How To Keep Your WordPress Website Secure

Security for your website is very important. This article includes some tips for increasing security for your WordPress site.

1. Personal Workstation Security

A. Have antivirus programs and regularly scan your machine for viruses or malicious software.

B. Update your browsers, anti-virus, and operating system regularly.

C. Install security patches as soon as they become available.

D. Use a firewall, at the router and the ISP level if possible.

E. Update local passwords often, at least every 2-3 months.

2. Strong Passwords

A. Create a strong password. You can find more about strong passwords here.

B. Don't share your password.

C. Don't use the same password for multiple websites.

D. Don't have the mindset that someone isn't going to hack you.

3. Protect Your 'wp-admin' Users

A. Rename the admin user to something unique, but know that your username is published in a variety of locations on your website. Just renaming the admin user may not necessarily protect your account.

B. Make sure that each admin user on your account has a secure and unique password.

C. Yubikey is an additional option that can further secure your log-in, check out the details for that here.

4. Keep WordPress and Other Applications Updated

A. These updates fix bugs, close security holes, and add functionality.

Hackers will scan for outdated versions of WordPress and attempt to hack in with these known vulnerabilities.

B. If you used Softaculous to install WordPress, you can also use it to update it. Read how to here.

C. Do the same for any themes or plugins you have installed - updates are vital to account security.

D. If you worry about themes or plugins being broken with updates, you need to utilize different themes or plugins - the providers of these addons should be keeping up with the WordPress updates to keep users like you as secure as possible.

E. If you're not a developer you should look at plugins/themes with paid update and/or support options. These themes will be more likely to help keep your website secure.

5. Control Sensitive Information

A. Permissions on files are configurable for a reason. Control what files are visible to the world, and limit the files that deal with your account functionality.

B. For example, disable word read permissions on the readme.html file to avoid letting outsiders see what version of WordPress you're using.

C. Make sure you don't have phpinfo.php, info.php, or i.php files accessible to everyone.

D. DO NOT leave .sql backup files in your web directory - your usernames and passwords are saved in those files with all your posts and comments.

6. Malware

A. Check for malware every day.

B. Do something about Malware! The tools above will actually help you resolve the issues that come up. Make sure that you are proactive in taking care of possible infections immediately.

7. Clean your site

A. Just like you complete daily chores around the house, you should regularly clean up your site and files that you do not need.

B. Having old files on your account can leave you vulnerable.

Even if you've deactivated the old plugin or kept a backup of an old version in your web folder.

C. Stay clean and keep things organized - you should know all the files on your account well enough to identify when something is there that shouldn't be.

8. Backup your website

A. A good plugin that can be used here is WP-DB Manager (note that it may consume excessive resources in a shared environment).

This plugin can be useful for reporting other vulnerabilities when it detects accessibility issues.

B. Remote backups are also good options, if you haven't already, check out ComCure:

9. Install Security Plugins

A. Remember to only install plug-ins offered through the WordPress control panel since external plug-ins may not be secure. Most plugins offered from WordPress.org are regularly audited.

B. Guard against brute force attacks. Thousands of failed login attempts happen on servers every day. While we do provide firewall protection to help defend against attacks like this.

i. Programs like Limit Login Attempts and CAPTCHA can help you defend your account from brute force attacks.

C. Use Exploit Scanner.

D. Install other useful plugins Bad Behavior and User Spam Remover

Want More? Check out:
WordPress Security - Part 2: Maximum Security!