15 WAYS TO HARDEN THE SECURITY OF YOUR WORDPRESS SITE

WHITE PAPER

"Security is not about perfectly secure systems. Such a thing might well be impractical, or impossible to find and/or maintain. What security is though is risk reduction, not risk elimination. It's about employing all the appropriate controls available to you, within reason, that allow you to improve your overall posture reducing the odds of making yourself a target, subsequently getting hacked." — codex.wordpress.org

One of the top concerns for WordPress site owners and prospects is website security. WordPress currently powers 27 percent of all websites on the internet, making it a popular target for hackers. Yet, even though WordPress is a common target, that doesn't mean your site has to fall victim to malicious behavior.

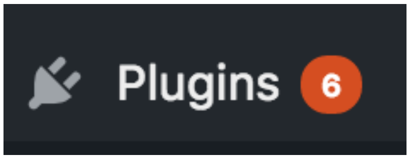
While no system is 100 percent hack-proof, there are certain measures you can take to prevent a hacked WordPress site. To reduce your chances of being affected by a disastrous brute-force or DDoS attack, read below for the most important WordPress security tasks you should implement to become more proactive against potential threats.

1 Keeping Software Up To Date

The most common culprit of a hacked WordPress website is due to an outdated component. Outdated **plugins**, **themes**, and **core** open the portal for a potentially hacked site. When left un-updated, these outdated files are traceable and make your site a target by outside intruders.

In fact, in one study 54 percent of reported WordPress security vulnerabilities belonged to outdated WordPress plugins. Outdated WordPress core accounted for 37 percent of vulnerabilities and outdated WordPress themes accounted for 11 percent of vulnerabilities.

Ensuring your WordPress site is up-to-date is simple. When you see an orange notification in your WordPress dashboard next to plugins, themes, or a notification to upgrade WordPress, **update ASAP!**



If your site is hosted with WP Engine, we'll automatically run these WordPress core updates for you, although you will need to be attentive with themes and plugins to update them accordingly to protect your website from malware.

How to configure automatic updates:

If you'd rather not do it manually, you can configure automatic updates. To auto-upgrade WordPress core, insert this code into your wp-config.php file:

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

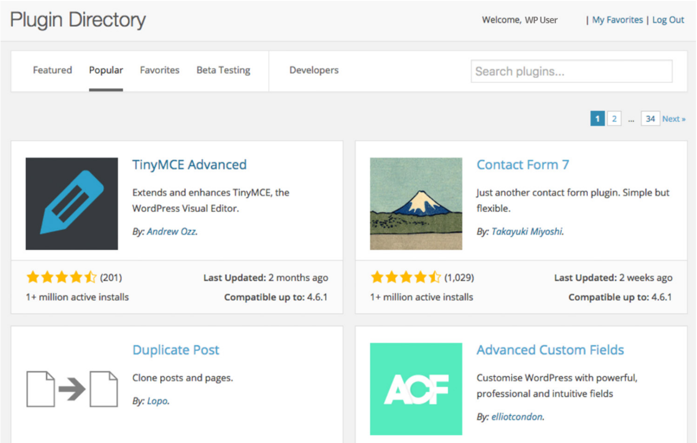
For plugins, use:

```
add_filter( 'auto_update_plugin', '__return_true' );
```

For themes, use:

```
add_filter( 'auto_update_theme', '__return_true' );
```

2 Avoid Installing Untrusted WordPress Plugins And Themes



TinyMCE Advanced

Extends and enhances TinyMCE, the WordPress Visual Editor.

By: Andrew Ozz.

★★★★☆ (201) Last Updated: 2 months ago

1+ million active installs Compatible up to: 4.6.1

Contact Form 7

Just another contact form plugin. Simple but flexible.

By: Takayuki Miyoshi.

★★★★☆ (1,029) Last Updated: 2 weeks ago

1+ million active installs Compatible up to: 4.6.1

Duplicate Post

Clone posts and pages.

By: Lopo.

Advanced Custom Fields

Customise WordPress with powerful, professional and intuitive fields

By: elliotcondon.

On WordPress.org the "Popular" and "Featured" sections of the plugin directory are a good place to start when looking for trusted, secure plugins.

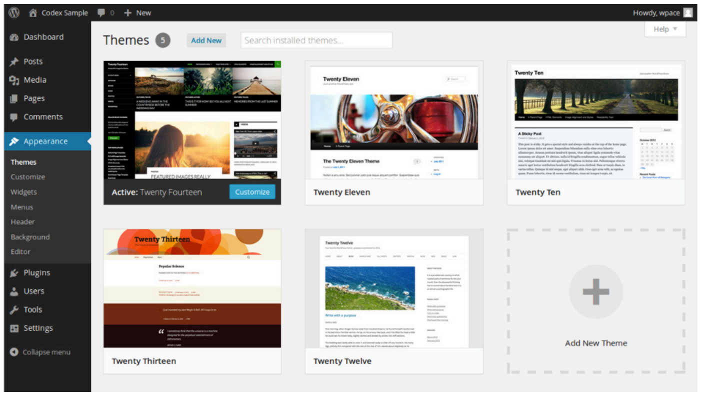
To detect if a theme or plugin can be trusted or not, first, read its ratings. There you can find clues to whether there have been security breaches or issues in the past, like buggy updates.

You'll also want to check to see when a plugin/theme was last updated. If a plugin or theme hasn't received an update in some time (say years), then the inactiveness in that plugin/theme is a sign you should look somewhere else.

In addition, analyzing a plugin or theme's popularity is another way to better ensure you aren't installing malicious code into your WordPress site.

A plugin or theme that's widely popular isn't necessarily less likely to be targeted by hackers, but is more likely to be updated with security patches regularly due to its wide use.

3 Don't Forget To Remove Unused Plugins And Themes



Over time, your WordPress site will require some housekeeping.

As you start to accumulate themes and plugins, you should go through and dispose of the ones you no longer use. Getting rid of unnecessary clutter is likely to make your site run faster, as well as remove security vulnerabilities from stagnant or outdated add-ons that you might have forgotten about.

If using WordPress multisite, try using a plugin like Plugin Activation Status to perform a plugin audit and detect unused plugins across all sites in the multisite network.

See the codex on WordPress housekeeping for more information on how to remove unused plugins and themes.

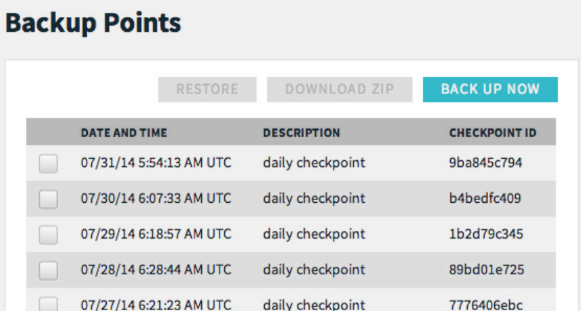
4 Install A WordPress Security Plugin

Installing a WordPress security plugin is a no-brainer when it comes to enhancing the security of your site. To become more proactive against security threats, try installing a plugin like one of these to minimize any security vulnerabilities.

(If you're a WP Engine customer, be sure to check our disallowed plugins list as there are a few WordPress security plugins we already install for you.)

- Sucuri Security
- iThemes Security
- Bulletproof Security

5 Regularly Backup Your WordPress Site



	DATE AND TIME	DESCRIPTION	CHECKPOINT ID
□	07/31/14 5:54:13 AM UTC	daily checkpoint	9ba845c794
□	07/30/14 6:07:33 AM UTC	daily checkpoint	b4bedfc409
□	07/29/14 6:18:57 AM UTC	daily checkpoint	1b2d79c345
□	07/28/14 6:28:44 AM UTC	daily checkpoint	89bd01e725
□	07/27/14 6:21:23 AM UTC	daily checkpoint	7776406ebc

WP Engine offers daily site backups and one-click restore so you can rest at ease knowing your work is safe.

Even if you take the above security precautions (and the ones listed after) you should always backup your WordPress site.

Backing up your WordPress site is fairly easy to do, as given these instructions by WordPress. Or you can try a plugin like BackupBuddy.

If it's something you'd rather not have to worry about, WP Engine conducts automatic backups for you every day. That way you can rollback to your original site *should* you ever lose your site due to an outside invasion.

6 Enforce Strong Passwords And Usernames

We're all guilty of using a password that's simple to remember. But using an easy password, say one that contains your birth year, makes it easier for hackers to crack the code using brute force automated scripts, which continuously try to guess your password and username over and over.

To ensure your password is strong and secure enough, use a tool like Strong Password Generator or Strong Random Password Generator.

You should also force other users on your site to use a strong password. You can use a WordPress plugin like Force Strong Passwords to enforce strong passwords. (If you're a WP Engine customer, we automatically install this plugin for you.)

7 Use Two-Factor Authentication (2FA)

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.

That way it's harder for an intruder to steal your information if they login through a different device.

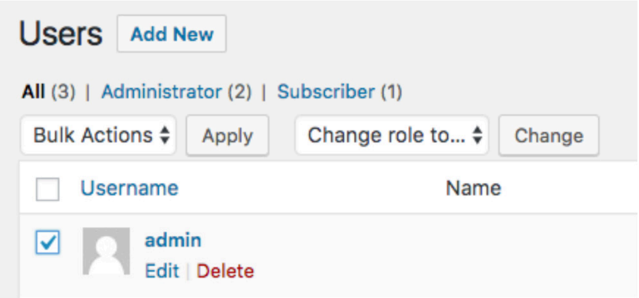
Here are some WordPress plugins you can use for 2FA:

- Google Authenticator
- Duo Two-Factor Authentication
- Two Factor Authentication
- Clef
- Authy
- Rubion 2FA

Graphic Source: Google Support

(WP Engine customers can implement two-factor authentication through the User Portal.)

8 Change Or Omit The "Admin" Username


Users Add New

All (3) | Administrator (2) | Subscriber (1)

Bulk Actions ⇕ Apply Change role to... ⇕ Change

□ Username Name

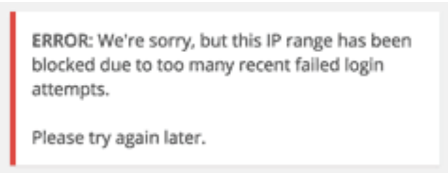
☑ admin
Edit | Delete

By default, WordPress gives the primary domain account the username "admin." Leaving the username as "admin" is an instant security threat to your site. If an attacker wants to crack the code, half of the puzzle is already solved and all that's left to guess is your password.

Removing or changing the "admin" username is the next step to improving site security. To do this, simply go to the "users" section of the WordPress admin panel and rename or delete the "admin" account or username.

WP Engine does not allow the use of the "admin" username and will automatically remove it for you, replacing the admin name with a "wpengine account" name. This account is used by our support team. We implement special configurations to prevent attacks on the "wpengine" user account specifically.

9 Limit Login Attempts


ERROR: We're sorry, but this IP range has been blocked due to too many recent failed login attempts.

Please try again later.

WordPress doesn't have a limit as to how many times one can guess a password to login. This presents a problem because determined hackers won't give up.

For example, a hacker could use a script to enter different password combinations (called brute-force attacks) until they've cracked the code.

To resolve this issue, you should limit login attempts. Here are some plugins built for limiting logins:

- Login Lockdown
- Limit Login Attempts
- Jetpack Protect

To prevent forgetful customers or employees from getting locked out, you can also whitelist certain IP addresses (Jetpack Protect is great for this).

If you using WP Engine, we've also built proprietary security into our platform to help limit login attempts.

10 Monitor Incoming Attacks

It's vital to log incoming security attacks so you're aware of what's going on inside your WP installation from a historical perspective. Here are a couple tools that can help you with malware monitoring:

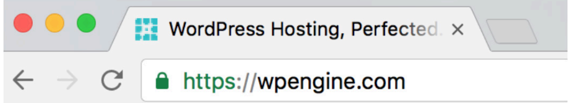
- Sucuri Security
- WP Security Audit Log

Getting insight into what's happening in your WordPress installation via a website malware scan tool is a good idea for tighter security and an easier diagnosis of any issues that might arise.

11 Use SSL

Enabling SSL is the next crucial step to a more secure site. SSL (Secure Sockets Layer) encrypts all information sent to and from your site. That way the private data visitors share with your site stays private.

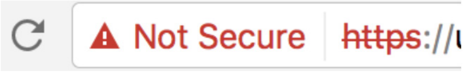
Using SSL ensures that hackers can't see or intercept the data your users share on your site. The secure tunnel SSL creates is especially important with sensitive information, like credit card numbers, usernames, and passwords.



Identifying whether or not a site is SSL certified is simple. An SSL certified site will start with an **HTTPS** in the URL address, while a site that's not SSL certified will begin with **HTTP**.

An SSL certificate helps a user's browser verify that they are not only accessing a secure website, but the certificate is also genuine and linked to the domain/website that was requested by the user.

This is especially important because Google Chrome has now started issuing "Not Secure" warnings for top-level sites that aren't secured over HTTPS.



With WP Engine, all customers are encouraged to obtain a free SSL certificate with Let's Encrypt.

12 Hide Your WordPress Version

If you defer WordPress updates, you should consider hiding your WordPress version because it leaves footprints, telling the hacker useful information about your site.

There are three areas where your WordPress version number will be hidden:

1. The generator meta tag in the header:

```
<meta name="generator" content="WordPress 4.0" />
```

2. Query strings on scripts and styles:

```
subscriptions.css?ver=4.0
```

3. Generator tag in RSS feeds:

```
http://wordpress.org/?v=4.0
```

To get rid of your WordPress version number in all three areas, add this code to your functions.php file:

```
/* Hide WP version strings from scripts and styles
 * @return {string} $src
 * @filter script_loader_src
 * @filter style_loader_src
 */
function fjarrett_remove_wp_version_strings( $src ) {
 global $wp_version;
 parse_str(parse_url($src, PHP_URL_QUERY), $query);
 if ( !empty($query['ver']) && $query['ver'] === $wp_version ) {
 $src = remove_query_arg('ver', $src);
 }
return $src;
}
add_filter( 'script_loader_src', 'fjarrett_remove_wp_version_strings' );
add_filter( 'style_loader_src', 'fjarrett_remove_wp_version_strings' );

/* Hide WP version strings from generator meta tag */
function wpmudev_remove_version() {
return '';
}
add_filter('the_generator', 'wpmudev_remove_version');
```

In addition, you should also make sure your **readme.html** file is removed from your install, as this exposes your version number.

At WP Engine we prevent access to this file on our platform to make fingerprinting WordPress versions more difficult.

13 Relocate Or Rename The Login Page

To make your site more bulletproof, relocating your login page is worth the effort. Not only does it hide the fact that you're on WordPress, but it limits brute-force attacks on your login page.

If someone was trying to hack your WordPress site and came across a 404 error upon entering your login page, say www.mysite.com/wp-login.php, they'd likely be deterred from breaking in.

Try using a plugin like Rename wp-login.php, Move Login, or iThemes Security to assist in moving or renaming your login page. But before you take this action, do be sure to talk to your web host or developer to ensure the steps you are taking are correct.

14 Secure The WP-Config File

The wp-config file contains your website's base configuration details, like database connection information. To protect your wp-config.php file from intrusion, add the following code to your .htaccess file to deny access to anyone surfing it:

```
<files wp-config.php>
order allow,deny
deny from all
</files>
```

For more information on moving the wp-config file, see the WordPress codex.

15 Use A Secure Hosting Environment

You can follow all of the security measures above, however, if you don't invest in a secure hosting provider, these efforts are all for nothing.

Secure hosting with WP Engine addresses many of the above tasks (daily backups, 2FA, etc.) with its proprietary security technology.

Here's just some of the security benefits WP Engine's enterprise-grade infrastructure contains:

Automatic Updates To New Versions Of WordPress

As soon as a new version of WordPress rolls out, we automatically upgrade your site for you so it contains the latest security patches.

Blocks Potential Hacks As They Occur

Our platform contains real-time security threat detection. We have the technology to block even the most sophisticated hacks, like JavaScript/SQL injection and XML-RPC attacks, along with garden variety DDoS and brute force attacks.

This technology also blocks IP addresses identified as belonging to spammers or hackers.

High-Performing, Secure Technology Stacks

Securing your web environment requires proper server configuration. 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.

Hacked? We'll Fix It For Free

While some consultants will charge thousands to fix a hacked site, in the unlikely event that your site is compromised, we'll fix it at no extra cost to you.

Final Thoughts

Now that you know about some ways in which to make your site more secure, if you ever do happen to discover a vulnerability, be sure to give back to the WordPress community by reporting it. You can send a detailed email to security@wordpress.org, or if you discover a plugin security vulnerability, email plugins@wordpress.org.