BIZCOMMUNITY

Telltale indications that your WordPress site been hacked

By Charles Mburugu

2 Jan 2018

Hacking has become a growing concern for website owners all over the world. Every year, thousands of WordPress websites are either compromised or hacked.

If you don't secure your WordPress site properly, you might find yourself being a victim sooner or later.

Here are some indications that will help you determine whether your site has been infiltrated:

1. A defaced homepage

This is one of the clearest indications that your site has been hacked. Most hackers will not leave such obvious signs since they want to cover their tracks. However, some will announce their presence by defacing your website. They might leave a message on your homepage as a warning or even attempt to extort cash from the website owners.

2. Inability to login to WordPress

There are several reasons why you might be unable to login to your WordPress admin area. First, it could be simply because you have forgotten your username or password. However, it could also be a sign that your WordPress site has been compromised. When hackers access your site, they are likely to delete your admin account. This means that you won't even be able to reset your password.

3. Spam user accounts

If spam registration protection is not enabled on your WordPress site, you might see some spam user accounts being created. However, such accounts can usually be deleted easily with one click. However, if spam registration protection is enabled and you see new user accounts, then your site might be compromised. In some instances, it might be impossible to delete such accounts from your admin area.

4. Drastic decline in website traffic

If you notice a sudden decline in your traffic, then it could be an indication that your site has been compromised. There are numerous trojans and malware that can intercept your traffic and take it to spammy sites.

Your website traffic could also drop if Google blacklists your site for phishing or malware. Therefore, be sure to use Google's safe browsing tool regularly to check if your website is safe.

5. Inability to receive or send WordPress emails

WordPress hosting usually comes with free email accounts. You are allowed to send and receive emails using the host's mail servers. However, if you find yourself unable to send and receive emails, it is possible that your mail server has been hacked.

6. Incorrect search results

If a Google search for your website displays the wrong meta description and title, then you might be a victim of hacking. When you look at your site, you might still see the correct description and title. This means that the hacker could have injected malware into your site which modifies how it appears to search engines.

7. Strange scripts and files on your server

There are several site scanning plugins that can notify you when malicious scripts or files appear on your server. Such files are usually found in the /wp-content/ folder. In most cases, these files go unnoticed since they are named like normal WordPress files. This is why you need to carry out a regular audit of your website's directory and file structure.

ABOUT CHARLES MBURUGU

HubSpot-certified content writer/marketer for B2B, B2C and SaaS companies. He has worked with brands such as GetResponse, Neil Patel, Shopify, 99 Designs, Norton, Salesforce and Condor. Portfolio: https://charlesmburugu.contently.com/ LinkedIn: https://ke.linkedin.com/in/charlesmburugu

- Telltale indications that your WordPress site been hacked - 2 Jan 2018
- Are you making these WordPress blunders? - 17 Jul 2017
- Tips for maintaining your WordPress business site - 25 May 2017
- Selecting a domain name: blunders to avoid - 3 Jun 2016
- Four Windows server backup solutions - 23 Dec 2015

View my profile and articles...