

Are You Doing Your Part In Securing Your Web Site?

By Barbara Camisa

Are You Doing Your Part In Securing Your Web Site?

Barbara Camisa
barbara@businesswebwise.com

Business Web Wise <http://www.businesswebwise.com>

If you are on a virtual (shared) server, you have limited control of security measures on your server. So, most of the security of your server space depends on how security conscious your host is.

There are many factors a web host faces in securing a server. Importantly: proper server configuration (a poorly configured server can make a hole in a good firewall), appropriate scripts such as monitoring software and firewalls installed, all unused ports closed, keep on top of upgrading security patches and only allow SSH (secure shell) to be used instead of regular telnet.

Keep in mind, that no matter how security-conscious your host is, you still should do your part in keeping your web site secure as you possibly can.

The main way you would compromise security of your own site is by installing a 3rd-party script (program) which is not compatible with the server that your site is hosted on. Many who install scripts on their shared servers are not literate enough in the scripting language of the program they're installing, to know if they're installing a script with potential to open security holes in your web site.

When using open-source scripts or those you purchase, use only those that have no known security issues and have an active team of programmers. Bugs are most likely to be found and fixed faster when there are active developers behind the script.

This isn't exactly a cure-all, as quite a few of the pre-written popular scripts can be dangerous as well. There are developers who are not all that security conscious. The best place to go to learn more about the security status of a script is at <http://www.SecurityFocus.com>. Go to their pull-down menu located at the upper right hand side of the page and choose BugTraq. Then type the name of the script and click on search to get the results.

Also, don't assume that all the pre-installed scripts that may come with your hosting account are well written. Go do a BugTraq search on them.

A few other things you can do towards the security of your web site:

- Be sure that anonymous FTP is disabled on your server. Many control panels on hosting accounts have the option of disabling FTP. Some hosts have that feature disabled by default.

- Create a password that is difficult to guess. Use both upper and lower case letters. It's more difficult to guess letters from the alphabet, being there's 26 of them as opposed to only 10 digits with numbers. Use no less than 8 characters, and more letters than numbers. Don't use words/names.
- Change your password once a month.

By implementing the points discussed in this article, you are doing your part in securing your web site.

~~~~~  
Barbara Camisa is a Web Developer, Advisor, Web Host Reseller, Domain Name Expert, and Web Dev Tutor, helping webmasters and web business owners since 1998. Visit her private coaching site at <http://www.BusinessWebWise.com> .  
~~~~~

[Get-Articles.com : 1000's of reprintable business and internet marketing-related articles.](#)

[Submit your article for reprint.](#)