Hacked!

My Business Was Ruined by a Hacker—Your Web Site Could Be Next

by Dennis Gaskill,
BoogieJack.com

This report details how a hacker ruined the search engine rankings—and business—of a well-established, popular, and trusted web site.

BoogieJack.com, a webmaster resource site since 1997, plunged from the top of search engine rankings to not being found, all within a few short weeks.

Any web site is a potential target. Keep reading for tips that will help you:

- Take preventative measures;
- Learn what to watch for;
- Know what to do if it happens to your site.

This report was written to help others prevent the kind of disaster from happening to their web site that happened to mine. I encourage you to share it with others. You may give it away via your web site, blog, email (no spam) or by other means. You may also include it as a free bonus product with other products you sell, but please DO NOT charge for this report. It needs to be distributed as far and wide as possible. You may also give it away as an incentive—for example, for joining your mailing list. This report may not be altered in any way.

The Early Warning

The first sign that something was wrong was a steady decline in sales. However, as an 11-year veteran of e-commerce, I was used to seeing sales slow down in the weeks leading up to the tax filing deadline. I chalked up the falling sales to that and consumer concern over rising oil prices and the economy in general.

After a few more weeks of further declining sales, it became obvious something more than short-term sales fluctuations was happening. I checked my site stats and was shocked at the downturn in web site traffic. What I first thought was strictly a loss of sales was instead a drastic loss of traffic from the major search engines.

I went to Google to search for my site using keywords and phrases for which it has traditionally ranked on the first page or two, but my site had seemingly disappeared. I clicked down into the search results for 50 pages without finding my site for any of my top keywords.

The First Clue

Concerned that my site was somehow no longer listed with the major search engines, I next searched for pages within my domain only. The first couple of pages brought results, so I knew my site was still indexed, but why had it fallen completely out of search results for keywords I usually dominated?

After clicking a couple of pages deep into the search results, I started seeing pages listed for my site that I knew I had not created. As I kept going, hundreds of pages not of my own making turned up. When I clicked the links for these pages to see if they were really on my site, all I got were 404 errors (file not found).

After discovering this, I logged into to my site via FTP to look for these specific pages, but they weren't there. I did make an important discovery, though. Hidden in a directory I seldom worked with, I found a strange file—a PHP script I didn't place there.

The Hacker's Script

In studying the PHP script, it appeared it was supposed to redirect people who clicked the bogus links in search engines to a Chinese web site, but apparently the script had an error in it so, to the search engines, all the bogus links ended up being non-existent pages on my site.

The links were for all kinds of things: shoes, porn, celebrities, MP3 downloads, pharmaceuticals, jewelry, sports equipment, and hundreds of other topics unrelated to my site.

But where were these links coming from?

A Second Discovery

After looking in all my directories, I next checked the source code of a few pages, which lead to a new discovery. All of the bogus search engine links were scattered throughout most of my pages, but they were placed *after* the closing HTML tags so they weren't visible on the web page if you were viewing my site in a browser. Unfortunately, the search engines picked them up anyway.

It seems obvious the hacker was trying to siphon traffic from my site. It's also possible the hacker was trying to boost his or her own site's popularity.

What the Search Engines Saw

To the search engines, my site had about 300 good pages and about 6,000 broken pages. Search engines penalize sites with too much link rot, and you can't blame them. Broken links in their search returns reduces the quality of their product. With all that link rot on my site, its search engine rankings were effectively destroyed.

With the hundreds of topics included in all the hacker-placed links, my site's tightly-focused theme had been totally destroyed, too. I'd found the answer to why my traffic and sales had suddenly died.

Words cannot express how I felt when I realized that eleven years' worth of work in building a successful online business had been wiped out by one person practically overnight.

The Full Impact

In order for you to understand the full impact this could have on *your* online business, I'll tell you how it affected my small business. My web site traffic went from 3,000 to 4,000 unique visitors a day to about that many in a month. Of course, that meant a huge loss of sales and advertising revenue.

Imagine, if you will, a loss of 60 to 70 percent of your income for a prolonged period of time, with no end to the drop-off in sight. This would have a very serious impact on almost any business, so take this growing problem seriously because the consequences can be devastating.

For us, the bottom line is that we have been forced to put our home up for sale.

Why Your Site Could Be a Target

In general, there are four kinds of hackers:

- Those looking for a real challenge, such as hacking into sites with elaborate security in place. They are looking to pit their skills against those who are the best at preventing hacking.
- Those trying to build a name for themselves within their circle of friends and online acquaintances. They just want to show what they can do—which is usually little more than defacing a web site.
- Those looking to steal something. It could be something as simple as software products, but it could also be something as vital as trade secrets.
- Those looking to create some sort of advantage for themselves, like the one that hacked into my site.

Most of us don't have to worry about the first type of hacker as our sites wouldn't present much of a challenge to them. The last three types of hackers are the ones most of us have to watch out for, and, fortunately, other than corporate spies, they're generally not as determined as those seeking a challenge. They're usually looking for easy marks.

Unfortunately, my site was an easy mark. I'd never had a hacker problem before, and I have a good reputation online (and off), so like many people do, I told myself, "It won't happen to me."

Well, it did happen to me, and it could happen to you, too, if your site is an easy mark. *It has nothing to do with you or me—it's our web sites that are the target.* These hackers don't care who we are, and they don't care what damage they do. We need to see clearly that we are not immune just because we happen to be a good person.

14 Tips on How to Make Your Site Less Vulnerable to Hackers (and Avoid Becoming a Victim)

It's highly unlikely that preventing your site from being hacked is even possible if the right person is determined enough. After all, if the Pentagon and NASA can have their computers hacked (and they have been), one should assume that any computer online can potentially be hacked.

Hacking can be made more difficult though, which is often enough to send most hackers in search of easier prey. I don't pretend to be an expert in preventing a hacker attack, but I will share what I know with you now:

1. Make your password as difficult as possible for software or humans to guess. Some hackers use software to blast user name and password combinations at a web site. This is known as a "brute force" attack. The longer your password is, the harder it will be to crack.

Ask your web site host how many characters can be in your password and what characters are allowed, then change your password to one that uses as many characters as allowed and also uses a healthy mix of upper and lower case letters, plus numbers and special characters if they're allowed. Each additional character makes the password exponentially harder to crack, so making it as long as possible is crucial!

> Using only the lower case alphabet, there are 456,976 combinations of letters possible in a four-letter password. A five-letter password has 11,881,376 combinations. You can see how a 12-letter password that uses lower case, upper case, numbers and special characters would be infinitely harder to crack. My calculator doesn't go that high.
>
> DO NOT replace characters with similar looking special characters, such as changing "password" to "p@$$w0rd". The better hacking tools have a "leet" feature, as it's called, which substitutes special characters for similar looking letters when it's trying dictionary words and proper names. In fact, your password should not spell any word at all. That will render dictionary attacks ineffective.

2. Make sure your passwords for all administration (FTP, control panel, software admin, and email accounts) are complex and difficult to guess. Use a different password for each application. If a hacker cracks one, he or she won't have access to everything else.

Don't choose a username like “admin” or “administrator.” If you use something that simple, a hacker is already halfway in. I've even seen people use "password" for their password. Sure, it's easy to remember, but the easier it is to remember, the easier it is to guess.

3. Use a web site host that uses "CAPTCHA technology” to gain access to your control panel. This will help prevent brute force attacks from working because the software can't read the CAPTCHA image. You still want to use the max password mentioned in Item 1 as well. *(CAPTCHA is*

a type of challenge-response test used in computing to ensure that the response is not generated by a computer. See Wikipedia.com for more information.)

4. In your control panel, disable anonymous FTP, or ask your host to do it if you can't find how. I never set my site up for anonymous FTP, but learned too late that it was set up that way by default. That could have been the opening the hacker found.

5. Visually inspect your web site directories, looking for files and folders you don't recognize as your own. Look in every folder on every level. How often you do this is up to you, but in many cases, the sooner you can find hacker-placed files, the less damage will be done.

Also visually inspect the source code of your web pages looking for inserted links, javascript, or other code that's not yours. Remember to look *after* the source code as well. I learned the hard way that the search engine spiders don't stop reading the page when the HTML element is cancelled; *they go all the way to the last character in the file.*

If you have a lot of pages, you'll probably want to break this task up and do a comfortable amount in several sittings rather than making an overwhelming chore of it in one sitting. If your site is too large for this step, at least make random checks periodically.

> *IMPORTANT: Before opening any unknown files you discover, be sure you have antivirus software running on your computer or you could accidently open a hacker tool that could give the hacker access to your computer. Good antivirus software will prevent the file from opening and notify you of the reason it was blocked.*

6. If you use any commercial scripts, keep them updated. Updates often include security patches against newly discovered vulnerabilities.

7. Use a web host that regularly updates its server software. As in the item above, updates often include security fixes.

8. Avoid open source software. Since open source software means the source code is basically available to anyone who wants it, that makes it

easy for hackers to study it for vulnerabilities. Similarly, do not install any software that is not from a trusted source, especially freeware. Software can contain a Trojan which allows a hacker to access your computer. They can hunt for the information they want from a distance if your computer is infected.

9. Research vulnerabilities in PHP applications. While I'm not an expert in PHP, I've seen many PHP vulnerabilities pop up in search results. If you're unsure about the software you're using or thinking of using on your site, try searching for it by name and adding "+exploits" to the end. You may be surprised at your findings.

10. Run only the software you need. The more software running on your web host's server, the more opportunities there are for a hacker to find a way in.

11. Do not use public wireless hot spots for sensitive computer work. If you use a laptop to access your web site or process any sensitive information, it will be easy (VERY easy!) for an experienced hacker to intercept your data.

12. Check your web site log files regularly to look for suspicious activity. In researching this topic, I found several Web pages that advised web site owners to regularly check their log files for suspicious activity. What I couldn't find was what to actually look for. No one that advised looking for suspicious activity defined what it was. The only thing I did find is that almost everyone that comes to your site will do so through your domain name, so if you see multiple accesses or access attempts using an IP address rather than your domain name, there's a good chance it's from a hacker's port scanning software.

13. Open an account at Google Webmaster Central to monitor which pages are indexed. If I had done this before my site was hacked, I could have spotted the hacker-inserted links much faster. There are many other good information resources available to you with a Google Webmaster Central account (which is free), including information on security threats.

You can also use a link checking service or link checking software to monitor your site for broken links. A quick search at Google for "link checking service" should provide you with several to choose from. A quick search at any leading shareware site will turn up software you can use if you want to do it yourself.

14. And of course, there's the obvious—never give out your user name and password to anyone unless you initiate the communication, and then, only if you trust them AND they have a need to know.

Two Additional Measures You Should Take

1. Keep up-to-date backup copies of your web site and databases so you can quickly restore your site if it is successfully hacked. (If you use databases, you'll have to take special measures to back them up. Ask your web host if you're unsure of how to do this.)

a) DO NOT count on your web host's advertised daily backups. This often isn't reliable. If you have the proper files your web host can restore your site easily, including the databases. If not, you'll be starting from scratch with any program that uses a database.

b) When you create backup files, make sure that you're not saving a hacker file or an infected file. If your site has been hacked, nothing in the system can be trusted at that point. Hackers sometimes replace common server utilities with Trojan versions, giving themselves a back door even if you've replaced the hacked web pages.

2. Use a hardware firewall and antivirus software program for your home computer, and keep it updated. Your personal computer could be the easiest to crack, allowing a hacker to access any information on your system, including login and password information. Install a good anti-spyware program, keep it updated, and use it regularly.

8 Recovery Steps

I have published this report in June, 2008, offering it free of charge on the Web while I'm still in the recovery process. My hope is that it will help others avoid the kind of pain and loss I've experienced. I believe that good will always returns in some form to its ambassadors.

At this point, it's too early to tell if my recovery strategy is working; I can only tell you what I've done in an attempt to recover my good standing with the search engines. I know this is going to take time, but it's my nature to remain hopeful.

Following are the specific steps I took to begin the recovery process on my hacked site—a list of things you should probably do if your site is ever destroyed by a malicious hacker as mine was:

1. I changed hosts to one that uses CAPTCHA technology to log into the control panel and has better security procedures. That's not a search engine recovery tactic, but hopefully one that will help prevent another successful hack attack. All the other tactics would do little good if my site were still located on a vulnerable host.

2. I redesigned my site from scratch to be sure I didn't miss any hacker files or hidden code, and also made changes to the content of each page so the pages would be updated for the search engines.

3. As I redesigned, I eliminated all my side topics and focused on my main theme (web site design) to help recover the strength of my site's theme.

4. I created an XML site map to help search engines index my site properly and more quickly. (They seem to favor XML site maps these days.) I submitted my site map to Google through Webmaster Central, which other search engines pick up from Google.

5. Still within Webmaster Central, I asked Google to reconsider my site. A reconsideration request allows owners of web sites that have been penalized or suffered a serious loss in rankings to ask Google to take a

fresh look at the site to hopefully get any penalties removed. (As discussed in point 13 above, Webmaster Central offers webmasters many different resources, including Webmaster Tools where you'll find the reconsideration request form.)

Of course, you will want to correct the situation that resulted in the site being penalized in the first place. For me, it was removing all the dead links that the hacker added. (To better understand what causes ranking problems, check Google's list of things that can cause penalties.)

6. I went back to work at gaining new links. There's a misconception that only links from similarly themed sites help your search engine rankings, but Google considers any link a "vote" for your site (unless it's from a bad neighborhood, *i.e.,* gambling sites, porn sites, etc.).

7. I disabled anonymous FTP (refer back to Point 4 above). Although not a search engine recovery tactic, this will help prevent further attacks. I don't know why a host would enable that by default since most don't need it, so be sure that feature is disabled on your site unless you do have a need for it.

8. I've issued a press release to help get this report into your hands through the mass media. (This cost me a pretty penny, so I hope you'll take this information seriously.) My thanks to author and editor Barbara Brabec for her complimentary editing and formatting of this report, and to Traci Hayner Vanover, publisher of *Create the Dream* magazine, for her generous assistance in writing and distributing my news release.

A Vulnerability Not Yet Mentioned

Having said all the above . . . it's possible my site wasn't hacked directly. The hacker could have attacked the server, which could have easily infected all the web sites hosted on that server. That's why choosing a GOOD web host that takes the matter of security seriously is so important. If the host doesn't practice good security measures, it may not matter at all what you or I do to protect our sites.

When I tried to elicit help from my Web host to find how the hacker gained access to my site, I was told they weren't interested, that security was *my* concern. That's another reason I changed hosts. Web site hosting is a partnership, and both parties need to take security seriously.

One Last Thing

This report doesn't cover every aspect of hacking and all the dangers from the dark side of the Net, nor does it cover all the preventative measures that can be taken. If your web presence is important, I would encourage you to do further research on your own.

I also recommend reading Trends in Badware. (If the link should go bad, visit StopBadware.org and search for the report there.)

Three Ways You Can Help Me

I truly hope you have found this report beneficial. I wouldn't wish what happened to me on anyone. If you'd care to help my small business recover, I've listed three ways you can help below, and I thank you in advance for your kindness.

1. Share this report. As indicated at the beginning of this report, you can give it away from your web site, to your mailing list, or simply share it with family and friends who have web sites of their own. You may also use it as an incentive or bonus product, but please don't charge for anything for it. This needs to reach as many people as possible.

2. Link to my Boogiejack.com web site. Here's the HTML code:

BoogieJack.com Web Design Tutorials

If you want the link to open in a new window, add the following code to the link after the title attribute and value: *target="_blank"*

3. Join my affiliate program and earn 35 percent from any sales you refer. You read that right. I'll pay you to help me. The affiliate program is administered through a third party so you're assured of honesty and timely payments. If you'd like to join my affiliate program, you'll find the information at i-Webmaster.org. (http://www.i-webmaster.org/affiliates.html)

Again, thank you in advance if you find it possible to help my site and business recover. As I said before, as surely as the seasons return, good will always returns to its ambassadors.

Whether you're in a position to help or not, I truly hope this report will help prevent your web site from being hacked. If you are reading this long after it was first published, understand that its general content will be applicable for years to come. However, if you're interested in what other actions I have taken to help my site recover, or in the results of my initial recovery efforts above, I'll be publishing updates in my newsletter. You can sign up for it or read the latest edition at i-Webmaster.org. (http://www.i-webmaster.org/newsletter.html)

Explanatory Note

So you're not confused by the two different domain names . . . BoogieJack.com is my primary web site and the source of most of my business.

The i-webmaster.org site is the member site for BoogieJack.com. It features about 100 standards compliant HTML and CSS tutorials, 31 handy reference charts, reprintable content, web graphics, exclusive fonts, free software, free ebooks and more.

The newsletter is in the public area, so you don't have to be member to read it.

About the Author and BoogieJack.Com

Begun as a hobby site in 1997, Boogiejack.com quickly became a full-time Web business for Dennis Gaskill, who has developed a reputation for honesty, fairness, and for his teaching skills and writing, which always includes a generous dose of humor.

Thinking "outside the box" from the beginning, Dennis quickly rose to prominence as an expert in his field. As a founding member of i-cop (the International Council of Online Professionals), and currently serving his second 3-year term as a member of Mid-State Technical College's Marketing Advisory Board, he has also established himself as a home business expert.

Dennis is the author of *Web Site Design Made Easy* (Third Edition), a web design book now being used as the teaching text in hundreds of colleges, tech schools, and high schools.

His award-winning, original content ezine about web design and life design--*Almost a Newsletter*--was named the Best Ezine of the Year by an independent newsletter review service and also named a Top 3 Ezine in *Writer's Digest* magazine.