PACIFIC COAST BUSINESS TIMES
Proudly serving San Luis Obispo, Santa Barbara and Ventura counties

Hack attack: How to keep your small-business site secure, on a budget

By Stephen Nellis on August 23, 2013.
Visit the live article at Pacific Coast Business Times

Michael Kramer, founder of Santa Barbara-based Ameravant Web Design. Web developers say a proprietary content management system, such as Ameravant's SiteNinja, can be a more secure option than an open-source option like WordPress. (Stephen Nellis photo)

It's a small-business owner's worst Web nightmare: A customer or business partner calls up and says your website seems to now be an ad for Viagra pills from China or just infected them with malware. You've been hacked.

In recent weeks, a wave of hacks have hit small business around the Tri-Counties. The Business Times reached out to Web developers around the region for advice on how small-businesses can keep their websites more secure. Experts say that even without a huge budget or a full-time webmaster, small firms can take a few easy steps to protect themselves from some of the most common hacks and recover quickly if an attack does happen.

One of the first things to understand is that even the simplest of websites are far more complicated than the days of HTML files pecked out on a keyboard. Most websites today employ what's called a content management system and a database. The database stores all of website's content and information, and the content management system is software that runs on the Web server to display the front end of the

site to users and let the site's owners create and manage content on the back end.

The rise of freely available content management systems such as WordPress, Joomla and Drupal has revolutionized Web development. Since they're free, some small-business owners try their hand at creating a site on their own, and others tap the vast number of developers who use the systems as a basis and take advantage of the millions of plug-in tools published for them.
Experts think that as many as half to three quarters of the sites on the Internet are running WordPress. That in itself is a problem: Hackers always target the most broadly used systems to get the best bang for their evil buck.

"One of the big dangers out there is using a pre-built CMS platform. They can be dangerous in that they have a lot of insecure plug-ins that were written by people that aren't security minded," said Forrest Hatfield, co-founder of ITECH Solutions in San Luis Obispo. "You have to be very careful about what you install."

ITECH uses an in-house built content management system to avoid a lot of those problems. While a system like that requires years of coding experience to build, one thing small-business owners can do on their own is use good password management by using a free tool like LastPass, which securely stores a range of different passwords rather than using the same password for email, websites and other services.

"One thing that's quite overlooked is that people tend to use the same password on different services," Hatfield said. "If any one of those services gets compromised, it's possible a hacker can get into other systems."

It can be hard to detect if you've been hacked. Often, your hosting provider — the service that actually provides the space and bandwidth for your site — will alert you to suspicious activity. Hatfield also recommends using Google's ability to search within your site — go to Google and enter "www.mysite.com" and a colon — to search for potentially malicious keywords like "Cialis" or "payday loans."

Hatfield also said that paying a little extra for a Web host that gives you a private server and backs up websites regularly can make the difference between getting constantly hacked and being down for days at a time or being back up within an hour. "If you pay a little extra, that web host should be doing weekly or monthly backups of your site and able to restore you easily," he said. "I always caution people that you get what you pay for."

Another option to go for what's known as a hosted service. Santa Barbara-based Ameravant Web Design not only uses its own house-built content management system, it also taps Amazon's cloud servers to host its clients sites and to run its software.

"When we want to deploy a new feature to all of our clients, we update it one time and literally hundreds of clients get it," said founder Michael Kramer. "Everything is in the security of Amazon's servers, and we

only have to worry about one environment. If there's any sort of error that occurs and it's not performing as it should, we get an instant text message notification."
In modern Web pages, the site itself is constantly pinging the database for content. One of the most common attacks is for a hacker to step in the middle of that that process and inject malicious code into the database. Kramer said his firm's software puts a middle layer between those functions, which stops most injection attacks.

Despite issues with WordPress, there are millions of sites that use it successfully — it just takes some good security practices, said Matthew Shuey, owner of GlobalWebFX in Ventura. A key measure is keeping WordPress up to date. Change the default accounts from "admin" user names. Hackers hit these common user names with brute force attacks that try millions of passwords until they guess correctly. And take advantage of security plugins that do things like lock out users after a certain number of failed login attempts.

"Installing security software on a fresh install is always the best thing to do — and keep those plugins up to date," Shuey said.

And budgeting even a few dollars a month to have a professional developer take a look at your site can save you a lot of money restoring your site in the long run. Many of today's hacks are designed to stay hidden for months, secretly using your web traffic to help give a boost to unscrupulous operators.
"Even though they don't show up, you always have to do a manual investigation to make sure you're website is completely clean," Shuey said.

By Stephen Nellis on August 23, 2013.
Visit the live article at Pacific Coast Business Times