Securing your Wordpress website

By Ryan Murphy

4 Mar 2015

If you've got a website that's based on Wordpress, you're part of the 76.4 million (according to reports) people who have websites that use the Wordpress content management system (CMS)...

Impressive. However, as with any CMS, there are certain disadvantages that come with a website that can be updated online.

© Bruce Rolff – 123RF.com

Constant updating and checking is required for any website, but with Wordpress, even more so. Unfortunately, hackers are smart and getting better at finding sneaky ways into the back-end of your website.

Here are some ways you can improve the security of your Wordpress website and try prevent those annoying hackers from destroying it.

1. Use a good password

Gone are the days you could use a password such as "yourname123", "admin", or even "password". This is just asking for problems.

Make sure your password is secure. You've probably heard this before, but use combinations of upper case and lower case letters, numbers and special characters in a password of at least 12 characters long.

As a general rule, never use your name or company name in the password.

2. Never use admin as a username

One of the flaws ofWordpress is that you can guess a username quite easily. By simply typing the potential username in a URL string, you can see if it exists or not, like this: http://www.yourwebsiteordomain.com/author/the-guessed-username.

Often, those who don't take security in mind when developing websites, or those setting up their own websites, will be tempted to use the username "admin". Don't do this. 'Admin' is one of the most popular usernames for Wordpress websites. Once a hacker knows what your username is, all they have to do is start guessing your password.

3. Make sure your hosting provider offers a secure hosting environment

You're not the only one who needs to take reasonable steps in securing your Wordpress website. Your hosting company will need to as well. Check with them about how they can secure your Wordpress website installation.

Remember, cheaper isn't always better when it comes to web-hosting providers.

4. Always update your website plugins and CMS

Plug-in and CMS updates often are released to fix security issues of previous versions. Keeping up-to-date with the latest versions of these will help prevent a hacked website.

5. Backup, backup, backup!

Always backup your website. If you're adding content to it often, then you should backup at least once a week. For a website that doesn't have new content added often, once a month should be fine.

There are plugins that can help you, but I'd suggest backing up via your web-hosting control panel. You'll get these details from your hosting provider when you register your hosting account with them, otherwise ask them.

Always make sure you backup the files and MySQL database.

Don't be shy to ask your web-hosting company for help with backing up your website.

6. Try not use free website themes and plugins

Free themes and plugins can help, but they also pose security risks and allow hackers to gain access to your website easily through vulnerable code.
Some things are free for a reason. Paid themes generally take longer to develop and security of the theme is taken into account when developing it.

7. Using a security plugin

A good Wordpress security plugin, such as All in One WP Security and Firewall, Sucuri-Sanncer or BulletProof Security allow you to block invalid login attempts to the backend of your website. They also allow you to rename your website backend login URL (/wp-admin/) to something different, so when a hacker tries to get in via 'www.yourwebsitedomain.co.za/wp-admin', they get a surprise.

8. Monitor your website

Sometimes when a website is hacked, it's removed completely from public viewing. Services such as Pingdom allow you to monitor website and receive email or SMS alerts when your website goes down.

9. Disable user registrations

Always make sure that user registrations are disabled on your website, if you don't require people to register. This is a potential security issue, which can lead to hacking. To do this, login to your Wordpress backend, visit Settings, the General and untick "Anyone can register".

10. Don't allow commenting

Some people like comments on their Wordpress websites, some don't. I have found it to be a security risk, with hackers gaining access to the website backend through comment boxes.

If you don't need it, you can disable it in the Wordpress settings and on individual pages under the discussion settings.

ABOUT RYAN MURPHY

Ryan Murphy is a small business owner of Chillibuzz - a digital brand management company that specialise digital public relations. Previously a Public Relations Account Executive at a Cape Town based PR agency, Ryan has PR experience which assists on a daily basis in servicing Chillibuzz clients.
- Securing your Wordpress website - 4 Mar 2015
- Don't build your own website - 19 Feb 2015

View my profile and articles...

For more, visit: https://www.bizcommunity.com