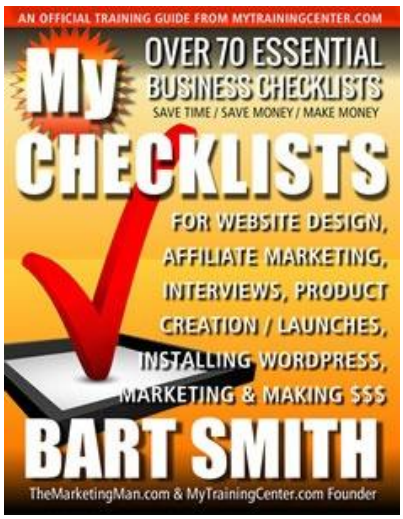
WordPress Security Checklist

by BartSmith.com | My Checklists Book Details Page + Video Tours



Website security is a serious issue with every website, particularly, if yours generates revenue and has a lot of traffic. You cannot afford to have your site compromised or shut down by your web hosting company due to malicious malware installed on your site unaware or without your knowledge.

Website hacks, malware, and other forms of vicious cyber attacks on websites should not be feasible on any site. Loss of data, down sites, suspended hosting accounts are serious problems when one is trying to earn a living online.

Protect your website, hosting reputation, and online income by becoming familiar with the benefits for installing a robust WordPress security plugin. Here's a checklist for several types of security measures.

KNOW HOW TO PROTECT YOUR WORDPRESS WEBSITE

1. ____ Ability to **add a simple math CAPTCHA to the WordPress login form** to fight against brute force login attacks.

2. ____ Ability to **automatically lockout IP address ranges** which attempt to login with an invalid username.

3. ____ Ability to **block fictitious Google Bots from crawling your website**.

4. ____ Ability to **disable the right-click function**, highlight/text selection, and copy option to protect your content.

5. ____ Ability to **hide your admin login page (http://yoursite.com/wp-admin/)**. You should rename your WordPress login page to only a name you know, such as, http://yoursite.com/imwonderful. This prevents bots and hackers from accessing your real WordPress login URL.

6. ____ Ability to **log all 404 events on your website**. This can help clean up dead-end pages on your website. You should also be able to choose to automatically block IP addresses that are hitting too many 404s.

7. ____ Ability to **prevent image hot-linking**, which is when other websites place your images on their website by linking to yours. This can kill your bandwidth if you have hundreds of websites linking to hundreds of images on your website. Turn it off. Keep in mind, if you allow affiliates to link to banners on your website, don't turn off the banners your affiliates need.

8. ____ **Ability to see a list of all users who are currently logged into your site**. If you don't recognize someone, you can check them out and decide to terminate their account if needed. I've seen it happen where people register and start blogging on your site with absurd, meaningless articles that have nothing to do with your website's theme or purpose so they can promote the garbage they sell.

9. ____ **Ability to use "honeypot login"** that helps reduce brute force login attempts by robots.

10. ____ **Add a CAPTCHA to your WordPress comment form** to add more security against spam comments.

11. ____ **Add CAPTCHA to WordPress Login form** and forgot password form.

12. ____ **Add firewall protection to your site with .htaccess file** to stop malicious script(s) before it even reaches the WordPress code on your site.

13. ____ **Add script to your .htaccess file so you can block unacceptable countries** from visiting your website such as China, Iran, Russia, Nigeria, etc.

14. ____ **Allows you to specify one or more IP addresses** in a special white list (a list of people/ products viewed with approval).

15. ____ As the admin, you can **view a list of all locked out users**.

16. ____ **Ban users by specifying IP addresses** or use a wildcard to specify IP ranges.

17. ____ **Block "bots" from constantly accessing your xmlrpc.php file** and wasting server resources.

18. ____ **Brute force login attack prevention**.

19. ____ **Database scanner feature** can be used to scan your database tables. It will look for suspicious-looking strings, javascript and HTML code in some of the WordPress core tables.

20. ____ Deny malicious query strings that show up in your WordPress database.

21. ____ **Detect if there is a user account that has the default "admin" username** and change the username to a value of your choice.

22. ____ **Easily backup your original .htaccess and wp-config.php files** in case you need to use them to restore broken functionality.

23. ____ **Easily change the default WP prefix** in the database to a value of your choice with the click of a button.

24. ____ **Easily view and monitor all host system logs** from a single menu page and stay informed of issues or problems occurring on your server so you can remedy them quickly.

25. ____ **Enable the famous "5G Blacklist" Firewall** rules courtesy of Perishable Press.

26. ____ **Forbid proxy comment posting** on your website.

27. ____ **Force logout of all users after a configurable time period** of trying to login.

28. ____ These backup files **.htaccess and wp-config.php files have restore features.**

29. ____ **Identify files or folders that have permission settings and if not secure**, set the permissions to the recommended secure values with click of a button.

30. ____ **Instantly block Brute Force login attacks** via our special cookie-based brute force login prevention feature. This firewall functionality will block all login attempts from others including bots.

31. ____ **Modify the contents of the currently active .htaccess or wp-config.php files** from the admin dashboard with only a few simple clicks.

32. ____ **Monitor the most active IP addresses** that persistently produce the most SPAM comments and instantly block them with the click of a button.

33. ____ **Monitor/View login attempts that show the user's IP address**, User ID/Username and Date/Time that show as failed logins.

34. ____ **Password strength tool** to allow you to create very strong passwords.

35. ____ **Prevent comments from being submitted** that don't originate from your domain to reduce the posting of SPAM bot comments.

36. ____ **Prevent people from accessing the readme.html**, license.txt and wp-config-sample.php files of your WordPress site.

37. ____ **Protect your PHP code** by disabling file editing from the WordPress administration area.

38. ____ **Schedule automatic backups** and email notifications or make an instant DB backup whenever you need it with one click.

39. ____ **The file change detection scanner** can alert you if any files have changed in your WordPress system. You can then investigate to verify a legitimate change or whether a bad code was inserted.

WordPress security evolves over time. Plugins evolve as hackers and spam bot creators evolve. The best thing you can do to protect your website is to install any one of the recommended **WordPress security plugins** found on MyTrainingCenter.com. You can check them out, read more about them, and install one (or more) simply by clicking on the link provided.

While there are several very robust WordPress security plugins, you cannot install all of them and hope they will doubly guarantee security. You normally would install one only. If you don't like the one you installed, uninstall it, and test another one. Many can be customized to meet your specific needs. By using more than one, multiple plugins working together are very often incompatible. So, research them, and try a couple of them. Most plugins working independently do a good job of preventing a fair number of attacks.

# # #

