Introduction.

TechWays hosts our platform with WP Engine - a US based hosting company that is very focused on security.

WP Engine is the world's leading WordPress digital experience platform that gives companies of all sizes the agility, performance, intelligence, and integrations they need to drive their business forward faster. WP Engine's combination of tech innovation and an award-winning team of WordPress experts are trusted by over 70,000 companies across 130 countries to provide counsel and support, helping brands create world-class digital experiences.

The below information is an excerpt from the WP Engine data protection service manual:

WP Engine supports businesses of all shapes and sizes in our secure server environment. We understand how important security is to the users and websites we support. With this in mind, WP Engine adheres to strong security guidelines and principles to protect your site from the most common attack vectors. In this document we will discuss the actions WP Engine and WordPress take to help protect your website, as well as best practices for security and hardening within your own team.

Database containment and Filesystem security

LIMITED PRIVILEGES TO PREVENT UNAUTHORIZED DISK WRITES

If an insecure version of a plugin or theme is installed on your website, it is possible that code could trigger the site to write new files with more malicious code on your site. WP Engine helps limit damages by limiting disk write privileges, allowing only authorized users to write files on your server.

DATABASE CONTAINMENT PREVENTS SPREAD OF DAMAGES

Containment is a common security principle that states, should one entity become compromised, damages are limited by logically separating environments and users. WP Engine manages database containment by creating and managing separate database users for each of your WP Engine sites. This means if one of your sites contains vulnerable code, any resulting damages will not extend to your other sites.

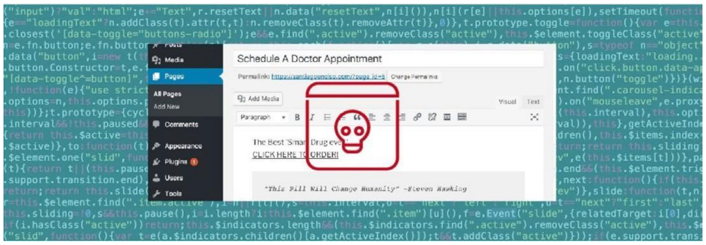
CONFIGURATION FILE PROTECTION AGAINST UNAUTHORIZED CHANGES

Some of the most important settings on your site are managed in a small handful of configuration files. WP Engine automatically protects these files so they cannot be accessed by the outside world. We also protect your site's uploads folder to ensure unauthorized file types are not recognized.

Behaviors WP Engine automatically blocks

INTELLIGENT BRUTE FORCE PREVENTION AND BLACKLISTING

Attackers often try to unintelligently "brute force" your login page by trying thousands of username and password combinations until they find the magic pair to login to your website. WP Engine detects when bots make fake requests for the login page and automatically returns an empty response.



AUTOMATIC BLOCKING OF SPAMBOTS AND BAD ACTORS

Bots are a common problem that often go unseen. A spambot often doesn't load your site's JavaScript files, meaning they aren't detected by Google Analytics, but they are present all the same. These bots can overwhelm your server's resources in a number of ways, or simply send spam emails, comments, and form entries. WP Engine automatically identifies and blocks bots with bad behavior to protect your site and server environment.

AUTOMATIC DETECTION AND BLOCKING OF COMMON ATTACKS

The XMLRPC.php file on your website exists to help apps and remote posting services create new posts. However, attackers often know of this file and send targeted attacks to it with fake requests. WP Engine blocks XMLRPC attacks by automatically detecting users trying to exploit this file.

Encryption on the WP Engine Platform

ENCRYPTION OF USER DATA

Another common area of concern is protecting the data users enter on your website. Interactive websites often feature contact forms, cart and checkout forms, or comment forms for posts. WP Engine offers free Let's Encrypt SSL Certificates. Protecting your site with an SSL certificate not only gives you a green lock in the URL bar, it also encrypts the data users input on your website.

FILE TRANSFER ENCRYPTION

Users may also be concerned about the security of their files when transferring them to and from their site. WP Engine enforces secured file transfers by requiring the use of SFTP. This means your files are safe and encrypted as they are transported, protecting them from any attackers who could be "listening" on the network.

About WP Engine.

WP Engine is the world's leading WordPress digital experience platform that gives companies of all sizes the agility, performance, intelligence, and integrations they need to drive their business forward faster. WP Engine's combination of tech innovation and an award-winning team of WordPress experts are trusted by over 70,000 companies across 130 countries to provide counsel and support, helping brands create world-class digital experiences.

Founded in 2010, WP Engine is headquartered in Austin, Texas, and has offices in San Francisco, California; San Antonio, Texas; London, England; Limerick, Ireland, and Brisbane, Australia.

www.wpengine.com