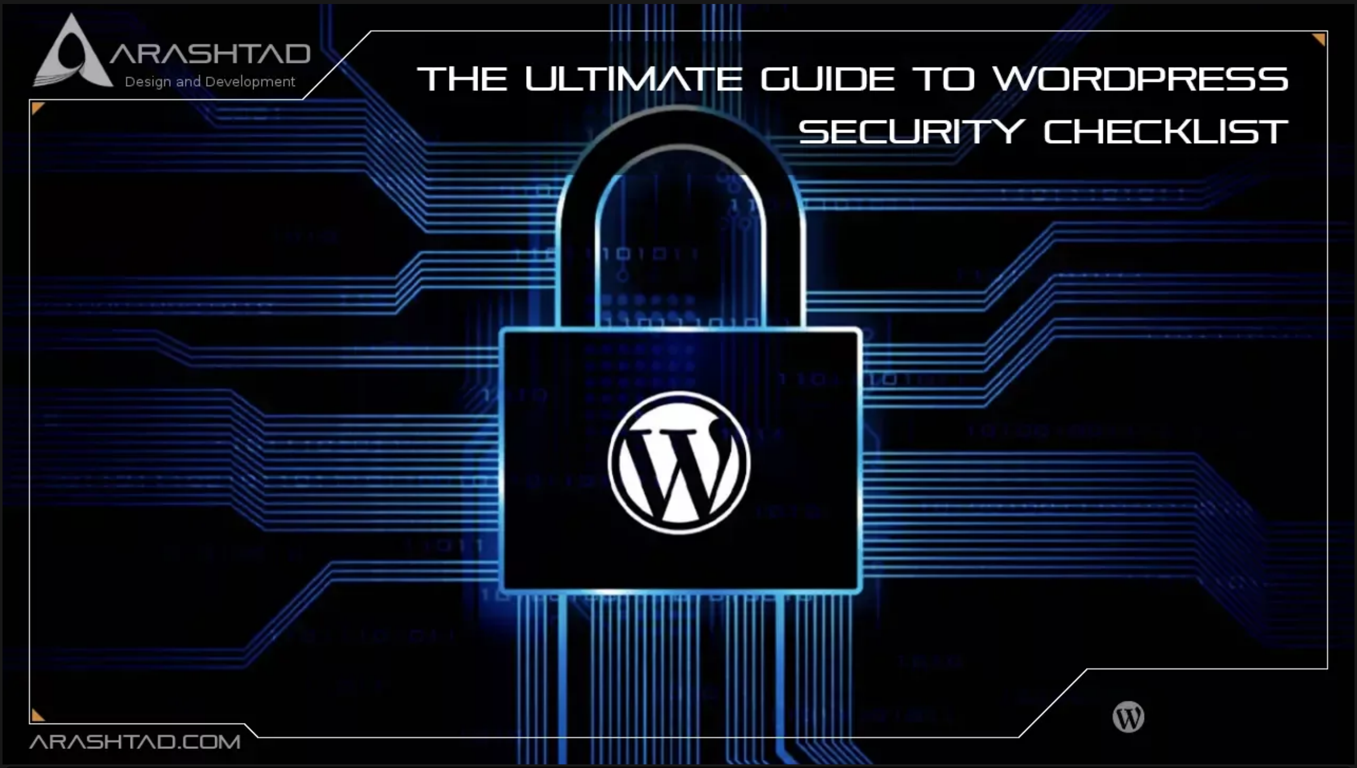
The Ultimate Guide to WordPress Security Checklist

No comments



In general, WordPress is a secure CMS, but open-source means it has a few critical vulnerabilities. Fortunately, you can secure your WordPress site by following these steps. We'll start by talking about WordPress security dangers and vulnerabilities. Then, we'll explain how to manage a secure, safe WordPress site.

Why WordPress Security Is Important?

In order for a website to be successful, it must be secure. This applies to businesses of all sizes, reputations, and industries. Here's why.

1. Keeps Your Information and Reputation Safe

Getting personal information about you or your site visitors from an attacker is a risk. Security breaches expose you to risks such as public data leaks, identity theft, ransomware, server crashes, and the list goes on. These events will negatively impact your business's reputation and cost you time, energy, and money.

2. Google Prefers Secure Websites

A higher ranking on the search engine results pages (SERPs) means more visibility, and visibility means more visitors. Luckily, making your site secure is one way to increase your chances of getting Google's attention. Because a secure website is searchable. WordPress security directly affects your visibility through Google searches (and other search engines) and has for some time.

Security is one of the simplest ways to boost your search rank. It is obvious that protecting your online properties is your top priority. Your website must ensure that your visitors are protected when using it.

3. Your Visitors Expect it

Your visitors expect that your site is secure. If we cannot provide this basic service from the start, we undermine their trust in us. By earning their trust, we ensure that our customers will return to our site. You need to ensure that your customers trust that their information will be handled and stored responsibly, whether it's their contact information, payment information (PCI compliance), or even a survey response.

Your customers won't know about your security measures if they work. But if they do, they will probably not return if they hear bad news.

The Best Way to Secure Your WordPress Site

WordPress security is all about following best practices. If you do so, you will have a lower chance of experiencing a problem, but there is no guarantee that you will never experience one. Many of these best practices apply to all websites (such as strong passwords, two-factor authentication, SSL, and firewalls), while others are tailored specifically to WordPress sites (such as using secure plugins and themes). In order to keep your site safe, you should adhere to as many best practices as possible. Let's start with the best basics.

WordPress Security Checklist

1. Make Sure Your Login Procedures Are Secure

In order to keep your website safe, you must secure your accounts against malicious login attempts. To do this, follow these steps:

Use Strong Passwords

Although people used to think flying cars would be available in the future, this year they are still using "123456" as a password. It is crucial that all users with access to your WordPress site use strong passwords to log in. In the event that one weak password is used, it could spell trouble for all other users. It may be a good idea to use one of our password managers to create strong passwords and keep track of them for you.

Enable Two-factor Authentication

Here's how to enable two-factor authentication in WordPress. Second-factor authentication (5FA) requires users to confirm their sign-on with a second device. It has proven to be one of the most effective ways to secure your login - and it works. When attackers attempt a brute force login, admin is likely the first username they plug in. If you've already created an administrator account with this name, create a new administrator account with a different name.

Limit Login Attempts

Your site is protected if you limit the number of times people can enter incorrect credentials. If people attempt to log in too many times, the CMS locks them out, preventing brute-force attacks from occurring. Depending on your hosting service and firewall, you might be able to disable this, but you can also use plugins such as Limit Login Attempts.

Add a Captcha

This security feature is common on many websites. They verify that the person logging in is a living person to add an extra layer of security.

Enable Auto-logout

Remember to log out, especially if you're using a public computer. Auto-logging prevents strangers from snooping on your account if you forget. Install the Inactive Logout plugin on your WordPress account to enable auto-logging.

2. Use Secure WordPress Hosting

you need to take a lot of factors into consideration when choosing a service to host your website, but security should always be at the forefront. Find out what steps the business takes to protect your information and recover quickly in case of an attack.

3. Make Sure WordPress Is Up-to-date

In order to avoid this issue, make sure that you regularly check for WordPress updates and install them as soon as possible to eliminate vulnerabilities. You may also need to update your plugins to be compatible with the latest version of WordPress. Back up your site and check that your plugins are compatible with the latest version of WordPress. Follow the WordPress website's update instructions after updating your plugins.

Image not found or type unknown

The Ultimate Guide to WordPress Security Checklist

4. Make Sure Your PHP Version Is Up-to-date

One of the most crucial steps you can take for WordPress security is updating to the latest PHP version. WordPress notifies you on your dashboard when an update is ready, so be sure to watch your dashboard. After that, you will be prompted to upgrade your PHP version via your hosting account. To upgrade, contact your web developer if you do not have access to your hosting account.

5. Add WordPress Security Plugins

When it comes to website security, you don't have to do it all by yourself: you can rely on a security plugin. We recommend installing one or more reputable security plugins. They scan your website for infiltration attempts, change the source files that might leave your site vulnerable, reset and restore the WordPress site, and prevent content theft like hotlinking for you. Make sure the plugin(s) you install, whether security-related or not, are well-established and legitimate.

6. Make Sure Your WordPress Theme Is Secure

As with not installing sketchy plugins on your website, resist using just any WordPress theme that looks good. This might make your site vulnerable to major problems. Choose a theme that adheres to WordPress standards to prevent vulnerabilities caused by WordPress themes. Check whether your current theme complies with WordPress' requirements by pasting the URL of your website (or the URL of any WordPress site or demo) into W3C's validator. You can search for a new theme in the official WordPress theme directory if your theme isn't compliant. All themes in this directory are safe to use with WordPress.

7. Enable SSL/HTTPS

An SSL (Secure Sockets Layer) connection encrypts data between your website and your visitor's web browsers, protecting traffic between your website and their computers from unwelcome interception. When you use CMS Hub, SSL is built right into the platform, so you're good to go. If you use WordPress, you can either manually enable SSL or use a dedicated SSL plugin. Besides boosting SEO, it also plays a part in how your visitors perceive your website.

Google Chrome will even warn users if the site they're visiting doesn't follow the SSL protocol, which reduces traffic to your website. Visit your WordPress site's homepage to see if it follows the SSL protocol. If it does, your connection is secured with SSL if it begins with “https://” (the “s” stands for “secure”). You will need to purchase an SSL certificate if your website's URL begins with “http://”.

8. Install a Firewall

It prevents unauthorized traffic from entering your system or network from the outside by sitting between the network that hosts your WordPress site and all other networks. By eliminating a direct connection between your network and other networks, they keep out malicious activity.

9. Take a Backup of Your Website

It's annoying to be hacked. It feels like a violation of your digital space, and if you lose all of your data, it's even more frustrating. However, you can avoid that from happening by backing up your site with WordPress and your hosting provider. You can gain access to your data if an attack (or any other incident) occurs. We recommend automatic backups as well.

10. Regularly Scan WordPress for Security Issues

Our last recommendation is to run routine check-ups on your site. This should be done at least once a month. Unfortunately, you won't need to do it yourself. You can use some WordPress security plugins.

Conclusion

In spite of the fact that cybercriminals are constantly evolving and learning new methods to exploit companies' online presence, security engineers continue to develop new methods to stop them. We're all caught up in this ever-shifting security cycle on the internet. Make sure your customers are safe, so they don't have to worry about anything.

Join Arashtad Community

Follow Arashtad on Social Media

We provide variety of content, products, services, tools, tutorials, etc. Each social profile according to its features and purpose can cover only one or few parts of our updates. We can not upload our videos on SoundCloud or provide our eBooks on Youtube. So, for not missing any high quality original content that we provide on various social networks, make sure you follow us on as many social networks as you're active in. You can find out Arashtad's profiles on different social media services.

Get Even Closer!

Did you know that only one universal Arashtad account makes you able to log into all Arashtad network at once? Creating an Arashtad account is free. Why not to try it? Also, we have regular updates on our newsletter and feed entries. Use all these benefitial free features to get more involved with the community and enjoy the many products, services, tools, tutorials, etc. that we provide frequently.

SIGN UP NEWSLETTER RSS FEED