

5 Tips for Keeping Your Website Secure

So, you've gone to a lot of trouble and effort to get your business website looking just the way you want it. Don't forget to make it safe! You've probably heard about the increased risk of hacking, data theft, and web attacks, but there is a lot you can do to protect your website. There are some key measures you can take to minimize your risk and reduce your website's vulnerability.

1. Minimize the risk from plug-ins

Experts say that vulnerable plug-ins are the top way hackers can gain access to WordPress sites. When it comes to plug-ins you should:

- Keep the number of plug-ins to a minimum. You really don't need that many, tempting as it might be!
- Delete any plug-ins you're not using and keep the others updated.
- Check and double-check plug-ins before you download them to make sure you're getting them from a reliable source.
- Remove plug-ins that haven't been updated in over two years, and regularly check to see if your plug-ins are current. Check the Wordpress Directory to make sure your plug-ins are still live.
- Use Wordpress Security plug-ins to detect threats, and block attackers and malware. Popular ones are Wordfence Security, iThemes Security, and All in One WP Security and Firewall.

2. Make it hard to login as you

Using 'admin' as your username, or having a weak password is like leaving your front door open. It's almost inviting hackers in! Make sure you don't use the default 'admin' username. Think of a unique and difficult username to guess. Similarly, come up with a strong password using a combination of letters, capital letters, symbols, and numbers between 10 and 15 characters long. If you find this difficult, you can use Strong Password Generator to make one for you.

And don't forget to change your password regularly. Schedule it in as a regular business task, so you don't forget.

3. Make your website HTTPS

Changing your website to HTTPS encrypts the connection between your web server and your web browser protecting your data from attacks. And as an added bonus, HTTPS improves your Google rankings!

4. Use two-factor authentication

Two-factor authentication protects your website against an attack that tries unlimited combinations of usernames and passwords until the hacker gets into the site. Adding Google Authenticator to your website will add this feature automatically.

5. Backup and update

Doing regular backups and updates will keep your website data safe, so even if the worst happens, and you are hacked, you'll be able to get your site back as soon as possible.