Guide to Securing Your WordPress Site

VACANO | CREATIVE

Hi, I'm Chris Vacano, owner of Vacano Creative in Portland, Oregon. I've been building web sites for over 20 years and have worked exclusively with WordPress for 10 years. I want to start off by thanking you for downloading this guide, and let you know I really hope you find it helpful. I put this checklist together because I fundamentally believe that prevention is the key to stopping trespassers and vandals.

This list is the result of many years of research, trial and error, testing and tuning, and talking to other WordPress pros. I know this multi-layered approach works because I've been using it on behalf of my clients for close to 6 years now, and in that time, not a single site that I've secured has been compromised.

As you're reading this, the bad guys are out there looking for sites they can break into and wreak havoc. The sooner you protect your site, the sooner you can let go of the anxiety that you might be the next target. This checklist is intended for you to be able to get started on securing your site right away. You should be able to take care of most of the list in just a couple of hours, so what are you waiting for?

Lock it Down! (from the inside)

- ☐ Firewall and Antivirus Plugin(s) – this is the cornerstone of your defense
- ☐ Ensure you're using trustworthy plugins by reputable developers
- ☐ Install an SSL (Secure Socket Layer) Certificate and force https: – many hosting providers will set this up for you by request
- ☐ Block traffic from countries where you are not conducting business
- ☐ Make sure your hosting provider has good server and network security in place to detect and stop DDoS and other attacks

Limit Login Access

- ☐ Enable 2-Factor Authentication (2FA) and enforce strong passwords for Admin users – not recommended for *Subscriber* users because this will just annoy your guests unnecessarily
- ☐ Set registered guest users to *Subscriber* level
- ☐ Hide the WordPress Admin Bar from *Subscribers* – they don't need it, and most will find it confusing or annoying
- ☐ Limit number of login attempts in a specific period

- ☐ *Optional: set up a "honey pot" field on forms*
- ☐ *Optional: use Captcha or reCaptcha on forms*

Reduce the Attack Surface

- ☐ Close all unnecessary points of entry
- ☐ Remove all unused themes and plugins
- ☐ Block long & unusual character strings in forms
- ☐ Remove all WordPress markings and headers – no need to make it easy on the bad actors to spot you
- ☐ Optional: hide the admin login page – this is not super-effective on its own, but it may slow some of the troublemakers down
- ☐ Only manage/edit your site from a trusted computer on a secure wi-fi or wired network (for example, your office or home)
- ☐ Limit Admin access hours – like locking your doors at night

Maintenance is a Must

- ☐ Update the WordPress core, theme(s), and all plugins regularly
- ☐ Set up email or SMS notifications for logins, file changes, and uptime
- ☐ Schedule regular backups to an off-site location (in other words, don't save your backups on the server where your site is hosted)

BONUS – Use a Content Distribution Network (CDN)

- ☐ A CDN is a cloud-based service where you route all your site traffic through a secure, globally distributed network of computers that serve exact copies of your site to any and all outside visitors.

Do half of the things we listed here, and you're in pretty good shape. Three quarters, and you're doing well. Do them all, including the optional and bonus tasks, and you can sleep easy: your site is basically bullet-proof!

Have questions? Drop us an email at hello@vacanocreative.com

www.vacanocreative.com

VACANO | CREATIVE