A 16-Step Guide to a 99% Secure Wordpress Website

Need help?

13884 Montoclair Ln
Dale City VA 22193
(571) 406-2689
nate@valiantchicken.com

Let's get started

For a platform that powers a quarter of the websites in the world, Wordpress is surprisingly insecure. The default settings leave a site open to being hacked a half-dozen different ways., and hackers know that, but you don't have to be their next victim.

The Basics

Passwords

The current consensus is that passwords need to be long enough that they’re hard to guess but also simple enough that you can remember them.

Bad: K5^KB@sUv0YasF9u)

Good: Battery Horse Staple Correct

Backups

Set up regularly scheduled backups so that if your site gets hacked, you can restore the backup and then patch the security hole.

Unused Accounts

If you gave a web designer an admin account in order to work on your site, be sure to downgrade the access level as soon as the work is done, This will keep hackers from using that account to take control of your site.

Firewall Plugin

A firewall plugin will alert you to someone trying to hack your site, and it can also tell you if a hacker has already gained access and is making changes.

Wordpress Updates

If you keep your plugins, theme, and core WP files up to date, you will reduce the number of opportunities for hackers to gain access to your site.

Limit Login Attempts

Hackers will try to gain access to your site by guessing your password. They'll hit the login page with thousands and thousands of guesses. This will crash your site, which is why you should set the firewall plugin to limit login attempts.

Two-Factor Authentication

2FA is when you require users to use another method to confirm who they are before they log in. Usually this involves accepting a notification on their smartphone, or confirming a link sent to their email account. Using a plugin to enable this feature helps further protect you from brute force attacks in case a hacker is able to guess your password.

Don't Use Public Wifi

While the public Wifi at fast food chains is probably safe, people have been hacked after using the Wifi offered by some random coffee shop or retailer.

The Basics, part two

Remove Unused Plugins

Every piece of code on your site is just one more way for hackers to get in, and that is why you should remove any plugin that you aren't using.

"Admin" Username

If you log in under the uername "admin", you should know that hackers always target that username first. Immediately set up a new account. Give the new account administrator privileges and then disable the old account.

Block Spam Comments

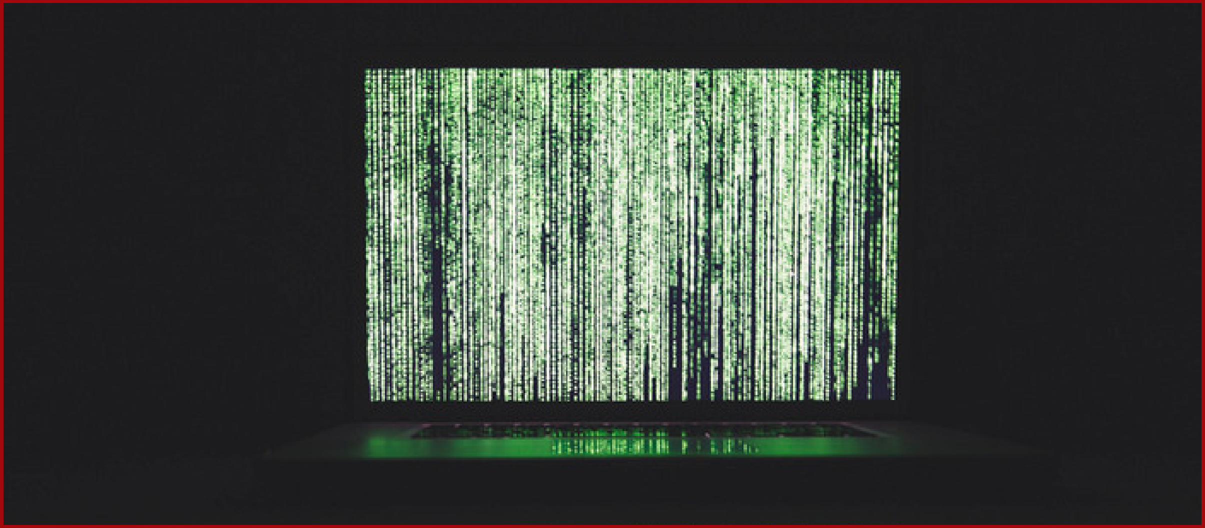
Install a spam blocker like Akismet to keep hackers from using spam comments to target your site's readers with links leading to malicious sites.

Run Security Scans Weekly

Here's a scary thought: your site might be hacked without showing any signs. That's why you should use Sucuri's free online scanner at least once a week to check.

It takes a community

Website security is incredibly important, but you're not in this alone. There's a large online community of security professionals who can keep you up to date on the current best practices.



Advanced Measures

SSL & HTTPS

Adding an SSL certificate and upgrading your site to full HTTPS will protect your visitors and users from what is known as "man in the middle" attacks.

Database Prefix

It is SOP when creating a new Wordpress site to add the prefex "wp_" to all the tables in a database/ Hackers use this detail when targeting your site's database, which is why you should change the prefix.

Disable Folder Browsing

Folder browsing can be used by hackers to find out if you have any files with known vulnerabilities, so they can take advantage of these files to gain access.

Check File Permissions

All Wordpress sites use the same set of standard system file names, and if a hacker can directly read/write the files then they can hack your site.