7 Simple Steps to Secure Your WordPress Website

Struggling to secure your WordPress site??You’re not alone.Today, we are going to show you how to fortify your website easily.

With cyber threats on the rise, ensuring the safety of your WordPress website is non-negotiable WordPress, powering over 40% of the internet, is a prime target for hackers due to its widespread popularity.These seven steps are simple, effective, and can be implemented quickly.

In this blog we’ll cover everything from basic setups to strategic that adhere to wordpress security best practices.Get ready to make your website for maximum security measures.

Keep WordPress and Themes Updated

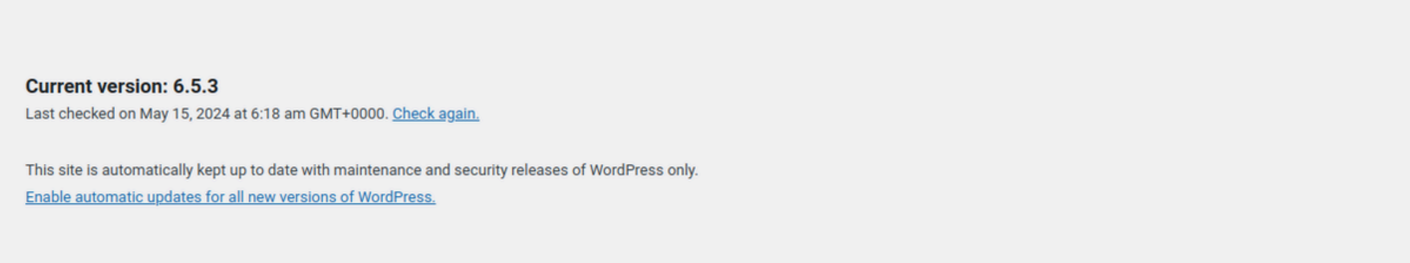
Maintaining an updated website is one of the simplest methods to provide your site an extra layer of security. To enhance security and speed, WordPress releases updates to its software on a regular basis. Also protecting your website from online threats are these improvements.

One of the easiest methods to increase the security of WordPress is to update your version of the software. Nevertheless, with around 50% of WordPress websites still using previous versions of the software, vulnerabilities exist.

An update is typically released by developers to address vulnerabilities they find in their code. Hackers are more likely to target your website the longer it remains on the out-of-date version.Themes and plugins that you may have on your website fall under this as well.

Keeping WordPress and all of its components up to date is the simplest approach to defend yourself against these vulnerabilities. This might be as easy as regularly viewing the dashboard to see what updates are available and executing them out.

Log into your WordPress admin area and select Dashboard → Updates from the menu panel on the left to see if you have the most recent version of WordPress installed. In the event that it indicates that your version is out of current, we advise updating it right away.



Current version: 6.5.3

Last checked on May 15, 2024 at 6:18 am GMT+0000. Check again.

This site is automatically kept up to date with maintenance and security releases of WordPress only.

Enable automatic updates for all new versions of WordPress.

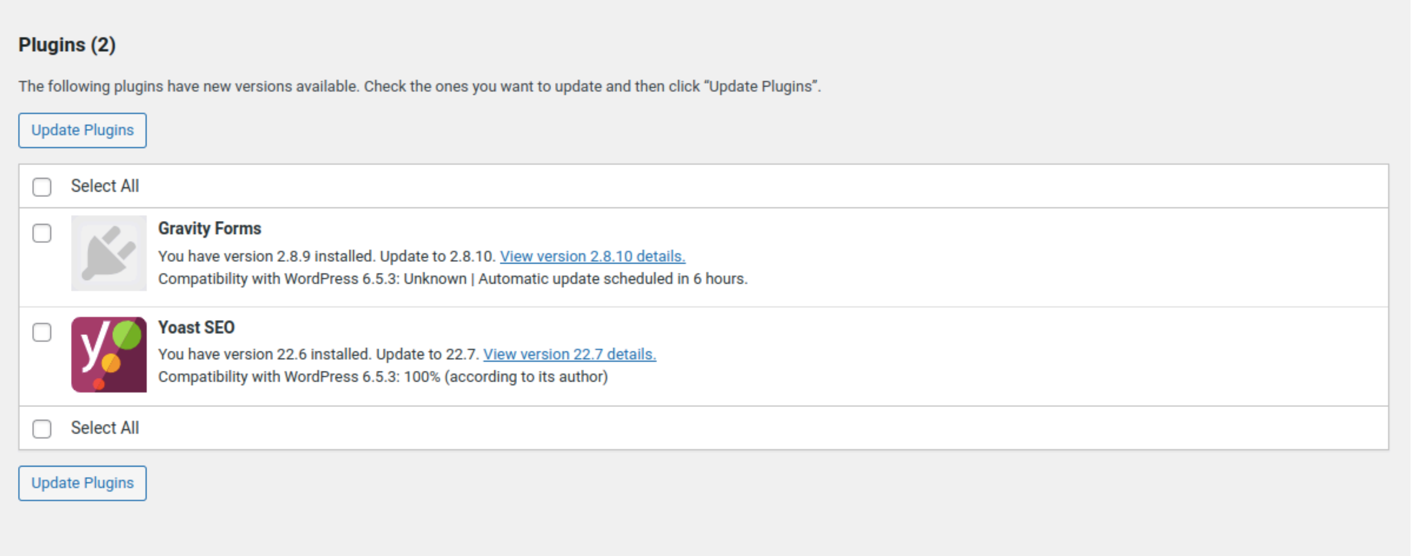
Updating the WordPress themes and plugins on your website is something else we suggest. The most recent version of the WordPress core software may not work with outdated themes and plugins, which might lead to security risks and mistakes.

Take the following actions to remove out-of-date plugins and themes:

To access Dashboard → Updates, navigate to your WordPress admin panel.

When you reach the Plugins and Themes sections, scroll down to see the list of themes and plugins that are prepared for upgrades. Take note that they can be modified individually or all of them at once.

Click Plugins Update.



Plugins (2)

The following plugins have new versions available. Check the ones you want to update and then click "Update Plugins".

☐ Select All

☐ **Gravity Forms**
You have version 2.8.9 installed. Update to 2.8.10. View version 2.8.10 details.
Compatibility with WordPress 6.5.3: Unknown | Automatic update scheduled in 6 hours.

☐ **Yoast SEO**
You have version 22.6 installed. Update to 22.7. View version 22.7 details.
Compatibility with WordPress 6.5.3: 100% (according to its author)

☐ Select All

Set Strong Passwords

The most frequent error made by users is to use usernames that are simple to figure out, such "test," "administrator," or "admin." This increases the likelihood of hacking attacks on your website. Additionally, this kind of attack is used by attackers to target WordPress websites with weak passwords.Make use of special passwords. Make secure usernames. Employ a password organizer.

Hackers are not new; they are familiar with all the most popular passwords and will try each one using the login "admin."Use online programs like 1Password and LastPass if you need assistance creating a strong password. To securely keep strong passwords, you may also make advantage of their password management services. You won't have to commit them to memory in this way. It will simplify site logins and assist you in creating and storing complicated credentials. particularly when working with a group!

As an alternative, do the following actions to establish a fresh WordPress administrator account and username:

Go to Users → Add New from your WordPress Dashboard.A new user should be made and given the Administrator position. Once you've added a password, click the Add New User button.

Your password should contain both capital and lowercase letters, numbers, and symbols. Additionally, since passwords with more characters are far more difficult to crack, we advise choosing more than 12.

Implement Security Plugins

WordPress security plugins frequently include an array of tools and features to assist you in safeguarding your website. Usually, these consist of:

Protection against spam

Protection against denial of service (DDoS) attacks

A firewall for web applications (WAF)

Malware removal and scanning

automated backups

To improve the security of your website, install popular WordPress security plugins like Wordfence, Sucuri, iThemes, NinjaScanner, or WPScan.Find out how these plugins actively protect your website from online dangers.

Utilize an SSL certificate to provide HTTPS encryption.

A data transmission protocol called Secure Sockets Layer (SSL) encrypts the information sent back and forth between a website and its users, making it more difficult for hackers to steal sensitive data.

With HTTPS, the safe version of HTTP, your website can load thanks to a secure sockets layer (SSL) certificate. The certificate points to the authenticity of your website and the encryption of browser-to-server communication.

Furthermore, SSL certificates improve WordPress websites' search engine optimization (SEO), which attracts more users.

It is simple to recognize websites that have an SSL certificate installed since they will utilize HTTPS rather than HTTP.

SSL is typically included in hosting packages. For instance, all of Hostinger's hosting packages come with a free Let's Encrypt SSL certificate.

Activate the SSL certificate on your WordPress website after installing it on your hosting account.

Simple SSL and SSL Insecure Content Fixer are two plugins that can handle the technical parts and quickly activate SSL. HTTP Strict Transport Security headers, which mandate the usage of HTTPS while accessing the website, may be enabled using the premium edition of Really Simple SSL.

After that, switch the URL of your website from HTTP to HTTPS. To alter its URL, locate the Site Address (URL) box and proceed to Settings → General.

Backup Your Site Regularly

The most crucial thing you can do to protect your data is probably to consistently backup your information. A complete backup of a website can be invaluable in the event of a security breach or other issue.Probably the simplest solution to deal with a compromised or malfunctioning website is to restore a recent backup. The likelihood of losing any important data decreases with the age of the backup.

After the website is back up and running, you may take the appropriate precautions to keep it safe from future assaults.For WordPress, there are several backup choices. In certain cases (usually when it’s a managed service), web providers include automatic backups in your hosting package.

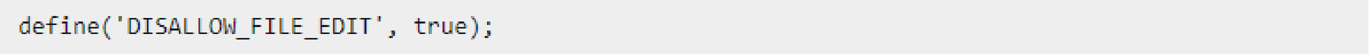
It’s advisable not to depend entirely on these backups, though. The backups may also be compromised if your server is, whether by a hack, host problem, or code error.

Disable File Editing

WordPress comes with an integrated file editor that makes modifying PHP files for WordPress simple. But if hackers take over, this feature can prove problematic.

You may alter the code of your website using these file editors without requiring an FTP connection. This method has the drawback that a hacker might wreck havoc on your website if they manage to get access to an account that is authorized to utilize these editors.

Because of this, some WordPress users would rather turn this function off. Disabling file editing in the wp-config.php file requires adding the following line of code:



```
define('DISALLOW_FILE_EDIT', true);
```

Take in consideration that some plugins and themes will prevent file modification by default. You’re probably using one of these programs if you can’t see the file or theme editors on the dashboard.Using an FTP program or the File Manager on your hosting provider, erase the old code from wp-config.php to reactivate this function on your WordPress website.

Monitor User Activity

Track activity in your admin area to find any unwanted or harmful behaviors that might endanger your website. For WordPress websites with several writers or users, we suggest using this strategy. This is due to people accidentally changing settings such as themes or plugin configurations.

You may determine who made those unpleasant modifications and whether someone unauthorized gained access to your WordPress website by keeping an eye on their activity.

Activity logs are instruments for tracking certain occurrences and recording their times. You have access to that record, which shows you who did what and when. This makes it possible for you to identify situations and behaviors that can compromise the security of your website.

WordPress does not come with this functionality by default, but you may add it using a plugin.

The other easiest way to track user activity is by using a WordPress plugin such as:

WordPress Activity Log: tracks modifications to various sections of a website, such as pages, themes, plugins, and articles. Additionally, it records changes made to any file as well as newly inserted and removed files.

Simple History records all action associated with several third-party plugins, including Jetpack, WP Crontrol, and Beaver Builder, in addition to the activity log on the WordPress admin.

Conclusion

In conclusion, safeguarding your WordPress website is achievable by following these 7 simple steps. By keeping WordPress updated, enforcing strong passwords and user permissions,

implementing security plugins, enabling HTTPS, backing up your site regularly, disabling file editing, and monitoring activity, you can significantly reduce the risk of cyber threats.
At Techspawn, we understand the importance of web optimization and security. As we are one of the best wordpress development company check out our resources for more web performance improvement tips and insights. Remember, maintaining these above mentioned security practices is key to the long-term success and protection of your website. Stay proactive, stay secure!