Protect your business against cybercrime

Ron McCabe

Ron McCabe, president at Everbearing Services in Portland, Oregon, has been a technologist for over 35 years and an expert digital marketer for 13 years. Visit his website and subscribe to his newsletter at www.everbearingservices.com, or reach him at rmccabe@everbearingservices.com.

OVER THE LAST FEW years, the green industry has rapidly pivoted to online sales and customer service. Growers and retailers were increasingly forced to interact with clients without face-to-face contact as they switched to online ordering and delivery, curbside pick-up, and virtual or socially-distanced landscaping services.

From wholesale growers to garden centers and landscape technicians to designers, every business had to shift quickly.

Unfortunately, some moved so fast that they overlooked or deemphasized the importance of protecting their online presence.

Web-based cybercrime is a lucrative and growing business. Cyberattacks to disrupt the American economy are now commonplace, often launched by foreign actors sitting comfortably behind a keyboard far, far away. The main goal of cybercrime is usually to disrupt business activity. These attacks can cost opportunity, revenue, clients, and prospects.

Cybercrime does not discriminate; any business can be targeted. According to the Hiscox Cyber Readiness Report, nearly one-quarter of U.S. small businesses fell victim to cyberattacks during the previous year, costing an average of $25,000 each. What's more, the smallest businesses often sustained the most significant losses relative to company size.

Website security breaches accounted for 30% of cyberattacks and were more likely to cause the website to fail. There are often hundreds of intrusions or hacking attempts every day on a website. Unfortunately, as these attacks are not visible if they are not being monitored, decision makers can often have a false sense of security.

Most cyber criminals or hackers are attempting to load malware, a malicious type of software. Malware performs various tasks in the background to capture critical information from a website, such as contact information for clients or prospects.A common example of malware is a keystroke logger. It is used on unsecured websites where hackers can upload their malicious software. Once the software is installed onto the server, it automatically proceeds to try and download malware onto visiting systems.

From there, it will try to gather credit card numbers, passwords, Social Security numbers and other sensitive information. This confidential information is then regularly transferred back to the attacker.

Keeping them out

Many agricultural businesses disregard this risk, citing the size of their operation. The reality is that virtually all cyberattacks are automated, and these attackers know that smaller, unmaintained websites are the best targets. These scripted attacks do not discriminate. They attack everyone, looking for any opening to get in.

To install malware, cybercriminals look for holes in website security. Out-of-date security patches and software often create these openings on a website. Failing to update and secure the website content routinely makes the company more vulnerable to attacks. Performing updates and installing patches for any plug-ins or extensions will help thwart these attacks. So, make sure to perform regular security updates when they become available.

As there is a potential for more credit card or account information on an e-commerce site, small and large businesses are high-risk and often the most targeted. To stay up to date, schedule the following updates weekly or at least bimonthly:

Put up a wall and actively guard the site. For extra protection, businesses should also consider an active firewall — a digital wall against intruders — with malware scanning. This software protects websites from outsiders attempting to monitor online activity 24/7.

While this software is actively detecting intrusions, it performs malware scanning. This is like an antivirus scanning a computer, constantly searching the website to detect and eliminate malware. Many of these website firewalls have active security monitoring to alert administrators if an attempt or breach of information has been made.

An opportunity and a risk

Entering a website through the contact form is also a common tactic. If a company updates and monitors the website, this exploit usually does not provide access. In cases when a cyber attack is successful, these intrusion attempts most often break in through a contact form.

It is not usually noticeable when a contact form is broken. However, a simple way to make sure this has not happened is to manually check that the contact form is working correctly. Do this monthly. This helps facilitate a quick repair and ensures leads continue to come through.

Use a secure, knowledgeable host

We are long past the days that allowed companies to throw up a webserver and ignore it. Self-hosting a website is not recommended unless a business has a talented IT staff on-site to maintain hosting actively. Securing and protecting a website is a separate specialty and skill.

As a result, most companies elect to use a dedicated web hosting compa- »

ny. Unfortunately, like anything else, not all web hosting companies are the same. One of the areas where some of these companies cut costs is security.

An unsecured web host can cause vulnerability to intruders, who often try to break in through hosting like a burglar goes through the back door. They can break into an entire website, cause damage and corruption, or even shut it down. Hackers may also elect to load malware and leave it undetected.

Use a web host that stays on top of the most current cybersecurity practices and knows how to efficiently and effectively respond to an attack.

Look into insurance

Cyber insurance, which is also referred to as cyber liability insurance, protects companies against direct and indirect (third-party) liability. These policies deal with data breaches, malware, ransomware attacks, and online compromises of business accounts. As the extent and the sophistication of these attacks increase, more and more small businesses are affected.

The green industry is particularly susceptible as there is a general attitude in horticulture that we are either too small or too new to online and digital to have any real liability. The recent pivot to online plant sales and payment has also increased risk leves higher than previously assumed.

Purchasing cyber insurance is a relatively inexpensive way to protect against the unseen and unknown. In addition, this type of insurance is a good umbrella to cover loose ends on the overall website security practices.

The good news is that by following these practical, actionable steps, business owners can improve their website's cybersecurity and reduce the risk posed by cyberattacks.

As the well-known saying goes, "The best defense is a good offense." Taking these proactive steps to enhance your website security now will be a solid defense of your time, money, and brand. We all need to work together to protect our green gold as we innovate and shift digitally.

Editors Note: Ron's column on marketing and technology debuts in this issue and will appear periodically.

References

Hiscox Ltd. (2021, May). *Hiscox Cyber Readiness Report 2021 don't let cyber be a ...* Hiscox Cyber Readiness Report 2021. Retrieved March 1, 2022, from https://www.hiscoxgroup.com/sites/group/files/documents/2021-04/Hiscox/Cyber/Readiness/Report/2021.pdf