Too Small to Hack? Think Again.

By Karen Nardozza

There are plenty of nefarious characters out on the fringes of our digital world. But it's safe to assume smaller brand websites fly under their radars. Right?

Sadly, wrong. As you read this article, there's a good likelihood an attempt is being made to hack your website.

Small websites are a surprisingly tempting target for hackers for many reasons. A successful hack could provide information, exposure or simply bragging rights. Quite frankly, though, it's about the money—and there is a lot to be grabbed. Here are just a few examples we've been contacted to help fix:

A company's website had some malware installed that created jihadist messaging. A visitor couldn't navigate away from the site short of shutting down their browser.

A new page was created on a website that mimicked a national bank's login page, seeking user names and passwords.

Malware was installed, and the company's Google listings turned into spam advertisements for Viagra. Visitors could clearly see the site had been hacked and didn't want to click on a Viagra ad.

These weren't mega-sites. They had fewer than 20 pages and 200 visitors per month.

Recovering from a hacked website can take days to resolve and return the website to its normal state. The time and cost are scary—doubly so when you consider these hacks could create an indelibly negative impression that tarnishes your brand image and company reputation. It's not uncommon with small businesses that their customers are the first ones to report a hack.

WHO GETS TARGETED?

We've seen in the news how large and even giant websites—from multinational companies to movie studios to municipalities—get hacked. But far more common are the hundreds of thousands of small websites attacked every day.

In general, smaller sites are easier to hack. They're often hosted on shared servers—which lowers cost but also increases risk. If a hacker figures a way into one website on a shared server, it's much easier for them to infect other websites on that same server.

According to the leading web technology survey firm W3Techs, approximately 32 percent of all websites are built with WordPress. This popular content management system, or CMS, is open source. That means the codebase, which refers to the human-written programming code for a specific program or application, is available for anyone to review. Hackers find this extremely enticing. It's very easy for a hacker to exploit a security vulnerability found in WordPress, especially if they found the vulnerability and did not report it to the WordPress development community.

Google and likely your hosting company take an interest in whether or not your website has been hacked. Both could blacklist your website from displaying to visitors until the suspected issue is resolved. Google could remove your website from their Search Engine Results Page which would be bad for the reputation and bottom line of any company or brand.

HOW HACKS HAPPEN

"Access" is key when talking about hacking a website. How does a hacker get access? There are several ways, but the most common are through your hosting account, your server or your content management system. Once the hacker gains access, they will usually follow one of three methods to insert their malware into your website:

SQL Injection—If a hacker finds an

improperly programed form on your website, they can attack it by quietly submitting malicious scripts into the website database. Scripts are used when visitors engage with a site and add information to a page such as entering information for an online order. Hackers are usually looking for data: usernames, passwords and credit card numbers.

Brute Force—Brute force website hacking is using any method to figure out your password. This is often done with an automated script or "bot"; a program that tries different character combinations until they get it right. Brute force methods can cause significant server performance problems such as slow-loading pages or pages that fail to load at all.

Cross-Site Scripting—XSS for short, is a malicious script that can create redirects, sending people somewhere else when they intend to visit your site. These scripts could also cause you to download malware onto your site.

WHAT CAN YOU DO?

Pick Perplexing Passwords. It's mind-boggling that the most common usernames for a website's administrator are still "Admin" or "Admin1." And readily-available lists reveal there are some surprisingly common—and surprisingly easy to guess—passwords still used by many users. Do "123456" or "password" ring any bells?

Secure, Encrypt, Backup. If your server is not behind a firewall, it's time to make that happen. Host your website with a highly-rated, reputable company. If you send or receive data from your website (we're talking to those of you that have forms on your websites), make sure your form is programed with security in mind and the form data is encrypted using Hypertext Transfer Protocol Secure (or HTTPS), which supports more secure online communication. You should also be backing up your website data regularly. Having a recent backup means you can restore your website quickly in the event your website gets hacked.

Stay (Mostly) Up-to-Date. It can be worrisome to think the bad guys are out there trying to attack your website daily.

But the good news is: the good guys are working to stop them just as tirelessly. Make sure your site, CMS, software add-ons and everything else are up-to-date with the best versions for your site's needs—which isn't always the most recent version. A web development and security professional can advise you when to stay fully up-to-date and when to wait and update later.

If all of the above sounds like a foreign language to you, that's OK. It just means you probably should work with a professional web development agency that has expertise in website security in addition to website design and programming. Be careful out there! **CG**