WPCOPILOT

by Chris Finnegan

Meet WP Copilot

We are a Melbourne based team of WordPress experts who copilot WordPress websites so you can get on with running your business. Our support plans provide maintenance, backups, security, developer support and resources for one of your business's greatest assets.

You can take a look at our WordPress support plans and find more WordPress resources HERE

If you find this guide useful please share it with others would could benefit from reading.

11 WAYS TO BOOST WORDPRESS SECURITY

WordPress now powers 18.9% of the internet, and that kind of popularity attracts the attention of thousands of potential hackers.

How hackers are hacking wordpress sites

- 41% were hacked through a security vulnerability on their hosting platform
- 29% were hacked via a security issue in a WordPress Theme
- 22% were hacked via a security issue in the WordPress Plugins installed
- 8% were hacked because they had a weak password.

Figure 1: In 2012 over 170,000 wordpress websites were hacked[1], and in 2013 this is set to increase.

What would the cost be if your website was hacked?

It may take several days to realise your website is hacked in the first place. By then you've lost sales and had your reputation damaged through a defaced website and or spam emails sent from your account.

You then have to find a developer to restore or fix your website which could be another few days of lost sales and reputation, while adding to the cost. Not to mention the high stress levels through the whole experience!

Thinking it won't happen to you is not a plan!

Following this list of wordpress security tips to reduce the chance of discovering your WordPress website has become the victim of an attack.

Don't use 'admin' as your username

Hackers trying to access your WordPress admin area will often try using the default username 'admin' as their first point of entry. WordPress gives you the option to change your admin username into whatever you like. By changing this a brute-force hacker has to guess both your username and password to access your WordPress website.

2 Use a strong password

Many people use weak passwords which are easy to break with modern brute force attack software. Hackers use this software to try 1000's of common password combinations, eventually gaining access to accounts with weak passwords (about 8% of WordPress websites are hacked with this method).

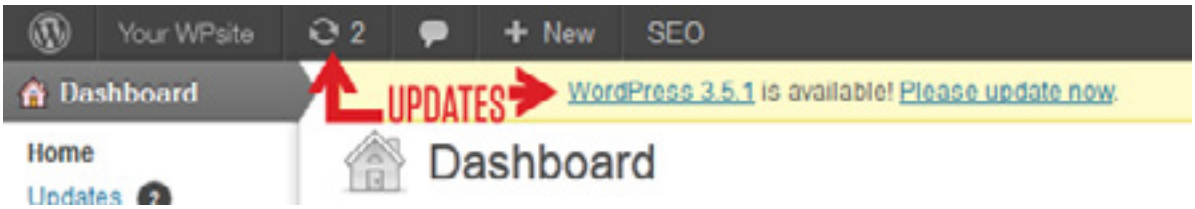
WordPress has a password strength indicator which is displayed when changing your password. Use this to ensure your password's strength is adequate. A secure password is a string of 10+ characters with including a mix of capitalised and lower case letters, numbers, and symbols.

Not wanting a difficult to remember password is no excuse! **Simply adding a couple of symbols before and after your password can make it far more secure** and no harder to remember.

---

3 Update WordPress, themes and plugins

As new security vulnerabilities are detected, software developers release new versions to block them. Keeping your WordPress core, themes and plugins up to date means you'll be taking advantage of the latest security patches for each.



Make a time on a regular basis to review and update your WordPress website, plugins and themes. Always backup your website before making any updates, so you can revert back in the event that something goes wrong.

---

4 Check plugin code is maintained

Just because there are no updates does not mean a plugin is actually up to date! It could be that a plugin has been abandoned by the developer. Visiting the plugin page at the WordPress plugin directory will tell you the time it was last updated. WordPress actually puts a banner on pages where the plugin has not been updated in over 2 years.

Figure 2: The banner Wordpress displays to indicate that a plugin has not been updated in over 2 years

If a plugin appears to have been abandoned that means nobody is reviewing and fixing security issues that may be present, so it's best to find an alternative with an active developer and community.

Keep it tidy!

Review and remove any unused user accounts, WordPress themes and plugins. This will reduce the number of possible security issues, eliminate wasted maintenance and upgrades, and may actually speed up your website!

Hosting environment

Not all web hosting services are equal, remember 41% of wordpress websites are hacked due to a hosting vulnerability.

Carefully choose your hosting provider, don't simply go for the cheapest available. Find a well established business with a good track record by talking to other business owners about their experiences, and reading reviews. We recommend Digital Pacific for WordPress hosting.

Home or office computer security

Security issues on PC's or other devices you use to update your WordPress website can effect your website security.

PC malware can record your passwords as you type them using "keylogger" software. So it's important that any and all PCs and devices you use are kept properly secure.

Make sure you're running the latest version of your web browser, antivirus software and operating systems.

Avoid free themes

Avoid free themes and only purchase themes from reputable websites.

This is for two reasons. A paid theme gives the developer some income and motivation to continue to upgrade and maintain the theme security. Secondly free themes can often contain things like base64 encoding, which may be used to insert links into your site, or other malicious code that can cause issues that are difficult to detect. As shown in this experiment, as high as 8 out of 10 sites reviewed offered free themes containing base64 code.

Themeforest is a theme marketplace that has a huge amount of options together with user reviews and other useful information to find a suitable WordPress theme.

Limiting failed login attempts

Brute-force attacks repeatedly try to login to your website using 1000's of passwords. Limiting the number of failed login attempts from a single IP address can reduce the effectiveness of brute-force attacks.

The Limit Login Attempts plugin does just that, allowing you to specify how many login attempts are allowed, and how long an IP will be locked out for too many failed login attempts.

Changing file permissions to secure WordPress

You may have seen file permissions like 644 or 755, associated with your website files and folders. These numbers are very important, setting who can read, write and execute the files. Not having the correct permissions can leave you with serious security holes.

Wordpress.org describes the correct settings and how to change a file's permissions using an FTP program. Some security plugins like the File Permissions & Size Check plugin can actively check file permissions for you.

Hacked website recovery plan

Do you have a plan for website recovery if your website is hacked? Although this won't help prevent your website being hacked directly, it will minimise the damage and response time should this happen.

How do you know if your website is hacked?

There are companies and plugins that can help monitor your website for malware. If you're not a WP Copilot customer the Sucuri team not only scans for malware, but also helps you clean it up once it's detected.

Make sure you have multiple website backups and backup regularly. Yes your website hosting company does backups but you shouldn't rely on them. If someone hacks your website and you don't have a backup, it can be very difficult to restore it back to its previous state.

Have a plan and test it before you need it to ensure the backup system works.

Don't procrastinate!

Thanks for taking the time to read these tips, now do yourself a favor and implement them! If you don't have time to follow all of the above tips, please follow at least two of them, and schedule a time to revisit this ebook. It will help you to enjoy the effort you invested in your WordPress website.

If you find that you simply don't have the time, know-how or would just like to outsource wordpress security consider a WordPress support plan at WP Copilot.

WPCOPILOT

WordPress Support, Maintenance & Security

WPCOPILOT

www.wpcopilot.com.au