Seven Ways to Protect Your Website From Hackers

Those of us who are hackers would be offended by the article's title. Hackers are ethical testers to find faults in systems so they can be corrected before unethical hackers (crackers) exploit them. So, this articles is really about how to protect your website from crackers.

Keep your files up to date.

If your site uses the popular SendMail script, please be sure your version is a current one. Visit Anti-Spam Provisions in Sendmail 8.8 to edit the FormMail script. We have the updated SendMail in use for the Harley Shopping Cart site. FormMail is another popular script used to send form results to an email address or database. We use that file for our website form. These scripts are located in the cgi-bin on the web host server.

Signing up for updates for scripts (programs) your site uses will let you know if there are any. You should use the latest update to protect yourself. This is often the reason the update is released. If you are unsure of the scripts used on your website, contact your web developer.

Remove unnecessary files.
your website changes, old files are ignored. They should be removed. Keep copies offline in case you wish to add them again, but remember to update any scripts. Old files are often indexed by search engines. So even if you do not link to those pages anymore, the search engines lists them for Internet users to find and visit.
Automated programs to search for these files can find them to exploit them.

Implement passwords.
Any sensitive files, databases or scripts should be protected. Please use passwords that are difficult to guess. Use letters AND numbers, but be careful to keep the number of characters within the programmed limits and remember that passwords are case-sensitive.

Include robots.txt
Create a file to tell search engines not to index files that are restricted to certain users. You can also disallow indexing of images, so people who search for images to use illegal do not steal your images.

Check permissions of uploaded files .
Left-click each filename in your web host server, then right-click and select CHMOD to make sure files are set to the proper permissions. Check with your web host if you are unsure. Remember to upload images as binary and most other files as ASCII files. Choosing Auto for automatic selection may be incorrect if certain extensions are not specified.

Protect email addresses .
If you ever got a strange email that tested your form or simply sent you an email to yourself, one of those spammer programs found your email address from your website or someone else's. There are scripts to split up your email address, so spammer software programs cannot read them. Another way is to place your email address in an image or simply have an "Email us" link. I haven't done this, but I didn't have any problems until recently. I still want to make my contact information visible to my target audience.

If you sign guestbooks, go to forums or newsgroups, or share your email address with anyone else, your email address can be posted and shared all over the Internet. I often use several email

addresses when making posts, because spammers look there first for email addresses. To spammers, a guestbook is an email address database. So use a Hotmail account for your email, but you can still include your web address in your signature. If the Internet user visits your site, the user can contact you using the link on your site. The spammers probably won't visit your site, so the spam goes to the posted email address.

Protect your source code .
Some people use that stupid right-click script to protect their source code. Not only does that not protect your code, you are disabling browser functions such as adding your site to their favorites or printing. Though many people have "borrowed" my source code, I would not want to disable functions that my target audience wants to use. There are scripts to make your source code hidden. This is more effective, but a pain for anyone who wants to edit your site. The preferred method is external files such as external style sheets or javascript files.

Include copyright information on the page and in the meta tags for every web page.
Watermark all images. Keep copies of previous versions of your site with the last modified information intact. Save files on disks, so they can be retrieved. if necessary. Visit the WayBack Machineo find previous versions of websites, if you cannot find your files. Though the information is incomplete, it is better than nothing. Buy the copyrights to important files to protect yourself from competitors or other parties.