Law Firms Using Wordpress: Beef Up Your Security

Steve Matthews | March 2011

WordPress is one of best examples of an open-source community delivering a feature rich and market-leading product. From lawyer blogs to law firm websites, it has become as popular within the legal community as it has elsewhere. But the benefits of open-source software ownership inevitably come with some requisite cautionary advice.

Last January, I wrote about a hacking trend [http://www.stemlegal.com/strategyblog/2010/watchthatpage-response-time-hackers/] whereby automated scripts test every word in the dictionary trying to gain access to your WordPress administration password. This is a problem, not least because at least 55% of all content management system (CMS) [http://w3techs.com/technologies/overview/content_management/all] installs operate on WordPress.

It's becoming clear that all well-trafficked WordPress sites are (or soon will be) a target. Accordingly, law firms need to consider additional security measures to keep their WordPress websites secure. To start, here are a few preventative steps worth considering:

Create better passwords: No matter where you look online, you can find at least one article instructing you *not to use* dictionary words as passwords. There's no need to dwell on this practice — unless you're still doing it.

Deny the search engines access to your CMS: Every website should have a robots.txt file [http://www.robotstxt.org/] installed that clarifies which directories the search engines should index and which should be excluded. Be sure to deny indexing access to the following:

- your images directory,
- any custom scripts, and
- the WordPress *wp-login.php* file and the associated directory structures: */wp-admin/*, */wp-content/* and */wp-includes/*.

While this won't protect your website from a hacker's attack, it will remove any record of your WordPress installation from the search engines, creating a lower profile for the administrative areas of your website.

Verify your website ownership in Google webmaster tools: How do you know for sure that your website has been hacked? There are a number of monitoring tools that will confirm if your page code has been modified (watchthatpage.com is one), but that's not always an intrusion. For a full confirmation on your

(Continued on page 2)

Steve Matthews is the Founder and Principal of Stem Legal, a company dedicated to bringing web visibility to the legal industry. A prolific blogger, Steve co-founded the Canadian legal blogging cooperative Slaw (www.slaw.ca), and maintains his own blogs: Law Firm Web Strategy (www.stemlegal.com/strategyblog) and Vancouver Law Librarian Blog (www.vancouverlawlib.blogspot.com). Steve can be reached at steve@stemlegal.com.

status with Google, try logging intothe Google webmaster tools website [http://www.google.com/webmasters/]. Immediately upon login, Google will produce a status message confirming whether it has detected any kind of malware.

Unfortunately, a malware notice often confirms more bad news: that Google has put your website under a temporary penalty. Until you clean up your website code and remove all associated records from Google's database, your website will remain all but invisible to search engine traffic. Fixing these problems is a lot of work, but on the bright side, Google's response to post-hack re-inclusion has improved significantly in recent years. You can go as far as submitting a manual re-inclusion request, but Google has gotten much better at automatically detecting that the proper fixes have been completed.

Use additional security plugin modules: Each of the following modules will either add protection to the WordPress login area or deliver better monitoring within the WordPress CMS:

Limit Login Attempts [http://wordpress.org/extend/plugins/limit-login-attempts/]: This plugin prevents endless password attempts. If a user fails to login three times, their computer's IP address location is denied from further attempts for 20 minutes. Three such denials on any given day, and that IP address location is locked out for the next 24 hours. Our goal here is to reduce script-based attacks, and the *Limit Login Attempts* plugin adds more variables to the hacking equation. It also offers some additional features that comparable products don't; such as sending an email alert to the website administrator when lockouts do occur. Those IP addresses should then be permanently banned within your website hosting company's control panel.

WP Exploit Scanner [http://wordpress.org/extend/plugins/exploit-scanner/]: This tool will sometimes mistake innocent developments for real security compromises. But if you overlook the few red herrings, you'll find it provides a competent "quick check" of your database and template files. Any type of hidden code insertion will quickly be brought to your attention.

Stealth Login [http://wordpress.org/extend/plugins/stealth-login/]: It's important to remember that these less-sophisticated attacks are both automated and uniform. Hundreds of thousands of websites are being tested, so *any*functional change that stands out from the crowd will help. This is the case with the *Stealth Login* plugin, which renames the default wp-login.php file. Rather than having the same front door as everyone else, customizing your login location instantly changes your entrance and causes yet another difficulty for the automated attack.

WordPress is valuable for its simplicity, but like many open-source solutions, shouldn't be used out of the box without a proper development plan. Website owners must make decisions to customize their website appropriately, and that includes undertaking basic website security.

This article originally appeared on Slaw.ca.