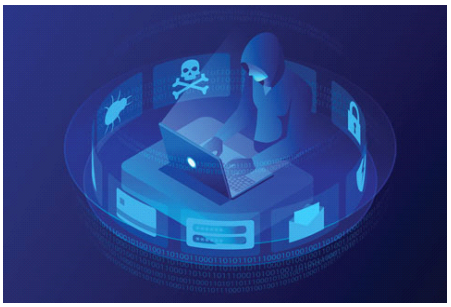
GROWERTALKS

Features

12/1/2018

Could You Get Hacked?

Jennifer Zurko



It's the news du jour: large companies' computers coming down with viruses, suspected foreign interference in our election process and on our social media platforms, retailers' credit card systems getting hacked. It's a scary proposition and even more of a possibility for businesses now than ever before. Many experts believe that the next Cold War will be fought over the Internet.

With more banking and purchasing transactions being conducted digitally, businesses have to ensure that they take all of the necessary steps to avoid having sensitive information stolen, like employee's Social Security numbers and/or their customer's credit card numbers.

Have you done enough to ensure that your software and hardware systems (and for you retailers, your POS systems) are protected? Here's a checklist of what you should be doing to avoid a cyber-attack:

• **Know the risks** by understanding the internal and external vulnerabilities of your business to a hacker. How could a hacker can gain entry to your system? Start by identifying points of weakness. The best way to do this is by getting informed about the various cyber fraud schemes and threats—phishing, malware and system hacking—that businesses face.

• **Use a commercial-grade firewall** from a firm like Sophos, SonicWall, Fortinet, Cyberroam or Cisco.

• **Forgo retail anti-virus software and choose a cloud-based, commercial-grade option** that updates every few minutes, requires almost no user input and provides reporting on potential threats to your network.

• **Back up your data online** with a program that uses "versioning," which allows you to see different versions of files. While you may prefer to do local backups, viruses, crypto viruses and malware often look for and encrypt local devices.

• **Keep your software up to date.** Almost all network hacks come from unpatched exploits. Devoting 30 minutes a week to software updates may be annoying, but it's cheaper than spending weeks rebuilding what you lost or closing up shop because it's now been locked down with a crypto virus.

• **Encrypt data.** From bank routing digits to employee social security numbers, today's hackers are on the hunt for standard company-held information that typically gets left lying around. For companies holding important data, be sure to take measures to always have this information encrypted. Keep your information safe by turning to full-disk

encryption tools that come standard with most operating systems.

Using this feature does require some added attention, though. This is because the encryption will only activate in scenarios a login is not in use. For hackers, this means that all they need is for an employee to take a brief break and head over to the office kitchen in order to attack a system with virus and malware. So, to enforce your measures, be sure to set your computers to automatically log out after five to 10 minutes without use.

• **Be sure that your hardware is secured.** Not all cyber-attacks come through a computer system; most cyber-attacks occur when physical electronic equipment is stolen. To make sure that no one walks away with loads of information stored on your office computers, make sure your systems are physically locked down. Kensington lock ports are a small securing feature present on most laptops and desktops. They feature a small loop that keeps a device tethered down to a desk. Of course, they're not entirely impossible for a thief to circumvent, but their presence will require more time and effort as they try to make an escape with your equipment. Cloud computing software also allows businesses to track down mobile laptops, devices and even desktops that are taken.

• **Embrace security as part of your company culture.** You can't be the only one taking measures to keep your company's and customers' information safe. Employees must be aware of the ways in which they themselves can put the company at risk. To keep them aware of possible cyber-attacks, make sure, in your role as leader, that your employees know to always keep their eyes peeled for potential threats and be aware of how to keep information safe. Hackers can worm their way to obtain private information through email servers, apps and pop-ups.

Start by having a formal company Internet policy specified for your business. Draw the line on what Internet practices are prohibited within the office and on devices. If you've yet to issue a rule about which types of emails are okay to open on your devices and what type of attachments are okay to retrieve, talk to an IT specialist and draw up a set of rules.

Keep the threat of cyber-attacks on your employees' minds by sending them brief emails about threats and having occasional meetings featuring information from an IT expert. The most effective way of preventing everyday hacks is to set a rule for employees that prevents them from accessing their personal email on your company's Wi-Fi system.

Sources: Forbes, Entrepreneur

Data Held for Ransom

One weekend in July 2017, a few people went into work at Takii's headquarters in Salinas, California, and realized that their Internet was down. They contacted their tech infrastructure consultant and found out that they'd been hacked, affecting their ordering and inventory systems. The kicker is that they'd just started work on migrating all of their systems to Microsoft Office 365, so when the ransomware hit, the only thing that had been moved to the new program was their email.

Holes in their firewall allowed the hacker to enter their system through a backdoor portal via an email sent to an employee, said Steve Wiley, Takii's GM and COO. When the email was opened, it encrypted Takii's system, bringing everything to a halt. And because they had a manual backup system that had to be activated by an actual person, their data hadn't been backed up in 10 days, putting them behind the eight ball to try and re-create 10 day's worth of lost information, which took almost three months to do.

"We had to just buckle down and go to a manual sales system and the trouble with manual sales is it makes it hard to send the invoices out," explained Steve. "We could ship seed, we could create packing lists, but

putting it onto our accounting system was difficult. So it did take us a little while to reconcile how to get manual invoices out."

There was a ransomware note asking for 10 Bitcoins, which at the time was worth about $30,000, said Steve. Takii decided that they wouldn't pay it, which they agreed would make them feel like they accepted that kind of dark web behavior.

So the team at Takii, along with their tech consultants, buckled down and got to work to re-construct the system. A better-quality firewall was purchased, which closed down any backdoor entrances, and they invested in a more robust malware detection service. They also went from a manual backup system to a cloud-based one.

"We went to a cloud-based backup system that was done every night, so that if this ever does happen [again], we would never lose more than 24 hour's worth of data," said Steve. "The lesson is make sure you automate your backups, so if your front line of protection breaks down, you need to have the backup systems to be able to not lose data."

Takii did report the ransomware attack to the FBI, but heard nothing back, which Steve found disappointing, but not surprising.

"Unfortunately, you can't count on the government to help you out with this," he said. "Not that it would have prevented it from happening, but maybe it would prevent it for other people, if the FBI were to pursue these leads. Maybe there are just so many out there that you have to be General Motors or Amazon, where people's Social Security numbers and millions and millions of dollars are affected, not just some small seed company. It just shows you that the government has bigger fish to fry."

Thankfully, most of their customers were flexible and understanding while Takii was trying to sort everything out—and sympathetic to the fact that it could also happen to them. It helped that all of their hard work to keep up with orders and not letting it affect shipments paid off.

"At the end of the day, it cost us time and it cost us the money it took to re-create the systems," said Steve. "I don't know that it cost us a lot with regard to orders, but we had to stop everything and do manual inventory. There was a lot of starting and stopping, but we managed to be able to make the big push of seed that happens in November, December and January without missing any orders. We were able to stay on top of our quality assessments. It was a lot of hard work internally to be able to stay up and at it without missing a beat."

If Steve were to give anyone advice on how to avoid a cyber-attack, it would be "don't rely on people to do your backups. The more automated you can have the system, the easier it is if somebody forgets to do the backup to go back in and check at a later date to make sure it's been done."

Size Doesn't Matter

The chances of being affected by a cyber-attack doesn't increase if you're a larger company; even small businesses can experience a malware issue or virus and it can cause just as much of a headache.

Jim Clesen, owner and VP of Ron Clesen's Ornamental Plants (RCOP) in Maple Park, Illinois, said that they've experienced some issues in the past and have hired an IT expert to make sure all of the safeguards are in place to avoid future problems.

One challenge they've had to tackle is the company's emails being pirated, said Jim, which flags them as being suspicious to other email servers or "blacklisted." So they've had to make changes to procedures, mail hosting and ISP (Internet Service Provider) configurations to ensure that emails being sent from RCOP are "whitelisted" and don't end up in recipients' junk mailboxes.

Other things RCOP has done to protect their and their customer's information:

• They've changed their email host provider (to Microsoft Office 365) and filter incoming emails through two anti-virus/malware programs—one for their server and one for their hardware.

• They try to stay vigilant, being aware of senders' email addresses, which may not match what they know is already in their system. "When in doubt, do not open," said Jim.

l• Jim says they limit their exposure on any computer's remote access, with usually only their IT guy able to gain access to fix any issues. RCOP's "environmental computers" that their growers access through their smartphones are standalone devices and not connected to their network, so there's less of a worry about those.

• On their website, photos are scanned for viruses when uploading off of the Internet or off a device, although they try to take most of their own photos in order to limit any possible issues (plus, they'd rather show more "real-world" images taken from their greenhouse). When they do upload images, their host provider provides another level of virus and malware protection. **GT**