Oceania
Business Solutions

Some of the Ways Hackers Might Have Gotten into Your Website

The list below gives some common ways websites are hacked, as well as a few things you can do to protect your website.

Your Web Host may be Vulnerable

Our policy surrounding hacked websites has stood the test of time and we have only ever known hacks to occur on random sites. Certainly we have never seen an entire server affected. Upon investigation the causes of the hack have always been due to some combination of the methods listed below.

Dedicated hosting plans (Please call 1300 301 990 for more details) are available for anyone who would like to move away from any perceived risks in hosting their site in a shared hosting environment. Please do note however that the same issues as are outlined below will still apply.

Your Computer or Your Web Developer's Computer Has Been Compromised

It could be that root of the problem lies with computer used to access the backend of your website and not a vulnerability of the website itself. Hackers can infect a computer with malware, enabling them to steal saved passwords or infect files as they are uploaded to a server.

To prevent this from happening, the computer used to access a website via FTP or SSH should be regularly scanned for spyware, viruses and malware. Additionally, unencrypted passwords should not be stored in FTP programs.

Your Passwords Have Been Leaked or Are NOT Strong

When it comes to passwords, they can only protect your website when they are strong. This means that passwords must adhere to the following criteria.

1. Use twelve digit alpha-numeric combinations- something like: JK,y=y u%TyG3 or similar non-words. Absolutely NEVER use the above “example” password.

   Update your password in all “Applications” includes and is not limited to:

   - Cpanel
   - email accounts
   - any CMS applications you are using like WordPress, Joomla or Soholaunch etc
   - Your sub-user accounts in any CMS you have installed and who have password access should also be updated.

2. Have a different and unique password for each application as when hackers can crack one – all other logins with same or even similar passwords will be vulnerable

3. Private. Be careful about who you share your passwords with and how you share the passwords. If sending a password via email, consider transmitting it as an image instead of via plain text.

4. Regularly Changed. By periodically updating your passwords, you lessen the chance that a leaked password can be used to gain access to your website.

Additionally, if your website has been hacked, make sure that the hacker has not created any unauthorized accounts that could be used for subsequent hacking attempts.

Your Content Management Software Has Security Holes

Content management systems (CMS) such as Joomla, Wordpress, SohoLaunch etc are used by websites to make it easier to manage content or maintain other functionality. But there is a big downside. Regardless of which CMS is used, there are always security holes that can be exploited by hackers.

To keep a CMS as secure as possible, there are certain basic recommendations that you or your developer should always follow:

- Hide your CMS version and make sure it is not displayed in HTML markup.
- Verify file permissions are correct and not too permissible.
- Hide your directory structure.
- Do not let two or more applications share the same database.

Additionally, the programmers behind your CMS may release updated versions or patches when vulnerabilities are discovered. And while it may be expensive or time-consuming to keep your CMS updated, it is worth the effort. After a new update is released, details about security flaws in the older version are often released. And what this means is that if you don't upgrade to the latest software version, hackers will literally have a roadmap to getting into your website.

Your Code is Poorly Written

Poorly coded website forms, dynamic pages, and CMS plugins/modules could result in easily exploitable security holes. To prevent this from happening, make sure that all custom code is fully tested and coded with security in mind. And before installing a 3rd-party plugin or module for your CMS, review the feedback and/or take a look under the hood to make sure that the plugin is well-coded.

No Website Is Hacker-Proof

Even after employing the best preventative measures, it is still possible for your website to be hacked. As a result, it is a good idea to regularly monitor your site and its log files so that you know if any changes have been made to its files or if hackers are trying to gain access. There are also a variety of 3rd-party monitoring tools which can be used to alert you if your website has been compromised.

Expert advice - See Data Protection Tips - a very worthwhile read!

https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe