WORDPRESS SECURITY CHECKLIST

WORDPRESS SECURITY CHECKLIST

"Most successful Wordpress hack attacks are typically the result of human error, be it a configuration error or failing to maintain Wordpress, such as keeping core and all plugins up to date, or installing insecure plugins, etc"

Robert Abela, WhiteSecurity

Recent statistics show WordPress is powering 26.5% of the Web. It is, by far, the most used Content Management System with a **59.6%** market share. On a daily basis there are over **500** new sites being created on WordPress.

There are **1500** files on average per Wordpress installation. This number goes up with the more plugins and themes you install. There are currently over **44,000** plugins available to extend Wordpress functionality.

Security for Wordpress sites is an ongoing process, as it is constantly being updated and there are many moving parts. Nothing is 100% secure, but what you can do, however, is take preventative steps and security measures to protect your Wordpress site and reduce your risk of getting hacked.

"No one is interested in hacking my site.
I've got nothing valuable to warrant being hacked."

Hackers aren't usually targeting you personally**, they are targeting one of the most used systems.**

You can still be a target, even if you don't have a high profile / highly valuable site. One of the more common hacks is getting malicious code or database injections onto your site that link back to other sites. **Your site can simply become one of a network of link referring sites.** Things like Viagra ads could appear on your site in obvious or not so obvious ways. Some hackers are tricky with these and will put them in places like your footer text. Your site can work as normal, while at the same time you are quietly assisting the SEO of the target site with these "hidden in plain sight" type of links.

The largest journalist data breach in history, known as the Panama Papers Leak, with 11.5 million documents — or 2.6 terabytes of data released — was partly due to law firm Mossack Fonseca not keeping their Wordpress (and Drupal) web sites updated. Ouch. Someone probably got fired over that one.

WORDPRESS SECURITY CHECKLIST

If you have a successful membership site, the hacker could be trying to get access to your user database with all their emails, which can then be used – either by the hacker or whoever gets that list - to send spam messages to. We have a habit here of using a unique email address when signing up for services. It's shocking how many of those email addresses somehow become compromised and spammed, even though they are unique and only used for that particular service. Somehow someone somewhere got a hold of it.

"Security is not my problem"

If you're running a site or service online, security should always be part of your business plan and near the top, if not the very top, of your priorities. Especially if your site is actively handling the personal data of others through the use of ecommerce or memberships.

So what can you do to help protect yourself and secure your Wordpress site?

Here are some quick ways you can lock down your site and increase your overall security. They should be pretty straight forward and fairly easy to implement if you have basic knowledge of your Wordpress site and its structures. If you don't, many good hosting companies out there will implement things for you if you simply ask.

If you have any trouble, don't have the time, or just don't feel comfortable doing things yourself, connect with us at TLCforCoaches.com for a quote.

Always make backups of your site and files before installing plugins and making any changes!

QUICK SECURTY METHODS

☐ INSTALL A FIREWALL PLUGIN

There are many plugins and services that can act as a firewall for your website. Some of them work by modifying your system files and restricting some access at the Apache level, before it is processed by WordPress.

Two good examples are iThemes Security or All in One WP Security.

Other firewall plugins act at the WordPress level, like WordFence and Shield. These try to filter attacks as WordPress is loading, but before it is fully processed.

A lot of security plugins overlap in functionality. So if you go this route, **be sure that only one is installed and active** on your site to avoid conflicts which can interfere with your site. In other words, don't install 6 security plugins at once.

Once you choose a security plugin, **be sure to take the time to read all the documentation**.

ADVANCED / MANUAL SECURITY METHODS

A lot of the measures here work by manually modifying the .htaccess file in your root directory. What the heck is an .htaccess file?

To quote Apache:

> *.htaccess files (or "distributed configuration files") provide a way to make configuration changes on a per-directory basis. A file, containing one or more configuration directives, is placed in a particular document directory, and the directives apply to that directory, and all subdirectories thereof.*

You can usually access your .htaccess file by using FTP software, or through your hosting control panel. The .htaccess file can be touchy, especially if you don't get the formatting correct.

Always make backups of your site and files before making any changes!

☐ LOCK DOWN YOUR DIRECTORIES

Add the following code to your .htaccess to prevent access to directories.

```
#make folders private
Options All -Indexes
```

Please note that sometimes hosts will hide this file for added security.

WORDPRESS SECURITY CHECKLIST

LIMIT LOGIN ATTEMPTS

You can limit your login attempts using a plugin like Limit Login Attempts. Some hosts already include this by default on their Wordpress hosting packages. Limiting login attempts basically locks someone out after so many attempts to login.

Essentially your site is saying *"ok, you've tried to login x times. I'm going to put you on the ban list and notify my owner."*

If you have a membership site, you'll probably have a few users that simply forgot their password and decide to try everything they think it is to get in – therefore triggering a ban for themselves. The best way to try and mitigate this is to put up friendly text for your users that simply explains what happened and to contact you or do a password reset to regain entry to their account.

PROTECT YOUR WP-CONFIG FILE

Your wp-config.php file contains all sorts of confidential details about your site, such as your database username and password. It is generally not accessible online – but if your server is compromised or you have a backup of the file on your server – typically renamed wp-config.old – your database info, the core of your Wordpress site, can be exposed.

Scan the root directory of your site, and make sure you do not have any wp-config.old files (or variations thereof). **The only one you should have is wp-config.php**

To further protect your wp-config.php file, add the following to your .htaccess file.

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

HIDE LOGIN ERROR MESSAGES

The default Wordpress error message can be an issue as it can actually be valuable for someone trying to hack your site. The default message is typically:

"ERROR: The password you entered for the username is incorrect. Lost your password?"

This can be an problem because if they are guessing usernames and passwords, it essentially lets them know if they got the username correct!

To hide login error messages, put the following code in your functions.php file:

```
function no_wordpress_errors(){
  return 'Wrong username or password!';
}
add_filter( 'login_errors', 'no_wordpress_errors' );
```

☐ DISABLE EDITORS IN THE DASHBOARD

By default, most Wordpress installations will allow you to edit themes and plugins within the admin Dashboard. This is convenient, especially if you like editing PHP and CSS files directly. However, most Wordpress admins don't use the editor. Some refuse to touch it completely and ignore that it is there.

Disabling the editor improves your security because even if someone does get access to your admin Dashboard, they likely will not be able to modify your PHP files through there. **This is often the first tool a hacker will use** if they are able to get into your site because it allows code execution. If this is disabled, they would need to have access to your FTP / Control Panel, which is typically an entirely different login than your Wordpress admin login.

To disable the theme and plugin editors, enter the following code in the wp-config.php file:

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

HELPFUL HINTS AND TOOLS

Keep Your Wordpress Core Updated

It almost goes without saying, but a lot of people do not update Wordpress. It's become such an issue that a lot of hosts now have automatic updates a week or so after a new version is released. They'll just do it and send you an email that they've updated you. While that is good overall, you should always strive to do the updates yourself. It puts you in control of your own site and allows you to make any proper backups beforehand. This is especially true if you have a more customized Wordpress site, as some updates can break things.

WORDPRESS SECURITY CHECKLIST

Keep Your Plugins Updated

It is important to keep any plugins you have installed up to date as well, as many updates will patch new-found vulnerabilities. Furthermore, you should also remove any plugins you are not currently using to reduce your risk.

Always Use Strong Passwords

The stronger and more complicated your Dashboard password is, the harder it will be to compromise. The best passwords have a mix of upper and lower case letters, numbers and other symbols. Additionally, the longer they are the better.

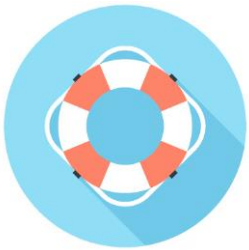
Research Wordpress Plugins

You might be surprised how many seemingly useful plugins have malicious code inserted. Before installing any plugin or theme on your site, you should, at the very least, do a Google search on it and scan to see if others have had issues with it. Reading the reviews of the plugins on the Wordpress Plugin Directory can also be helpful. A little time spent researching before installing something might save you a bunch of headaches later.

If you're looking for a quick list of safe and trusted plugins, we have a list of ones that we use on a regular basis for both ourselves and clients here:

www.tlcforcoaches.com/training/plugins

Make Backups of Your Site Regularly



If you do not have a regular backup plan in place, you should get one right away. There are plugins and services that will assist you in creating a backup plan. A lot of hosting companies now include automated backups as part of your service. You should check with them and see exactly what they are backing up, how often they are doing it, and how easy it is to restore if there is ever an issue.

Again, good security is a process. As Wordpress powered sites continue to grow, threats to security will also increase. Simply keeping on top of your core and plugin updates, hardening your security, choosing good passwords, making regular backups, and being aware of potential threats will greatly reduce your risk of being hacked.

WORDPRESS SECURITY CHECKLIST

TLC for Coaches

www.tlcforcoaches.com

We are a team of virtual assistants and web developers that specialize in supporting great coaches – allowing them to focus on doing what they love, while saving them time and money.

How can we help you be more awesome today?

/blog

www.tlcforcoaches.com/blog

Get more Wordpress tips, helpful hints, free goodies and fun stuff on our blog.

facebook

www.facebook.com/tlcforcoaches

twitter

www.twitter.com/tlcforcoaches

pinterest

www.pinterest.com/tlcforcoaches

youtube

www.youtube.com/tlcforcoaches