



Be aware that hacking activity is continuing to rise to all-time highs.

At this point we're seeing Wordpress sites being hacked on a monthly, and sometimes weekly, basis. It is more important than ever to observe all possible security precautions. Most people are unaware that 24/7/365 there are hackers around the world hitting their site trying to find vulnerabilities! Unfortunately, as thorough as Google is, it even helps hackers find what target sites are out there and what (vulnerable) versions of software they might be running. Hacking toolkits are also freely available across the internet that help anyone in the world with an internet connection hack away at any site they choose – and often they can even automate the process by trying to hack countless sites at the same time.

When a hacker exploits a site, they cause problems for all of us in downtime, expenses, and other consequences – for your business and ours.

Here's some of the most important security precautions that should be implemented ASAP:

1. Make sure that Wordpress and all its plugins are continually updated – either bi-annually or quarterly. No matter how simple a plugin is, if it has a vulnerability then your **WHOLE SITE CAN BE COMPROMISED**. This is the cost of modern-day CMS websites – they are not projects to be setup one-time and then left alone. **These sites require regular maintenance.**

2. Install security plugins – there's a number of free ones available.

Cheap Wordpress Sites - A Hacker's Paradise

Written by Kalin

Monday, 10 February 2014 08:33

3. For instance - Did you know all Wordpress sites by default have the SAME admin login page? That means hackers simply have to go to that page and start guessing away at any login credentials in the system – and they can automate that process (aka 'brute force' hacking). There are plugins that can be installed and configured to lockout the admin login page so that only those with a secret link can access it.

4. **Use secure passwords – EVERYWHERE!** Simple passwords WILL be hacked at some point. Also, if you use the same password or two for all your online accounts, all a hacker has to do is find it on one account and they'll use it everywhere they can.

5. **DO NOT allow browsers to 'Remember Passwords' for you!** All it takes is a simple script injection attack on a site you go to and the hacker receives a perfect display of your login and password – not just for Wordpress, but for ANY stored password they want to request from your browser.

6. Use only qualified, experienced Wordpress developers. Time and time again, we inherit 'bargain' Wordpress sites because someone who learned how to install Wordpress thought they were suddenly a webmaster and charged an unsuspecting client a 'fantastic deal' minimal fee to create their site. *What is actually produced is often a temporarily-decent-looking hackers' amusement park.* The saying is as true as ever – "You get what you pay for" – and we could share countless examples where those deals cost much more time, money, and headaches than simply doing the project right from the start.

If you need help with updates or plugins, please let us know - Or, if you have a 3rd party working on your site(s), *please share this with them right away.*

Let's all do our part and work together to keep hackers out and our information safe.

{loadposition calltoaction}