What to Do if Your Site has been Hacked

What if you uploaded a blog, committed to backups, installed all the right plugins (like a firewall) and kept WordPress up to date and still get hacked? In this article, Linda explains how to handle that situation.

Expect a Hack

If you're running a WordPress (WP) blog, you can expect to a hack attempt. Even the least visited WP site on the Web has potential for a hacker's experiments. While I mentioned in earlier articles what you might do to avoid an attack on your blog or your database, I want to approach this subject again in more depth, with plenty of links to get you straight on what you need to do if you're hacked, and what you can do to prevent harm to your site.

The problem with hacking is that you may experience one of four (or more) problems, and two of them may not be immediately visible to you:

1. Your site is hacked, but you don't know it. The way you find out is through friends who tell you that your site isn't showing up (although you can see it just fine because of your cache).
2. Your site is hacked, and you still don't know it, until your Web host contacts you to let you know that either your blog or someone else's blog/database has been compromised.
3. You see immediately that your site has been hacked, but no one else seems to notice.
4. It's apparent to all concerned, including you, that your site has gone missing or is replaced by the Dr. Doom Death Flag (I made that up).

I'll cover all four issues below, along with a wide variety of solutions to help you overcome simple attacks against your site.

If your site has been hacked, and you found this article in hopes that I might have some solutions for you, the best thing I can say to you right now is: "Take a deep breath and calm down." Whatever the issue, you may be able to reconstruct your site before night falls. In the meantime, you need to stay calm so you don't make any mistakes.

First Step: Scan YOUR Machine

Sometimes, you may be the culprit behind your 'hack' by introducing malware through a compromised computer system (desktop, laptop, mobile, etc.), especially if you're running a PC and/or a Windows system. Run a full anti-virus / malware scan on all machines that you use to upload information to your blog.

You may need to change virus software, if your machine allows you to do so (some viruses prevent users from deploying new anti-virus software), to check your machine. Your current software may not have caught the hack. If you cannot upload new software to test your machine, take it to a professional to get their opinion.

Check with Your Hosting Provider

I host with Media Temple, and they recently came under attack and it affected many blogs on their servers (the same attackers also hit other servers, not just MT). Since they use shared servers, this was a spectacular problem. But, Media Temple took it on, checking everyone's databases and changing the system so that it is more difficult to gain access to those databases.

In another case, another blogger had made his site vulnerable, and the database attack spread across the container where all my blogs were located. I lost many images, databases and sites, which needed to be

rebuilt. Shared servers ARE an issue; however, it's a trade-off for a busy site, as shared servers can carry the weight of a spike in traffic, heavy traffic and ease of use.

It's up to you to decide which server you want to use. I'm staying with MT, as they are tops at what they do, and their service department is the best I've ever dealt with. But, I also use other tools to safeguard my sites, and I'll let you know about those tools in a moment.

Read these Articles

Although this article is from 2008, it contains some key information that you might need for future protection. Several point to take note about include updating your WP files, making sure that your backups are done as often as you need them and to make sure that no "backdoors" or malicious code are left on your system. heck with your hosting provider.

If you discover you are hacked, make backups of your databases if they still are there, but be sure to label them as a "hacked" site backup. You may need to resort to a previous backup (but, even then you might check that backup).

Oh, and I'm sure you want to know how to completely clean your hacked WP installation, right? Just follow the advice in this article. Another article, Removing Malware from a WordPress Blog (2010), also explains in detail some steps you may need to take. Those articles are too detailed to include here, but they have been up for several years (even the one from 2010 has been up and updated).

You also want to check your .htaccess file for hacks, as hackers can use that file to redirect to malicious sites from your URL. Once your site is recovered, check your site logs to see if you can discover how the hack took place. Open source tools like OSSEC can analyse your logs and point you where/how the attack happened.

What's Next?

If you can restore your databases, then consider wiping the current WP files off your server and reinstalling WP from a freshly downloaded .zip file. Before you restore you databases (if you can restore them), check to make sure you have installed the latest version of WP.

If you can restore known, clean backups of your WP database, do so now. Be sure to replace your plugin and theme files (fresh applications, rather than ones that have been stored on your computer might be a wise idea).

Be careful about uploading backup files, as you may not know how long your site has carried this hack. Check all backups thoroughly before you upload them again. You may need to go back a week, a month or several months (hopefully not) before you find clean files. But, if those backups can keep you from losing your entire site, then you might realize how valuable those backups are to you.

About Passwords and Key Generators

When you upload a new version of WP, change your password. In fact, you and other users at your Web site should change passwords every week at least. Truly paranoid people might change their passwords twice per week.

Also, if hackers have stolen your password and are logged into your blog, they will remain logged in evern if you change your password. This is possible, because their cookies remain valid. To disable those cookies, you need to create a new set of secret keys.

The way to change your keys is to first visit the WP key generator to obtain a new random set of keys. Then, overwrite the values in your wp-config.php file with the new keys. Another article that might help you with

understanding the key generator for your wp-config.php file is "Your WordPress Site Can Get Hacked If You Don't Have This."

Finally, if you are changing passwords on a regular basis, change them for your FTP, MySQL and at your online bank while you're at it.

Conclusion

One of the best plugins I've ever used to block attacks is WordPress Firewall Plugin. This plugin whitelists and blacklists pathological-looking phrases based on which field they appear within in a page request (unknown/numeric parameters vs. known post bodies, comment bodies, etc.). In the process, it can detect, intecept, and log suspicious-looking parameters — and prevent them compromising WordPress.

You can set this plugin up to email attacks to you...but don't become alarmed when you see the attacks, especially if you get more than five in a row. Robots, smart as they are, are dumb when it comes to attacking a site. They may try in several places within your site before they move on. And, although you know about the attack and may even be able to acquire an IP address that shows the attack's origin, I learned that the IP may be temporary or even a fake one that was set up for hacking.

The only thing you can do, possibly, is to notify your host server about the IP address. But, don't do this too often, or your host server may begin to wonder why your site is being attacked. Mainly, the email updates are to assure you that the firewall is working. Bravo, and yay.

Otherwise, keep backing up your site, through whatever tool makes you happy, and proceed with your blogging.