More Than 150,000 U.S. Small-Business Websites Could Be Infected With Malware at Any Given Moment. Here's How to Protect Yours.

Small-business victims were involved in 43 percent of data breaches over the course of a year, according to a recent report.

Hayden Field

Entrepreneur Staff, Associate Editor, June 12, 2019 9 min read

It was March 2, 2016, and Melissa Marchand's day on Cape Cod started out like any other. She drove to her job at Hyannis Whale Watcher Cruises in her mid-size sedan, picked up a latte with 1 percent milk at her local coffee shop and sat down at her desk to check her email. Then, Marchand got the call no website manager ever wants to receive: The site was down, and no one knew how to fix it.

After she dialed up the web hosting provider, the news went from bad to worse: Whales.net had been hacked and, to her horror, all visitors were being redirected to porn sites. Google had even flagged the company's search results, warning potential customers that the site may be hacked.

"It was a total nightmare -- I had no idea that something like this could happen," Marchand said in an interview with *Entrepreneur*. "I'd say 75 to 80 percent of our bookings are done online, so when our site is down, we're just dead in the water."

At the provider's suggestion, Marchand called SiteLock, a website security company, and granted its representatives site access. SiteLock discovered the hackers had exploited a security hole in a Wordpress plugin, which gave them the access they needed to redirect visitors to racy websites.

By the end of the work day, Marchand sat in her car in her gym's parking lot, speaking on the phone with a SiteLock representative to review the plan of action. She finally felt like things were going to be OK.

Within three days, Whales.net was back up and running, though it took another three weeks for Google to remove the blacklist warning from the company's search results.

The hack hit about a month before the whale-watching season began in mid-April, and though it wasn't peak season, the company still missed out on pre-booking tour groups from schools and

camps. Marchand estimated the attack lost the company about 10 percent of its March and April business.

A risk for small businesses everywhere

Small-business owners were victims in 43 percent of data breaches tracked between Nov. 1, 2017, and Oct. 31, 2018, according to a 2019 Verizon report. The report tracked security incidents across all industries, but the most vulnerable sectors this year were retail, accommodation and healthcare.

What does the issue look like on a national scale? If we take the sample size of infected sites SiteLock said they found in 2018 -- approximately 47,244 out of 6,056,969 checked -- and apply that percentage to the country's estimated 30.2 million small-businesses websites, minus the estimated 36 percent that don't have one, then we can loosely estimate the amount of infected small-business websites to be around 150,757.

As a small-business owner, you may not believe anyone would target your website, but that's just it -- bad actors are likely not seeking out your site specifically, said Mark Risher, head of account security at Google.

"Sometimes, we talk about the distinction between targets of choice and targets of chance," Risher said. "Targets of chance is when the attacker is just trying anything -- they're walking through the parking lot seeing if any of the car doors unlocked. Target of choice is when they've zeroed in on that one shiny, flashy car, and that's the one they want to break into -- and they'll try the windows, the doors … the moon roof. I think for small businesses, there's this temptation to assume, 'No one would ever choose me; therefore I'll just kind of skate by anonymously.' But the problem is they're not factoring in the degree of automation that attackers are using."

Even the least-trafficked websites still average 62 attacks per day, according to SiteLock research. "These cybercriminals are really running businesses now," said Neill Feather, president of the company. "With the increasing ease of automation of attacks, it's just as lucrative to compromise a 1,000 small websites as it is to invest your time and try to compromise one large one."

John Loveland, a cybersecurity head at Verizon and one of the data breach report's authors, said that since the report was first published 12 years ago, he's seen a definite uptick in attacks at small and medium-sized businesses. As malware, phishing and other attacks have become "more commoditized and more readily accessible to lesser-skilled hackers," he said, "you see the aperture open … for types of targets that could be valuable."

So what are the hackers getting out of the deal? It's not just about potentially lucrative customer information and transaction histories. There's also the opportunity to weaponize your website's reputation. By hosting malware on a formerly trustworthy website, a hacker can increase an attack's spread -- and amplify the consequences -- by boosting the malware's search engine optimization (SEO). They can infect site visitors who search for the site organically or who access it via links from newsletters, articles or other businesses, Risher said.

Even if you outsource aspects of your business -- say, time and expense reporting, human resources, customer data storage or financial transactions -- there's still no guarantee that that information is safe when your own website is compromised. Loveland said he saw an uptick in email phishing specifically designed to capture user credentials for web-based email accounts, online CRM tools and other platforms -- and reports of credential compromise have increased 280 percent since 2016, according to an annual survey from software company Proofpoint.

How to protect yourself and your customers

How can small-business owners protect themselves -- and their customers? Since a great deal of cyberattacks can be attributed to automation, putting basic protections in place against phishing, malware and more can help your site stay off the path of least resistance.

Here are five ways to boost your small-business's cybersecurity.

1. Use a password manager.

There's an exhaustive amount of password advice floating around in the ether, but the most important is this, Risher said: Don't reuse the same password on multiple sites. It's a difficult rule to stick to for convenience's sake -- especially since 86 percent of internet users report keeping track of their passwords via memorization -- but cybersecurity experts recommend password managers as efficient and secure workarounds. Free password manager options include LastPass, Myki and LogMeOnce.

2. Set up email account recovery methods to protect against phishing attacks.

Phishing attacks are an enduring cybersecurity problem for large and small businesses alike: 83 percent of respondents to Proofpoint's annual phishing survey reported experiencing phishing attacks in 2018, an increase from 76 percent the year before. Embracing a more cyber-aware culture -- including staying vigilant about identifying potential phishing attacks, suspicious links and bogus senders -- is key to email safety.

If you're a Gmail user, recent company research suggests that adding a recovery phone number to your account could block up to 100 percent of cyberattacks from automated bots, 99 percent of bulk phishing attacks and 66 percent of targeted attacks. It's helpful because in the event of an unknown or suspicious sign-in, your phone will receive either an SMS code or an on-device prompt for verification. Without a recovery phone number, Google will rely on weaker challenges such as recalling last sign-in location -- and while that still stops most automated attacks, effectiveness against phishing drops to 10 percent.

3. Back up your data to protect against ransomware.

Ransomware -- a cyberattack in which a hacker holds your computer access and/or data for ransom -- has kicked off a "frenzy of cybercrime-related activities focused on small and medium businesses," Loveland said. In fact, it's the second leading malware action variety in 2019, according to the Verizon report, and accounted for 24 percent of security incidents. Hackers generally view it as a potentially low-risk, high-reward option, so it's important to have protections in place for such an attack -- namely, have your data backed up in its entirety so that you aren't at the hacker's mercy. Tools such as Google Drive and Dropbox can help, as well as automatic backup programs such as Code42 (all charge a monthly fee). You can also purchase a high-storage external hard drive to back everything up yourself.

4. Enlist a dedicated DNS security tool to block suspicious sites.

Since computers can only communicate using numbers, the Domain Name System (DNS) is part of the internet's foundation in that it acts as a "translator" between a domain name you enter and a resulting IP address. DNS wasn't originally designed with top-level security in mind, so using a

DNSSEC (DNS Security Extension) can help protect against suspicious websites and redirects resulting from malware, phishing attacks and more. The tools verify the validity of a site multiple times during your domain lookup process. And though internet service providers generally provide some level of DNS security, experts say using a dedicated DNSSEC tool is more effective -- and free options include OpenDNS and Quad9 DNS. “[It’s] a low-cost, no-brainer move that can prevent folks from going to bad IP addresses,” Loveland said.

5. Consider signing up with a website security company.

Paying a monthly subscription to a website security company may not be ideal, but it could end up paying for itself in terms of lost business due to a site hack. Decreasing attack vulnerability means installing security patches and updates for all of your online tools as promptly as possible, which can be tough for a small-business owner’s schedule.

“It’s tempting for a small-business owner to say, ‘I’m pretty handy -- I can do this myself,’” Risher said. “But the reality is that even if you’re very technical, you might not be working around the clock, and … you’re taking on 24/7 maintenance and monitoring. It’s certainly money well spent to have a large organization doing this for you.”