The 10 Ways to Protect and Restore Your Website

Your quick tip guide on protecting and restoring your hacked site

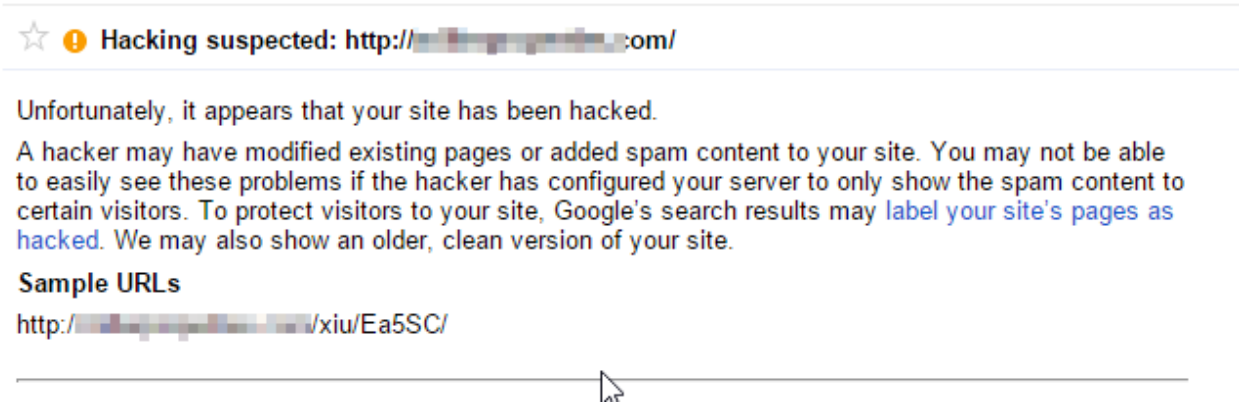
from

www.Cohlab.com

By

Cliff Robbins

1. It's important to remember that the first thing is to remain calm. Take a deep breath and remember that you are not alone. Things will turn out OK so don't panic. Shortly after that crucial first step, be sure to change all current passwords to something new. This includes any passwords for email, ftp, CMS logins (such as Wordpress), and all database accounts. The goal is to stop the hackers current access as soon as possible.
2. If you are using a CMS, and you have the capability to do so, change the login URL as well. Furthermore, check to see if you can find any suspicious accounts in the various locations and remove or block them. If you are using Wordpress, we recommend installing the plugin iThemes Security (its free).
3. Google Webmaster can be a great help. It provides helpful tools for your site including health and malware checks. If you use Google Webmaster and were notified by them of any suspicious files, you have the ability to find the files Google has identified. Check the files and remove them if they are a verified concern.



4. Take the time to review your code and site files often, especially true if you manage or host your own site. There are three areas of code that hackers most often attack. They are .htaccess files, .php files, and media files. These file types are also much easier to reach when you have a lot of old or unnecessary files sitting in your file folders. Using these, hackers can insert hidden links to malicious websites, embed malicious code directly into them, or to encrypt them to disguise malicious links and malware even if the code itself seems harmless.
5. It's a good idea to perform a complete check of your website regularly. Make sure all links are working properly and your pages are appearing as they should.
6. Backup your website and database daily as well. Also, complete a weekly backup that is sent off-site. It's a good idea to have several previous backups saved securely in the event a full restore is required to fix things if an attack does occur. If you are using Wordpress we recomend using BackupBuddy or setup a conjob with php to automate the backup.
7. Even if you are hacked, make a backup of your hacked site as it is before changing or deleting anything. Just make sure you don't replace a previous "clean" backup with the compromised backup, keep them separate. Following the backup, find and remove any malicious code or files if possible. Then check your site links and pages as above. If it is not possible to find them, you may need to remove your entire website and upload a previous backup. A

program called Beyond Compare is helpful because it allows you to compare the 'clean' files to the current files on the website. You should still do a full check of your website after a complete restoration as well to make sure nothing was missed.

8. Finally, when your site is restored, submit to Google Webmaster that the website has been cleaned up.
9. There are also some security software tools available. These utilities can scan your code for you, and may be helpful as an extra layer of protection even if you are able to check the code yourself. Some of these tools involve a one-time fee or scheduled payments. Others, such as Google's Safe Browsing Checker are free. By typing the URL *http://www.google.com/safebrowsing/diagnostic?site=yourdomain.com*, and replacing "yourdomain.com" with your real domain will provide you with a valuable report from Google in seconds. It will list any suspicious activity, and if your site has been a distributor or go-between for any malware.
10. It is also important that you ensure the software used on your website is up to date. If you are using a CMS with any plugins, you will also want to ensure that those plugins remain up to date as well.
11. Bonus - Another plugin for Wordpress that can assist if you have been hacked or to assist with preventative maintenance is the Anti-Malware (get off malicious scripts) plugin.
12. Bonus - This may seem redundant, however don't make your password admin123. You need to get a bit more creative with your

passwords to ensure you don't get hacked. If you have trouble remembering your passwords, we suggest using software called LastPass to remember them for you.