WP engine®

HOW TO CONVINCE YOUR CLIENTS WORDPRESS IS MORE SECURE THAN THEY THINK

WHITE PAPER

You've probably heard or read about it at one point or another — "WordPress is not secure." Fearful of potentially falling victim to malicious behavior, you might be dealing with a client who is rejecting WordPress as a suitable CMS. But the truth is, WordPress core is one of the most secure publishing and web development platforms you can choose to develop a site on.

What most people don't realize though, is that WordPress is not a set it and forget it system.

Security isn't about setting and forgetting. Rather, it's about taking every measure you can to harden your website to prevent it from being hacked. It's not just up to WordPress to implement security for you either. Unless you're using WordPress.com (which hosts your site itself and takes care of site maintenance), using WordPress.org means YOU are responsible for site maintenance, including security.

While WordPress already does a lot to harden its core, there's a shared responsibility between **you**, your **hosting infrastructure**, and **WordPress** to be vigilant about enforcing security best practices.

So, if your client is rejecting WordPress due to security concerns, here are a few ways to convince them that WordPress is actually more bulletproof than they might realize.

The No.1 culprit of a hacked WordPress website is due to an outdated extension or outdated core.

Hacking is newsworthy

WordPress wasn't always as secure as it is now. Back in 2009, when WordPress was on the brink of massive popularity, the CMS contained a number of security vectors that were exploited and picked up by the news. The platform received extreme criticism, in which was really the community's way of saying that WordPress needed to up its game and become more bulletproof.

These security concerns were addressed in version 2.8, following a string of security patches to strengthen the WordPress codebase.

While security was on the shaky end then, today WordPress is quite secure. Yet, because WordPress makes up such a huge chunk of the internet (28 percent and rising; 1.2 billion downloads), if a hacker is scouring the web to cause trouble, there's at least a quarter chance they'll land on a WordPress website.

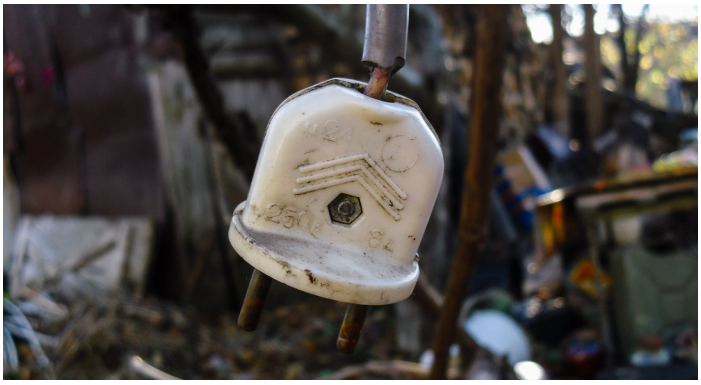
As such, these security exploits are publicized when any high-profile attack occurs. This gives WordPress a reputation for being less secure than comparable CMSs, like Drupal and Joomla. However, this is completely inaccurate.

The reality is, WordPress is secure enough for millions of end users and a number of Fortune 500 companies to trust their online business with.

CMSs like Drupal and Joomla aren't targeted as much, simply because they aren't as widely used as WordPress. While WordPress powers over half (52 percent) of all CMSs on the web, Drupal powers a mere **two percent** and Joomla only **six percent** of the CMS market.

So, when WordPress does get hacked, it's commonly covered by media outlets and the news. But what many people don't realize brings us to the next point.

Most security exploits are a result of an outdated component.



Most security attacks on WordPress occur through an outdated theme, plugin, or through WordPress core. Of all the high profile exploits in recent years, each attack has targeted vulnerabilities that could have been avoided with a simple update.

Therefore, it is not the fault of WordPress when these breaches occur in outdated components, like plugins, themes, and core.

It's your duty to update plugins, themes, and WordPress core accordingly.

While digital experience platforms like WP Engine run automatic updates to core for you, it's still your responsibility to update all plugins and themes to ensure they contain the latest security patches.

Also, it's up to you as an agency to familiarize and educate your clients regarding plugin and theme best practices. While free plugins and themes are awesome, when browsing the plugin repository, make sure the plugin/theme has been updated recently and works with the latest version of WordPress. If you activate a plugin/theme that's more than a year old, you could be potentially opening up a portal for hackers because the extension will most likely not have been patched with the latest security update.

Premium plugins and themes are less likely to contain security vulnerabilities because they are monitored and updated more regularly. That's one benefit of paying for a premium component — you won't have to worry about the author going astray and neglecting to keep the theme/plugin up to par with the latest security standards. However, do not try to pirate premium themes and plugins; this is a bad idea because they most likely won't contain the latest security scripts.

There are many security vendors working quickly to detect and patch vulnerabilities.

In terms of security, no system is perfect.

According to WordPress.org, "Security is about risk reduction, not risk elimination, and risk will never be zero."

This is true not just for WordPress, but for any system. That's why, in addition to the WordPress core team, many third-party security providers work endlessly to detect and fix vulnerabilities.

Even against the most secure systems, hackers can still find a way in if you don't take the right precautions; Image source: "Mission Impossible"

The open source nature of WordPress means that anyone can contribute to detecting security vulnerabilities, meaning faster fixes.

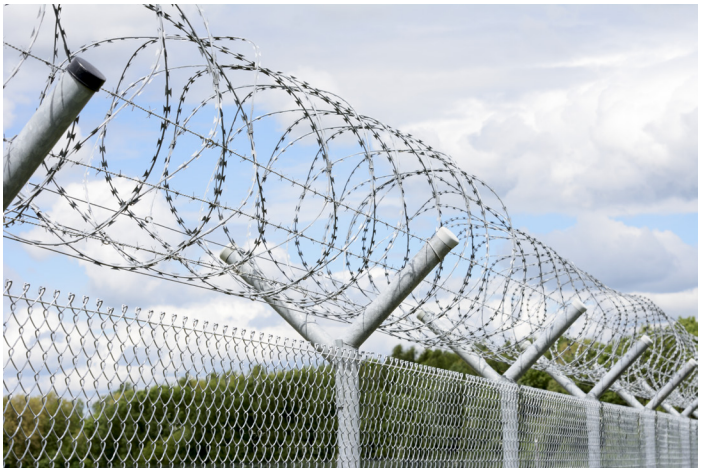
For instance, your client might have heard about a recent WordPress security breach through the REST API (introduced in version 4.7.0) where 1.5 million-plus pages running that specific version were defaced. Various security vendors detected the vulnerability and immediately reported it to WordPress to build an update.

If your client's enterprise site contains highly sensitive information, or they're just worried about this happening to them, there's no

way it could if they've invested in services that automatically run WordPress updates for you. We were notified of this breach by WordPress and immediately started issuing patches across the platform that contained the latest security patches so that nobody was affected.

Just remember...

WordPress is as secure as you want it to be.



If you want your site to be shielded with layers upon layers of security shields, then you can. But laxity in security will only result in exposure to vulnerabilities.

It's your duty and your client's duty to take additional measures to harden the security of the WordPress site you've built. With the help of digital experience partners, like WP Engine, security is taken to the next level.

To avoid a treacherous site invasion, there are some additional security measures you can (and should) take to harden the security of your WordPress site.

Enforce Strong Passwords

This is the most basic of security measures you should be taking. If a hacker decides to run a brute-force automated script, an easy-to-guess password will make it more accessible for them to crack the code. Instead, use a **strong password generator** to make sure your password is secure enough. You can also use a plugin like Force Strong Passwords to enforce strong passwords for other users on your site or with WordPress Multisite. (If you're a WP Engine customer, we automatically install this plugin for you.)

Use 2FA (Two-Factor Authentication)

Enabling 2FA adds an extra layer of security to your login credentials. 2FA works by requiring a second factor of information that only you can give, like a code sent to your phone to verify your activity on a specific computer. There are a number of WordPress plugins that can help with adding 2FA to your site.

Use SSL For Data Security

SSL (secure sockets layer) encrypts all information submitted to your site. This means hackers won't be able to see or intercept the data your users share on your site (like credit card info). While WordPress doesn't come with automatic SSL, many hosting providers offer Let's Encrypt, which provides free SSL certificates to place your site on HTTPS.

Let's Encrypt

Since Google has started issuing "Not Secure" warnings for pages not secured with HTTPS, it's critical that your client makes this transition to HTTPS if they haven't already.

User Role Access

Be cautious about who you give "Admin" privileges to. For instance, if someone leaves the company, you'll want to reassign their user role to "Subscriber" or a similar option. While WordPress out of the box is restrictive on customizing who can do what, you can install a user role plugin to expand user role permissions.

Getting Your Clients In The Right Mindset For WordPress Security

By now, your client hopefully feels more comfortable with WordPress. While WordPress is a common target, it's not easy to get hacked if you're taking the right precautions.

As an agency, you might not have time to implement every security measure. While you can educate your client on security best practices (like updating core components, enforcing strong passwords, etc.), they'll feel even more secure knowing their site is placed on a digital experience platform that provides a strong security environment.

Here are just a few benefits of WP Engine's security environment, built specifically for WordPress sites:

Managed Patching and Updates

Remember, when kept up-to-date, WordPress core is actually quite secure. You won't have to worry about updating your WordPress core with the latest security patches — we automatically do this for you (however you will have to be attentive with updating themes and plugins on your end).

Real-time Security Threat Detection

Our environment blocks millions of attacks per day so that your client's site is blocked from brute-force or DDoS attacks before they happen. Our proprietary system dynamically detects and blocks malicious behavior such as JavaScript/SQL-injection attacks and even more sophisticated attacks such as XML-RPC attacks.

Enterprise-Grade Infrastructure

From bloggers to Fortune 500 companies, more than 60,000-plus customers have entrusted WP Engine by placing their site on our secure technology stack. Shared plans are separated from other customers at the kernel and filesystem level, and enterprise plans run in dedicated environments not shared with other WP Engine customers.

In addition, we run a combination of firewalls to protect you from outside attacks. We also offer network analysis monitoring tools to guard against any malicious behavior within the network.

Finely Tuned Technology Stack

Proper server configuration is vital to securing your web environment. Our software stack includes provisions to ensure optimal WordPress performance, including disk write limitations and protection against scripts known to contain vulnerabilities. We also implement PHP tuning to disallow dangerous or insecure commands.

Security Audits and Code Reviews

We conduct periodic code reviews and security audits of all our internal environments and processes. Also, WP Engine partners with third-party, independent security firms to ensure best practice security measures are always in place. Lastly, we conduct frequent, proactive vulnerability scans and perform penetration testing, and we allow our customers to do the same if they choose.

To learn more about WP Engine's security environment, you are welcome to contact us.

Keeping your site secure is just one of the many features WP Engine's digital experience platform offers. To learn more about our enterprise-grade services, see wpengine.com/our-difference.

About WP Engine

WP Engine powers amazing digital experiences for websites and applications built on WordPress. The company's premium managed hosting platform provides the performance, reliability and security required by the biggest brands in the world, while remaining affordable and intuitive enough for smaller businesses and individuals. Companies of all sizes rely on WP Engine's award-winning customer service team to quickly solve technical problems and create a world-class customer experience. Founded in 2010, WP Engine is headquartered in Austin, Texas and has offices in Limerick, Ireland, San Francisco, California, San Antonio, Texas, and London, England.

www.wpengine.com

WP Engine 504 Lavaca Street, Suite 1000, Austin, Texas 78701 info@wpengine.com wpengine.com