10-POINT WORDPRESS SECURITY CHECKLIST

10 THINGS YOU CAN DO TODAY TO PROTECT YOUR SITE

FROM AGATHON

ABOUT AGATHON HOSTING

Agathon provides WordPress hosting by real people & for real people, with a focus on performance, security, and support.

Visit our blog or

learn more about Agathon hosting.

Agathon

AgathonGroup.com

WordPress is the most popular content management system (CMS) in use today, powering somewhere between 25 to 33 percent of all websites on the internet. Because of this, WordPress sites are popular targets for cyberattacks. We've designed our hosting environment from the ground up with security features that reduce the risk of these attacks**.** But your host's role in your site's security is only part of the story.

There are things *you* should be doing to keep your site safe as well. More often than not, attackers exploit the software running your site rather than the hosting environment underneath. As a site owner, you play a big role in helping mitigate or prevent these sorts of issues.

Use this 10-point checklist today to better protect your site against these attacks!

❑ Ask your host about their server-level security.

Contact your host to be sure that they're providing security for your site at the server level. This includes things like free SSL certificates, disabling insecure FTP on cloud applications, and putting a firewall in place to block problematic SSH login attempts.

❑ Make sure all plugins and themes on your site have been downloaded from official, trusted sources.

Plugins without oversight or accountability—or those that have been pirated—could introduce vulnerabilities to your site. If you've downloaded any plugins from unsecure or questionable sites, you should delete them and look for trustworthy alternatives.

❑ Update WordPress, themes, and plugins.

While you might think that updates to these simply provide performance improvements, they can also include important security patches that reduce vulnerabilities. Check your dashboard and run any available updates. Delete any plugins you no longer need in order to reduce the potential security risk.

❑ Rename your login page.

Renaming your login page hides it from attackers and offers "security through obscurity." The Move Login plugin makes this easy to set up in minutes.

❑ Customize your username.

If you currently have a standard 'admin' username on WordPress, now is the time to change it. You can create a new user—make sure it has all of the permissions you need!—and delete the old one. Or you can make this update in your database. If you want to take that route but aren't sure how, contact your host.

❑ Review and strengthen your passwords.

We recommend using either a random password generator with passwords of 16 or more characters or a string of 3-4 random words. Use a password manager (such as 1Password or LastPass) to keep track of your secure passwords.

❑ Review all user accounts on your site.

In addition to the 'admin' account, every user account on your site offers another opportunity for someone to hack in. If you have user accounts for one-time or occasional contractors that are not currently in use, be sure to downgrade their role to Subscriber.

❑ Be sure your site uses SSL.

Visit your site and check for the lock symbol or https:// in the address bar that indicates your site has an SSL certificate. If your site isn't currently secure, you should set up SSL today.

❑ Select and install additional security options.

In addition to the items above, adding a security plugin can provide additional layers against attacks. We recommend Stop XML-RPC Attacks for all of our hosting clients. WordFence and Sucuri both offer security plugins with a firewall and malware scanner to protect your site. And services like CloudFlare provide distributed distributed denial of service (DDoS) attack mitigation.

❑ Schedule regular backups.

Regular backups are the final layer of protection for your site. If you back your site up regularly, you'll be able to restore it without losing your latest changes, blog posts, or comments if anything happens. Your host should be providing daily backups (and have a way for you to easily restore those backups when needed), but we also recommend using Updraft Plus for an additional layer of protection.

Looking for a host that prioritizes security?

Email or call us today to talk to a real person about how we can support your blogging efforts with our secure, reliable cloud hosting packages!

Email: support@agathongroup.com

Phone: 888-543-9766