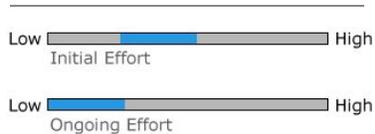


**3 Easy Things
To Do To
Protect Your
WordPress Investment
This Afternoon**



You've invested a lot of time, effort, and money into your blog. Don't let malware and spammers ruin your investment.

Security is an ongoing effort, but doing these three things will stop most attacks and give you a backup plan if the worst happens to your blog. Let's get started!



1. Create Passwords With "Brute Force Protection"

Let's make sure all users are using a strong password.

What's all this about strong passwords? Well it's not about people guessing your password, it's about computers doing it.

Computers are fast, really fast, and guessing millions of passwords is pretty easy for them. The longer the password and the more types of characters in it, the more the computer has to guess. This is called a "Brute Force" attack, meaning the computer just tries everything until it gets it.

WordPress will now tell you how strong your password is. Here's how:

- Login and go to "Edit my Profile" in the top-right menu.
You want something with 8 or more characters, including numbers and symbols. A pain, I know!

After setting up good passwords, installing Brute Force protection via a plugin of some kind will really help. There are different approaches, and they all slow the computers guessing way down.

WP Support HQ recommends one of the following plugins. Install and activate one, then make sure the brute force protection is on.

- **Anti-Malware Security and Brute-Force Firewall**

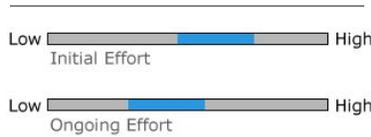
<https://wordpress.org/plugins/gotmls/>

This is our favorite. It works great, is easy to setup, and includes one of the best Malware removal engines we've used.

- **iThemes Security Pro**

<https://ithemes.com/security/>

For even more security iThemes Security Pro is great. It has tons of options and may be overwhelming at first. Budget some time to read the documentation and understand the options as you are setting up the plugin.



2. Build Great Content & Back it up!

“But my hosting provider said they provide backups!”

Did they? Is it a WordPress specific hosting provider? If so, you’re probably in good shape here. You’ll want to make sure they are running and you know how to restore those backups.

Not a WordPress specific host? No problem! There are a number of backup solutions out there.

What’s in a Backup and What You Need to Know About Backups.

WordPress is a set of files and a set of database tables, we’ll just call them the database.

Your backups should include all the files, this includes your plugins and themes, and it should include your database.

The database holds all your configuration settings, but more importantly, it holds all your content. Pages, Posts, Comments, everything. Each backup should include both, all the files and the database.

You Want your Backups Off-Site.

What does that mean? Basically, it means there should be a copy somewhere other than on the website server, on-site. This could be another server, like Amazon or Dropbox, or your local computer.

This is important because if something happens to your site and you need your backups stored on your site... you might be in trouble. The server could be down or malware could make the site un-accessible. Either way, having backups off-site will be a huge relief.

How to Restore Your Backups.

This is often an overlooked step, until it's time to actually restore the backups. We've found the best way to do this is backup your site and then restore it! Either to the current site or on a sub-site or staging site.

WP Support HQ recommends one of the following backups.

- UpdraftPlus

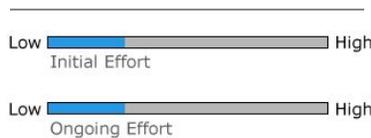
<https://updraftplus.com/>

This will allow you to create backups and download them to your computer as needed. The restore process is also good. They have a premium version that will handle scheduling backups and storing them off-site at a number of different storage providers.

- Duplicator

<https://wordpress.org/plugins/duplicator/>

This is another great backup plugin. The free version allows manual backups that you can then download to your computer. They also offer a Pro version with scheduling and cloud storage.



3. Keep Those Plugins Updated - *With Caution.*

Updates are important, but they can break your website, so many people just don't update.

The problem is updates aren't just about new features. Often they contain security fixes. Getting these security fixes is important because malware makers and spammers will scan the internet looking for "unpatched" websites. And since you now have backups, you don't have to worry so much about updates breaking your site!

This one's easy, here's how:

Just go to Dashboard > Updates at least once a month and update everything.

Reminders From WP Support HQ:

- It's a good idea to make sure you have a backup before running the updates.

- If you've made changes to your theme files, updating it will overwrite those changes. It's probably a good idea to move those changes into a "Child Theme" before updating the theme. Updates to everything else should be fine, so don't wait on those!

Bonus! Keep an eye out for important security updates and update as soon as you see them. These blogs are good sources to follow for security updates.

<https://wordpress.org/news/category/security/>
<https://blog.sucuri.net/>

We know this is a lot! But really, we think it's the minimum you should do to protect the investment you've made in your blog.

WP Support HQ specializes in taking care of WordPress sites. We do all the things above, plus a few more to keep your site running smoothly and securely.

Want WP Support HQ to take care of your blog while you take care of blogging?

[Sign Up](#) now! With free migrations we'll get you setup quickly and let you get back to running your business.

