Hackers

Home [1]
Viruses [2]
Back-Ups [3]

HACKERS

Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose. People who engage in computer hacking activities are often called hackers. Since the word "hack" has long been used to describe someone who is incompetent at his/her profession, some hackers claim this term is offensive and fails to give appropriate recognition to their skills.

Computer hacking is most common among teenagers and young adults, although there are many older hackers as well. Many hackers are true technology buffs who enjoy learning more about how computers work and consider computer hacking an "art" form. They often enjoy programming and have expert-level skills in one particular program. For these individuals, computer hacking is a real life application of their problem-solving skills. It's a chance to demonstrate their abilities, not an opportunity to harm others.

HOW TO PREVENT HACKERS:

1) Comment Attacks

Comments are one of most prized features for blogs, and helps create a great relationship between the author and the reader, and also between readers in the wider community. It would also be easy for someone to insert HTML code that causes trouble.

You need to "validate" the form input before it's accepted, to strip out all but the most basic HTML tags, for example and also if you're using WordPress – you can utilize the "Keyword Filter" to block out any harsh words that might raise an issue or two.

2) Unsolicited Installation of Scripts

It can be dangerous to install third-party scripts and programs on your website unless you understand what they are actually doing. Even if you don't fully understand the programming, you can read through the code and look for tell-tale signs such as references to third-party URLS.

You can also visit community forums such as SitePoint and DigitalPoint to ask around for better advice.

3) Avoid Scam/Spammy Websites

In a desperate attempt to get visitors you might consider try extensive viral marketing and other means of gaining the attention, this may cause a few people in the wrong community to raise a few eyebrows.

The last thing you need as a settled web-master is to cause a stir amongst the wrong people. Stay away from websites and especially forums that offer "information" or "get traffic quick" that uses illegal spam lists and such.

4) Clear the Cookies!

Personally, I use a lot of public computers to blog and do other online activities, maybe because it's convenient or

my unreliable ISP crashed on my once more. Inevitable there's many, many webmasters like me that use public services for either a quick access or regular work.

Just don't forget to clear out the cookies and cache before you leave! Even if the service provider claims, "no tracking of privacy" or anything along those lines, a quick clean before you leave wouldn't hurt anyone.

5) Prevent illegal farmers' from "harvesting" your lists

Hacking techniques are used to "harvest" email addresses, which are then used by spammers and other hackers for malicious activities. If you are storing email data on your website, for what-ever required reason, make sure it's stored in a secure format, such as a MySQL Database.

Most top-CMS such as WordPress and Joomla make this compulsory but there's many self written CMS's too. If your script simply writes data to a text called "emails.txt" it won't be long before someone sniffs it out.

6) Make sure your files are using the correct CHMOD Permissions

CHMOD File Permissions assign a specific value to every file/folder on your server, which allows different levels of access.

CHMOD Permission range from 000 (No access) to 777 (Full access), you must decide which files get what permissions, but be warned that some third party software require higher permissions to operate properly. You need to balance out features with security and make an informed decision.

Using a FTP you can change the permissions given to each file/folder on your server. This is vital to ensure any unauthorized access to your content is comprehensively denied.

Note – Make sure your CHMOD settings work with your current web-hosts. Some hosts prevent '777' for security reasons.

7) Don't use Generic Usernames

Using common words for usernames such as "admin", "administrator" or "Site Owner" can cause many implications because you are simply making the job of the hacker's a lot easier. By using such common words for your username, you are incredibly increasing the success rate of the hacker by at least a few points of a percentage, which is consider a lot where only one answer can be right from an unlimited range of combinations.

8) Securing your Ports

To put in simple words, a "PORT" is used to access data from outside the server. It also utilized to transfer data both ways, into the server and also outgoing. Most of this activity is behind closed doors and happens automatically, and only trained professionals tend to play around with such details.

Nevertheless, ports are constantly opened & closed for easy-access, for programs such as a FTP (File Transfer Protocol). This can be favorable for any hackers attempting to access your sensitive files, so make sure any unwanted ports are 'properly closed.'

9) Updated Security Patches

If your web hosting provider hasn't already done so, you should check that all the latest security patches for various aspects of the service are properly installed. As you might know, WordPress (self-hosted) is one of the most popular Content Management Systems out there on the market.

It is used by millions- so it's not surprising to see many hackers working day/night trying to hack it. Updates and patches are regularly released, so keep an eye out for all your plug-ins/core files.

10) Use Strong Passwords!

The number one technique you can possibly implement. Hackers are experts at programming computers to plough through huge amounts of data very quickly. That's the reason longer passwords are more secure; the number of possible combinations grows exponentially with every extra character added.

Hackers employ a technique called "dictionary attack" where they repeatedly try username and password combinations by running through hundreds of common words, phrases, numbers and combination them till they get lucky. It's important you use random strings like "j@m13s(!)" instead of perhaps "jamie123˝

Source URL: https://theingots.org/community/node/25154

Links
[1] https://theingots.org/community/node/22882
[2] http://theingots.org/community/node/24580
[3] http://theingots.org/community/node/25621