Barbarians at the Gate

Protect your WordPress Site from Hackers

A year ago Envision began installing security software directly on our clients' websites. The purpose was to monitor hacking attempts, malicious software infections and notices of WordPress software updates.

We were astonished by the number of invasion attempts -- having seen as many as 50-60 a day on just one site. Since 99% of attempts fail, you are likely unaware of the hoards of hackers trying to pound their way into your site. This security software certainly opened our eyes.

Types of Hacking

People typically think of hacking as objectionable changes being made to the pictures or content of their site. However in our experience most hacking goes unnoticed by the viewer. Malicious code frequently runs in the background with no obvious symptoms while assisting with other hacks, downloading infections and so on… the list is endless. Whatever it is, be assured you don't want it and that at some point it is going to cause trouble.

How They Get In

Hackers typically access your site:

- Through your server
- Through your code
- By brute force

How to Protect Yourself

Server:

There is little you can do if hosting your website on a shared hosting plan aside from choosing a reputable host. Hosts monitor their servers and are vigilant about thwarting malicious software but hackers sometimes beat them. If you are on a VPS (Virtual Private Server) and get a notice from your host, read it and do what they ask. If you don't know what they are talking about call them. If you don't know how to do what they want – pay them. It is usually a vulnerability patch and by ignoring it you leave yourself wide open.

Website Code:

The key to protecting yourself from a code infection is to keep all WordPress software up to date. Ensure that you are running the latest version of WordPress and update it as soon as new versions come online. Likewise, update your themes and plugins as soon as new versions are available. Updates frequently provide additional security and may be a response to vulnerabilities. Lastly, be sure to **delete ALL plugins you are not using**. One of the easiest ways for hackers to infiltrate sites is through old, unused plugins. People wrongly assume that if a plugin is on their site but not installed it is inactive. Not so.

Brute Force:
Brute force attacks are simply repeated attempts by a hacker to break in by guessing your user name and password. Hacking is less often a single person typing away on his keyboard. More frequently it is an automated attack run through multiple IP addresses across several days. Worse, these automated efforts can often pull information off the site that provide clues to usernames and passwords.

Don't use usernames like admin, your site name, your name (especially if you are the blog author) or other obvious words that may be easy to remember but also easy to guess. Use a username that is at least ten characters long, has no relation to your website and includes capital letters, numbers, and "symbols" such as $#@&. Your password should use completely randomized characters and look something like this: Z5#dfr$FBlk34. It's not a bad idea to change these every few months.

You can block IP addresses or block your site from being viewed in other countries since a great deal of hacking emanates from outside the US, in particular Eastern Europe.

Backups
When dealing with a site that has been corrupted we can often isolate and remove the malicious code then close any security gaps. In cases of a serious attack it is easier and less expensive to simply delete the old site and upload a new one. If you have a current and complete backup this is a straightforward process.

Your host can typically provide a backup but if their server has crashed or been corrupted you may be out of luck. If it took a while to realize your site was hacked all the backups may be corrupted as well. (Most hosts only keep backups spanning the past several weeks so in this case you would only have backups of the corrupted site.) Even if they do have a clean copy of your site it typically takes 24 hours to provide the backup and there is sometimes a fee. It is much more prudent to have a full backup at hand on your computer or in the cloud.

How to Make Backups:
We install a program called "Updraft" on our sites that greatly simplifies the process by making automatic backups – daily or weekly depending on the client. These are placed on your host server but you want to keep copies on your own computer and ideally also in the cloud for triple redundancy. It is best practice to have a clean and recent copy of your site readily available should you need to delete an infected site and do a clean install.

Summary
There is no way to guarantee that your site will not fall victim to a hacker. However the steps outlined above will significantly reduce the odds. Should you get a severe infection, frequent backups (the full site including database and themes) give you a valuable safety net. The adage about an ounce of prevention being worth a pound of cure is spot-on when it comes to protecting your website.