 to 83% in 2017, so it's even more important to stay vigilant in your security efforts.



Infected Websites Platform Distribution
Source: Sucuri.net
Hacked Website Report 2017

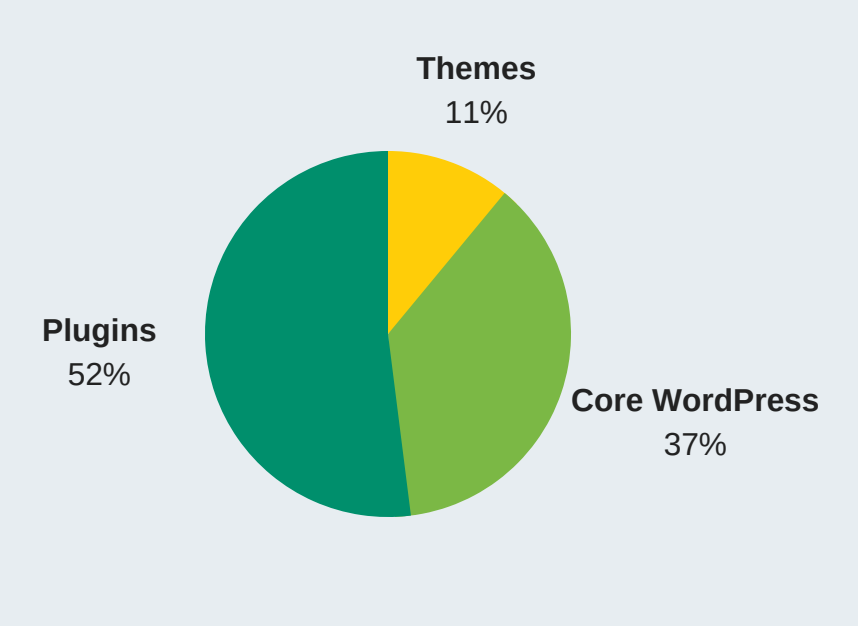
> "In most instances, the compromises which were analyzed had little, if anything, to do with the core of the CMS application itself but more with its **improper deployment, configuration and overall maintenance by the webmasters**."

2. WordPress has known security vulnerabilities.

According to a recent report by wpscan.org, WordPress has nearly 4,000 known security vulnerabilities.

Of known vulnerabilities:

- **52%** are from WordPress plugins
- **37%** are from core WordPress
- **11%** are from WordPress themes



Source: WPSCAN.ORG, 2018

As an industry standard, security vulnerabilities are disclosed to the public soon after they're discovered and only after a fix has been released to solve the issue. However, some websites continue to run insecure versions of plugins, themes and core WordPress despite the risk.

The Top 5 WordPress Security Issues

1. Brute Force Attacks

WordPress brute force attacks refer to the trial and error method of entering multiple username and password combinations over and over until a successful combination is discovered. The brute force attack method exploits the simplest way to get access to your website: Your WordPress login screen.

2. File Inclusion Exploits

File inclusion exploits occur when vulnerable code is used to load remote files that allow attackers to gain access to your WordPress website's wp-config.php file, one of the most important files in your WordPress installation.

3. SQL Injections

Your WordPress website uses a MySQL database to operate. SQL injections occur when an attacker gains access to your WordPress database and to all of your website's data. SQL injections can also be used to insert new data into your database, including links to malicious or spam websites.

4. Cross-Site Scripting

Cross-site scripting vulnerabilities are the most common vulnerability found in WordPress plugins. The basic mechanism works like this: an attacker finds a way to get a victim to load web pages with insecure javascript scripts.

5. Malware

Malware, short for malicious software, is code that is used to gain unauthorized access to a website to gather sensitive data. A hacked WordPress website usually means malware has been injected into your website's files.

A hacked website can be a headache for a number of reasons, and especially for your SEO rankings. Google and other search engines quickly blacklist websites that are discovered to be hosting malicious files or scripts. Some browsers, like Google Chrome and Firefox, will display warning signs to users or completely block the ability to view a suspicious website.

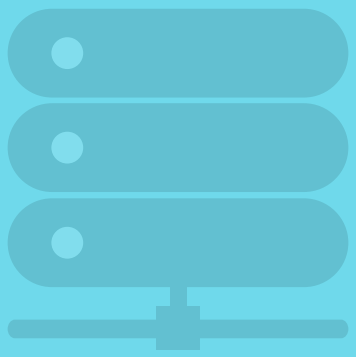
Types of Website Malware

Malware is a broad term for a family of malicious files that can vary depending on the attacker's intent. Several families of website malware have been identified:

Type of Malware	Description
Backdoor	Files used to reinfect and retain access to a website
Spam SEO	A compromise that targets a website's SEO
HackTool	Programs that may be used by hackers to attack computer systems and networks
Mailer	Spam generating tools designed to abuse server resources
Defacement	Hacks that leave a website's homepage unusable and promote unrelated subjects
Phishing	Attempts to trick users into sharing sensitive information (logins, credit card data, etc.)

Source: Sucuri.net

3. When running a WordPress website, your hosting matters.



Not all web hosts are created equal, and choosing one solely on the price alone can end up costing you way more in the long run.

Since the server where your website resides is also a target for attackers, using poor-quality shared hosting can make your site more vulnerable to being compromised. Shared hosting can also be a concern because multiple websites are stored on a single server. If one website is hacked, attackers may also gain access to other websites and their data.

While all hosts take precautions to secure their servers, not all are vigilant or implement the latest security measures to protect websites at the server level.

WordPress Hosting Tips:

- Choose a host with a solid security infrastructure. Security should be a primary selling point of their offering.
- Confirm access to 24/7 support.
- Research how the company handles hacked or blacklisted websites discovered on their servers.

WordPress Hosting Technical Specifications For Better Website Security

The following is a list of technical specifications to use as guidelines when choosing a hosting company for your WordPress website.

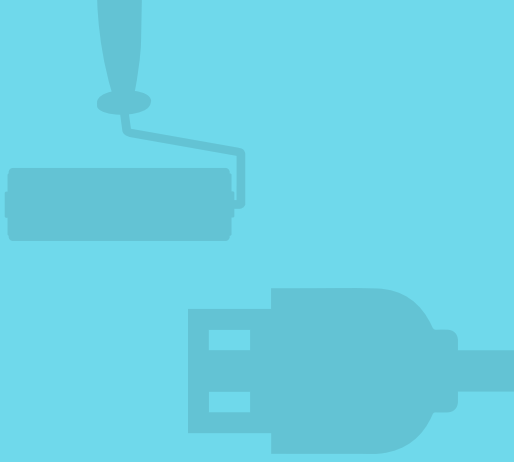
Recommended Security Guidelines for Your WordPress Hosting:

- [ ] Easy installation of SSL certificates*
- [ ] Active version management of server software
- [ ] Support for SFTP (not just FTP)
- [ ] Latest supported PHP version is at least 5.6, although 7.0+ is recommended.
- [ ] Support for TLS 1.2 and 1.3
- [ ] Firewall protection*
- [ ] Website log retention*
- [ ] Routine security audits
- [ ] Malicious activity detection*

** Note: Some hosting companies may offer these as separate services or add-ons with additional fees*

Need a WordPress hosting recommendation? Check out iThemes Hosting!

4. The plugins and themes you install matter.



Only install WordPress plugins and themes from trusted sources. Why? Unverified versions can contain malicious code.

Only install themes and plugins from WordPress.org, well-known commercial repositories or directly from reputable developers. It doesn't matter how much you lock down your WordPress website if you are the one installing malware.

If you find a premium WordPress plugin or theme that isn't being distributed on the developer's website or from a reputable marketplace, do your research before downloading it. Reach out to the developers to see if they are in any way affiliated with the website that is offering their product at a free or discounted price.

Tips for choosing plugins and themes:

- Only install themes and plugins from reputable websites.
- Avoid using "nulled" or bootleg versions of premium plugins or themes.
- Premium themes and plugins should always offer support option with your purchase.
- Make sure the plugin or theme has been updated recently.

5. Updates matter. A lot.

When your WordPress site is running outdated versions of plugins, themes or WordPress, you run the risk of having known exploits on your website.

WordPress runs on open source code and has a team specifically devoted to finding, identifying and fixing WordPress security issues that arise in the core code.
As security vulnerabilities are disclosed, fixes are immediately pushed out to patch any new security issues discovered in WordPress.

That's why keeping WordPress and all your themes and plugins updated to the latest version is a vital component of a successful security strategy.

WordPress Update tips:

- Update notifications are found in your WordPress dashboard in the top admin bar.
- Always backup your website before running major updates.
- Run updates as soon as a new version is available.

6. The quality of your password matters.

Your WordPress login is the most commonly attacked vulnerability because it provides the easiest access to your website's admin page.

Brute force attacks are the most common method of exploiting your WordPress login. Brute force attacks refer to a trial and error method used by hackers and bots to discover username and password combinations in order to gain entry to a website.

Brute force attacks can be effective because WordPress doesn't limit the number of failed login attempts someone can make. So be mindful of using a strong, complex password for your WordPress admin login.

Password Tips:

- Use a password with a combination of lower and uppercase letters, symbols and numbers.
- Never reuse passwords.
- Change your passwords often.
- Use a password manager like LastPass or 1Password to generate and store passwords.
- Turn on two-factor authentication for your WordPress login (see page 15).

7. If you don't have a backup plan in place, you're in trouble.

By default, WordPress doesn't have a built-in backup system. What are you doing to backup your website?

If the worst happens and your website is hacked, how do you get it back? How do you revert back to a clean version of your website? You'll need to have a backup—or a complete copy—of your website to restore it.

WordPress backups are critical to an overall security strategy. While your host may offer backups, not all are equipped to handle the complexities of a WordPress installation.

Make sure your backup solution handles backing up the database and *all* your website files and provides a way to restore it back.

WordPress backup tips:

- Set up backup schedules to automatically run.
- Store your backups safely off-site in a secure, remote destination.
- Run complete backups of your website's database and all files. A database backup alone isn't sufficient.
- Make sure your backup solution has restore functionality.

8. You can take steps to secure your website and minimize your risk.

Good news! Most WordPress security issues can be prevented if site owners simply follow WordPress security best practices.

Just like locking the doors of your house, investing in an alarm system and paying for insurance, your website should have security and safety measures in place. Better WordPress security can be achieved in just a few simple steps.

A Simple WordPress Security Checklist:

- [ ] 1. Choose quality hosting.
- [ ] 2. Secure your WordPress login with a strong password and two-factor authentication.
- [ ] 3. Keep your plugins, themes and WordPress software updated.
- [ ] 4. Uninstall and completely delete unused and abandoned plugins and themes.
- [ ] 5. Only use trusted software distributors for plugins and themes.
- [ ] 6. Have a WordPress backup plan in place.
- [ ] 7. Add SSL to your website.

9. Add two-factor authentication to your WordPress admin login.

One of the best ways to secure your WordPress site is with two-factor authentication.

Two-factor authentication adds an extra layer of protection to your WordPress login. In addition to your password, an additional time-sensitive code is required from another device such as your smartphone, in order to successfully login.

Two-factor authentication is one of the best ways to lock down your WordPress login and nearly completely minimizes the potential of successful brute force attacks.

While WordPress doesn't offer a built-in way to add two-factor authentication, you can use a plugin like iThemes Security to add the functionality.

WordPress Two-factor authentication tips:

- Use a WordPress security plugin such as iThemes Security Pro to add two-factor authentication to your website.
- Encourage privileged users such as admins to activate two-factor on their login.
- Mobile apps, rather than email or SMS text, are best for two-factor authentication. Try Google Authenticator or Authy for your two-factor method.

10. A WordPress security plugin can help.

Install a WordPress security plugin like iThemes Security Pro to add even more protection to your website.

Themes Security Pro works to lock down WordPress, fix common holes, stop automated attacks and strengthen user credentials.

You can download the free version of the plugin from WordPress.org or upgrade to iThemes Security Pro for even more security features like two-factor authentication, scheduled malware scans, user logging and more.

With a team of WordPress security experts behind you, you can have added peace of mind that your website is safe and secure.

iThemes Security setup tips:

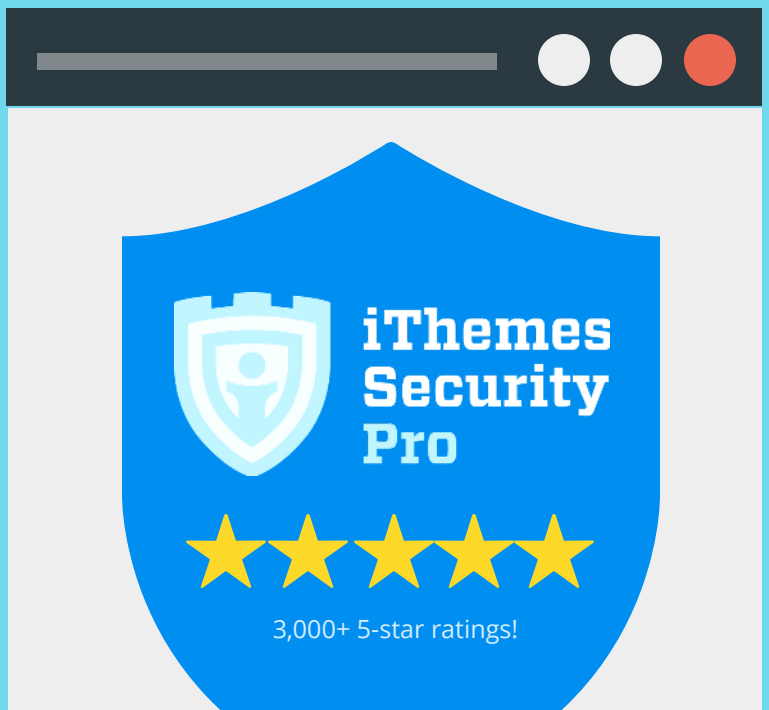
- After installation, use the one-click Security Check to activate the recommended features and settings.
- Enable two-factor authentication (Pro) and configure setup with the mobile app of your choice.
- Whitelist your IP
- Turn on email notifications to get security alerts and updates

SAVE 50% OFF ALL ITHEMES SECURITY PRO PLANS

SECURE & PROTECT WORDPRESS WITH A TRUSTED SECURITY PLUGIN

Use coupon code **SECUREWPNOW** to **save 50% off*** all iThemes Security Pro plans.

SAVE 50% OFF NOW



* Coupon good on any *new* iThemes Security Pro purchase. Can't be used to renew or extend and existing iThemes Security Pro subscription.