Article published on June 22nd 2012 | PPC Advertising

Imagine the following scenario:

Youâ€™ve just had a brand new website built for your business, and before you know it you are getting a warning from Google that your website has been hacked.

It would, undoubtedly, evoke anger towards the pests that are hacking your site, and resentment towards the guys who built your site and, in your mind, didnâ€™t put the measures in place to avoid this from happening!

We have, on numerous occasions, come across â€œVirus Attacksâ€• or â€œHacksâ€• as they are someti called. They commonly occur in Open Source Websites & are one of the few risks that come with using Open Source platforms.

While your IT Team should be able to fix this predicament in almost all cases they have very little to do with the originating problem (i.e. equipping the site against these types of attacks). In general, a Google warning is the first notification of such a problem to them, as well as to you.

What is at Risk?

The most common reason for a website hack in the case of a small to medium scale website is link-farming for SEO gains. Moreover, Hackers go after E-commerce sites for customer & possibly credit card data. Email addresses of customers are also up there in the list of things hackers are after.

How it Works?

There are two common ways that hacks occur. Of course, there are many other types of hacks as well but these two are the most common in small to medium sized websites:

1) SQL Injection

In this way, the hacker is very familiar with the database schema (or data model) of the site and creates a script that enters malicious code directly into the database table that carries the page content.

SQL Injection can occur in most open source platforms because open source systems database schemas are common public knowledge.

In Hosted platforms the risk of SQL injections is close to negligible as the databases are well protected & use connection methods / models known only to the company that runs the platform

Cleaning a SQL injection means searching the database and removing the code, which at times can cause service disruptions, layouts or breaks in website functionality?

2) File System Infection

In this way a hacker enters via an FTP or other channel for server vulnerability and actually modifies the source code files in order to place malicious code into the system

This type of hack is very tough to fix because the scripting can be intelligent, spread quickly and continue to replicate even after clean-ups. Sometimes hackers will plant â€œreceptorâ€• scripts that go undetected and look very normal until they connect to the hackersâ€™ own servers and pull down malicious code.

Cleaning this hack means effectively looking at each file individually and systematically cleaning up the code. Your IT team can undertake a mass â€œFind & Replaceâ€• approach to clean the code if they are able to locate the malicious code, but shortcuts almost always mean that they will miss out the â€œreceptorâ€• script that is infecting the files. This effort is extensive and can involve various elements:

Your base WordPress install version 3.0.1 has 756 Files! Version 3.4 has 1400+ files!

Your Joomla 2.5 install has 6000+ files with a standard set of components & plugins!

Sometimes clean up can also affect the functionality of the site or layouts, which result in a lot of lost productivity to the site

How do we fix it?

While your IT team doesnâ€™t bear the responsibility for the hacking, which is, in many cases, hard to predict and potentially unavoidable, there are certain measures that can be taken to prevent it from happening (please see details in the next paragraph). For starters, the password selection for the Admin panel or FTP must be as hard to detect as possible. Once the hacking has taken place you will have to work with a very skilled System Administrator and a Programmer (both skills are a must) to clean the infected website and reestablish functionality.

Once this action has been completed, the site must be re-submitted to Google as there are high chances that Google still has it detected as an â€œinfectedâ€• site.

How do we prevent hacking from happening in the first place?

There are many things that can be done at the website production stage to prevent- or at least reduce â€“ the risks.

â€¢ Your IT team can use a non-standard data model in with a regular CMS module â€“ This can be a fairly expensive solution and will need a talented developer to execute. The cost, however, may be prohibitive.

â€¢ Upgrade to the latest version of your platform. This may also be a costly affair depending on how much customization has been done to your website. Most platform providers will release security updates frequently because they are familiar with the common threats against their platform

â€¢ Use secure passwords and change them frequently. Use combinations of upper case, lower case, numbers and special characters, and make your passwords at least 8-10 characters long. NOTE: numbers-only passwords are the easiest to hack

â€¢ Try not to send out passwords by email, send user names and use SMS / texting to send the passwords

â€¢ Invest in a dedicated server

o Shared servers are very risky, mostly because you donâ€™t know who your neighbors are and you are sharing everything with them. Potentially you could be on the same file system as a highly infected site and the virus will spread very easily to your site. In such cases your IT Team cleaning up the virus is completely wasting their time as they canâ€™t clean the rest of the server, and itâ€™s only a matte of time before the infection comes back

o On Dedicated servers your IT Team will have access to the root file system and base modules so they can install a lot of tools & scripts to â€œhardenâ€• the server and secure it. This is not possible on shared servers

o Dedicated servers are more expensive to own & maintain

o Highly recommended: PaaS (Platform as a Service) hosting is the next generation of web hosting, which is highly secure

o You can consider the use of Reverse proxies & other advanced security tools, a few of these are now available on a service basis (SaaS)

Conclusion

We recommend Dedicated Servers to our customers along with a proper security and support package to help prevent such problems. It is very difficult for any IT team to guarantee that hacking wonâ€™t happen, but we can certainly warn of contributing factors such as shared servers / weak passwords / outdated software, etc. and make recommendations for the best ways to prevent hacking from happening. http://clicktecs.com/

Article Source:
http://www.articleside.com/ppc-advertising-articles/website-attacks-and-hacks.htm - Article Side

Jamshaid Hashmi - About Author:
ClickTecs is a specialized Digital Marketing Agency, headquartered in Toronto, Canada. We have made it our mission to help businesses navigate the shift from offline marketing to digital marketing by combining marketing creativity with technical expertise.

Article Keywords:
best search engine optimization, search engine company, search engine marketing company, search engine marketing optimization, internet marketing, best web design, best web design company, ppc marketing, online advertising, local search marketing, social