

How "Secure" Is YOUR Web Site?

By Robin Nobles

How "Secure" Is YOUR Web Site?

Robin Nobles
robin@searchengineworkshops.com

Search Engine Workshops <http://www.searchengineworkshops.com>

How "Secure" Is YOUR Web Site?

by Robin Nobles

A few days ago, an incident happened to me that has prompted the writing of this article. I'm sure that if this is an issue for me and one of my Web sites, it's an issue for many others.

With my personal Web site, I use a nationally known Internet Host provider to host it. They've hosted my site for years, and I can't really complain about their services (except that you can rarely find a real "person" to talk to).

However, a few days ago, I wanted to give a good friend of mine, Dave Barry, access to FTP into my Web site to download a particular file. Rather than using an FTP program, he used IE (Internet Explorer) to FTP into the site. The strange thing is, before I even gave him my username and password, Dave was inside the server where my site is hosted!

Dave said that the server, and any sites hosted on that server, were wide open for attack. He was able to see the System 32 Directory, passwords, etc. The good news for me is that Dave is a Certified Internet Webmaster Security Professional Instructor, so he knows exactly what he's talking about (and I don't).

He ran a report to show the vulnerability of my Web site. That report indicated that there were seven high risk vulnerabilities, four medium risk, and two low risk. It also said that it was imperative that I take immediate action in fixing the security issues of the network.

Now isn't this a comforting thought, especially since I've never questioned the security of my Web site? I use one of the top Web hosting firms in the country. This problem should NOT have happened.

I contacted the hosting company, and they're checking into it. At one point, they said, "A little further research on my part found that anonymous FTP is erroneously enabled on your website." Then, in a later e-mail, they changed their mind, "I did misspeak last night when I said that anonymous access was enabled, as I could not upload any files at all, though I could view some directories and files, evidently some relatively innocuous system data files."

Dave disagreed, and he promptly sent me two files to prove how vulnerable and insecure the system is. I sent them those files as well as the security report Dave ran, and they're continuing to look into it.

In my case, though this is a very disturbing situation, it isn't the end of the world. I don't sell anything on my Web site -it's there for informational purposes only.

But, for those of you who actually sell goods or services over the Internet, this could be a huge, and extremely distressing, problem. As Dave said, "I could crash the entire server in a matter of minutes." But, he's one of the good guys wearing a white hat, not a hacker. He's also responsible for 40+ Web sites through his company, all of which are extremely secure.

What can you do to protect your own Web site?

Now that we know how serious a problem this can be, let's look at some ways you can protect your Web site.

1. Contact a security expert like Dave Barry and have him run a security audit on your Web site. Visit Computer Concierge and complete the FREE Website security report. Find out what your Web site security vulnerabilities are, and learn what needs to be done to fix them.

<http://security-report.computer-concierge.com>

2. If the security audit on your Web site proves that you have security issues, and if your host provider can't give you a logical explanation, move your site to a different hosting company. I'm going to move my personal site to Combustion Hosting, where security is a #1 priority, and where I can get personal attention and support. <http://combustionwebhosting.com/products/secureplans/>

3. Ask your current hosting company about their security policies. Then, point them to this URL, which lists The Top 20 Most Critical Internet Security Vulnerabilities. This list was compiled by a list of security experts from the FBI and the SANS Institute. Though you may not be able to understand much of the report, your hosting company will. Not only does the report list the security risks, but it also gives solutions to the problems. <http://www.sans.org/top20/>

4. If you're a "do it yourselfer," visit the U.S. Department of Energy's site which offers a listing of tools for security analysis. <http://ciac.llnl.gov/ciac/SecurityTools.html>

5. Or, consider Retina, which provides excellent security software.

<http://www.eeye.com/html/index.html>

6. SecureNet Solutions also offers products that will run vulnerability reports for you.

<http://www.securenetsol.com/>

The main thing is to learn from my "mistakes" and don't be caught off guard. If you're using a hosting company to host your Web site, make darn sure that the server and your Web site are secure. Visit Computer Concierge for a free security audit. Then, go with a reputable hosting company who places the utmost importance on security, like Combustion Hosting.

Remember: Your Web site is your online business. Don't you lock the door and secure the windows of your "brick and mortar" business? Do you have an alarm system? Don't you think it's important to do the same with your online business?

Robin Nobles, Partner and Trainer, Search Engine Workshops,

(<http://www.searchengineworkshops.com>) teaches 2-day, 3-day, and 5-day hands-on search engine marketing workshops in locations across the globe. She also teaches online search engine marketing courses (<http://www.onlinewebtraining.com>) and has two books currently on the market at Amazon.

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

[Submit your article for reprint.](#)