(Video) Why is Your website a target of hackers

Posted on April 13, 2015 by RWSmith

Why your website is a target of hackers. And we're being very loose with the term hacker, because there are a number of different variations of people out there in the digital world who are deemed as "hackers."

We've got three types really.

- The main one and probably the most common one is the script kiddy. Now the script kiddy is the wannabe. The 14-year-old teenager who sits in the back room on a computer and thinks he's a hacker. They download an application from the internet from a very unsavory site. They install it on their computer, which then makes them part of a bigger system to attack other people. And then they quite happily go off and target people on the internet.
- The second is the hacktivist. Now hacktivists are people who can be the teenager, but they are also interested in pushing their own particular wheelbarrow. They are only interested in defacing websites or compromising people or finding out information about people. They are in a situation where they don't want to break anything. Some of they do. But they are more interested in raising awareness about what they are interested in.
- The third one is the true full-blown hacker. Now these are the guys, and there are probably .001% of the people who consider themselves hackers who are actually in it for the money. They are in it to disrupt and compromise things as much as possible.

So what are these people all after? It doesn't really matter what they are from a script kiddy to a hacker to a hacktivist.

Why do we have websites?

Well, in most people's eyes, and this is thinking from the last 5 years, a website is somewhere someone can come to your little piece of your digital world and get information about who you are, what you are, what you do, what you have to sell.

The second part of a website is a blogging website, where the content is changing all the time. You are putting videos up, you're doing blogs. You're getting your message out to the real world and getting other people to associate with you, join your tribe, get people interested in what you're doing.

And the last part of having a website is as an e-commerce platform, so you can sell stuff. You can get people interested in your product through the blogging. They come to your website, and they will then purchase something.

We know what the cost of a website is. The cost of a website is only part of the equation. We are looking at protecting not only the www component of your website, but if you've got a hosting platform where you're using C-panel, then you have to make sure that doesn't get compromised either.

You're trying to make sure that logging onto that digital location is really secure.

So what are the bad guys, the hackers after?

Well primarily and only one of the large number of components, they're after money. They're after your money, they're after other people's money, and they're access to money. So credit card details is one of their biggest targets. So if you've got an e-commerce site that takes credit card details, you have to make sure that they're not collected in a way that they can be used by other people.

They are also after intellectual property / trade secrets. There was a company in 2010 who made metal detectors, and they used them to detect metal. One of their salesmen went to China, logged onto a free Wi-Fi, and had his laptop compromised, and they stole the blueprints to the metal detector.

The people who stole the blueprints, sold it to another company. They started building replicated metal detectors, and from there they then undercut the original price. The funny thing was that the original makers of the detectors didn't realize they'd been compromised until some of the replicas created by other manufacturers started coming in as warranty issues.

But more importantly, the hackers are after your visitors. You've done all the hard work, you have used your SEO or payperclick money to attract people and they are quite happily coming to your site regularly. If your website is infected then they can compromise all those people.

So how do they get access to your website?

Well in the first case, they do a scan of the digital world. Remember those script kiddies, they are going to find out you've got a connection to it, whether it's on your website, your office or your office 365, but they are going to find out what your connection is.

All that information then becomes critical to what they do next. How about a little social engineering? They then associate your website with your Facebook, Twitter, LinkedIn accounts, any of your social media platforms that you're using. Now they can see exactly what you're doing, who your people are and what your products are.

So you're actually doing some of the hard work that the hackers need done by having all of that information out there.

I'm not saying you can't have it out there. I'm saying you have to be very careful about what you put out there.

And then from that, they see if they can compromise your website.

Now compromising your website is the hard part of the whole process. The above process are all easy, they're all done automatically. The next step is to come up with a plan of attack. That usually involves cross-site scripting or malware.

How are we going to go about protecting ourselves from these people who are targeting our websites? Well, one of the big things you can do and one of the main things you can do is you have complicated user names and passwords. And they are not only complicated but they are unique. They have to be 9 characters long. They have to have alphanumerical symbols. Everything that you can think of.

When you install a website through some of the hosting platforms, like the WordPress system, the first thing it does when you press the button that says install, it says it needs a username for the admin account. Your admin account is literally the keys to your kingdom. And a lot of people just go admin, password blank. So what you've done on the internet is give all of those hackers access to your site without you even doing anything in particular.

The script kiddies don't have to do anything because they first thing they're going to do with their automated systems is try admin blank, or admin password, admin 12345.

So instead of using admin, you use _29_admin41.

Yes, you have to remember that's the name of it. But, and then you use a complicated password, a really complicated password, 9 characters long, to make sure that people cannot get in there.

The next thing you have to do for your website, and one of the most important things is you have to make sure that all of the small applications on the website are up to date. If they plug into j-script, or they have a Java component, they need to be updated and patched to make sure that a) they've got the most secure version and b) they've got the newest version.

You know that your passwords are in place, and all your systems including the actual underlining system like C-Panel itself, or WordPress are all updated.

Getting down to the nitty gritty of the website, most people have comments automatically enabled. If you want comments coming through, or if you flip the comments through to your social media, but if you want comments on your blog site, then you have to make sure that people who are coming to your site to put on the comments are leaving their username, creating a username, creating a password, and leaving an email address that you can then verify.

The fourth component of what you need to do is if you are logging on to your system, you have to make sure that you're logging on through a secure connection. Used to be SSL. It's now TSL. SSL is a method of encryption, which is not as secure as TSL, but it still works.

The fifth thing you need to do is no matter what happens, you need to back it up. You never know when your hosting platform is going to have a fire and burn to the ground. What are you going to do if that happens? Are you in a situation where you can build your website straight up and down on another platform?

Or if you don't like the platform you're on, and you want to move it to another place. You have to have a backup of it. Otherwise there's a lot of work involved.

One thing that people don't do is they don't visit their site regularly. And I'm talking 1-2x a week, 1-2x a day, but no less than 1x a fortnight. Because you never know when these have to be applied. You never know whether someone's left a comment, unless it's emailing you as well. But if you're visiting it regularly, and you can see what is happening, then you know that the look and feel of the website that you've produced is going to stay the same. And it's very important you see it as regular as possible.

Getting down to the security component of what we're talking about, most websites do not have a way of informing you that people have logged on or that something has happened or there's no regular scan of

PHP or of SQL. Now this is a module that goes onto WordPress. I'll talk about WordPress here, but they have got modules that work with HTML and a number of the others CMS systems.

This module is very important. For one, it tells you when people log on, from where they're logging on and if people have failed to log on. So if these people are trying admin, you're going to get a message, or a consolidated message every day about these people who have been trying to access your site.

But Securi has two more things. They have a one-click secure system. So you install this plug-in on your website, and when you hit the secure one-click, it locks all of the PHP down, it changes some of the permissions to a level where things are still going to work, but they're a lot more secure.

And if you really want to be secure, and you start to look at other components like e-commerce and gateways, then you need to start looking at a proxy gateway. Now a proxy gateway will cost $20-$40-$60 a month. If you've got a regular website that is getting accessed every 2-3 hours, 10-20-30x a day, as a small business, you need to start thinking about what these people are doing and how they're getting to your website.

A proxy gateway creates your www request coming into the gateway and then getting physical forwarded to your hosting site. Now, what that does is it makes this part of your website very secure. Because they've got to come through this gateway before they can get to your site.

This site if it gets compromised, not a big deal, because there's no information on that site or that area of the gateway. But is it going to allow the system to be compromised?

So instead of affecting this, trying to affect that, nothing happens. So they're always in the situation where this information is going backwards and forward, and that is under SSL or TSL. So it's all secure. And you then know that your site is going to be relatively secure. And that makes it a lot better for your website itself and for your own peace of mind.

So as I said, they are out there. The cyber criminals are targeting you not because you have something they want, but because you are connected to the internet, and that is really important. It's a big message to get across. The fact that although you may think you don't have anything worth stealing, or you're too small to be a target, or it'll never happen to us, with the script keys and the hacktivists and the real life hackers targeting your website just because you are on the internet makes you a target.

So you have to make sure that although you are a target, you try to take yourself away by putting in a few initial systems that will protect you.

Now if you go to our website at the bottom of this page, there is a security website checklist. Just download it, leave your first name and your email address, and you can see – and this will give you an idea of where your website is and what you need to do to protect it.