greenPROFIT

Features

4/1/2021

Securing Your Computer Network

Joe Dysart

Always a pressing challenge, the security of your business' computer network is facing an even greater threat in 2021, given the stubborn persistence of the coronavirus, according to security pros.

Ever creative, hackers are riffing on coronavirus fears by sending employees official-looking emails pretending to feature new business policies on the pandemic, new announcements from government agencies or the latest updates on free government financial support during the epidemic. Unfortunately, all these hacker emails turn out to be malicious.

Pictured: Small businesses, with little or no cyber defenses, are now considered easy marks by hackers.

And they often result in the penetration of your business' computer network by hackers, the installation of malware on your computers—and worse. This is especially worrisome for green industry businesses, given that so many growers use environmental computer systems these days to control a vast array of growing functions—from irrigation to climate control, according to Lee Stiles, secretary of the Lea Valley Growers Association.

"If the environmental computer is breached and the vents are left open or the heat turned up even for a short period of time, the grower could potentially lose a one-season crop," Lee says.

Meanwhile, businesses are also facing increasing break-ins on cloud accounts in 2021 with more personalized ransomware attacks that use employee or manager credentials to penetrate your network.

"The risks are real and the precautions that we take—which might seem extreme to some—are a necessary reality for businesses today," says Craig Ruvere, marketing communications manager for The HC Companies. "The more businesses pivot online, the higher the risk."

Communication is Key

In addition to the threats already mentioned, there's also the age-old problem of employee insistence on using passwords that are ridiculously easy to guess. Relatively new, too, are hackers that prey on small businesses—even mom-and-pops. The reasons? Networks of many large corporations are tougher to penetrate these days and are generally armed with redundant, highly sophisticated state-of-the-art security systems.

In contrast, small businesses, with little or no defenses, are now considered easy marks. That's especially the case given that hackers can use ransomware software that can simultaneously attack hundreds and even thousands of the smallest of businesses.

"Hackers will gain entry to computers and servers simply by an unknowing employee clicking on a (malicious) download that looks legitimate," says Tim Mead, regional sales and marketing director for Johnson Farms.

Indeed, a member of the Lea Valley Growers Association was recently hit with a cyber-attack, according to Lee. He says the hacker most likely penetrated the business' computer system via Team Viewer. It's a computer-sharing application that was installed on the grower's computer, which offered access to its computer system via a remote computer.

The upshot: Businesses need to get current on what's expected to surge in computer network security threats in 2021—and then make the necessary moves to ensure they're protected.

"Focus on business requirements and understand how users and groups access data and applications," advises Kasey Panetta, senior content marketing manager at Gartner, a consulting firm specializing in tech. "Now that a few months have passed since the initial remote push (due to the coronavirus), it's time for a needs assessment and review of what has changed to determine if access levels are correct and whether any security measures are actually impeding work."

Protection Your Network

Towards that end, here are the key moves you need to make to ensure your computer network is protected from the coming storm:

Secure Your Remote Workforce: With so many more employees working from home these days, an IT department needs to take special care to safeguard network connections between work and home are secure.

A good place to start is to require employees to log into your computer network via a Virtual Private Network (VPN), according to the new Kapersky Report, "How COVID-19 Changed the Way People Work."

Essentially a VPN is an encrypted network that your employees use to access the Internet. Given that VPNs are a private gateway to the Internet, they make it much tougher for hackers to study how your employees are using the Internet—including how they share files or how they're using video meeting software.

VPNs also protect the identity of an employee accessing the Internet and they keep private a worker's IP address, location and passwords. VPN access is relatively inexpensive, running about $12 monthly or as little as $3.50/month for three-year plans.

Even with a VPN, it's a good idea to ensure the devices employees use to log in from home need to include security software to protect your business.

Phones used from home by employees are especially vulnerable. Ideally, you'll want employees to use business-issued mobile phones for work. If that's not possible, you'll want to consider specially designed software that separates business data from personal data on employee-owned phones.

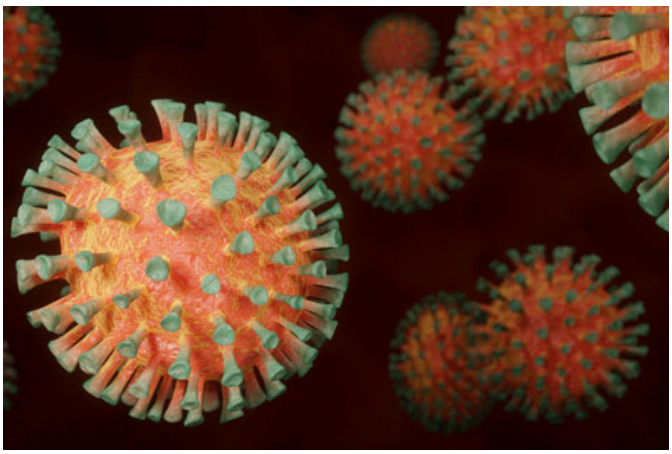
Essentially: Lost phones mean lost business data, so you'll also want to install software on all employee mobile phones offering anti-theft capability, such as remote device location, screen locking, biometric security features like Face ID or Touch ID locking, and the ability to wipe all data from the phone.

Employees using their own phones also need to know that if they lose their phones, you retain the right to wipe all data from the phone if business and personal data is mixed together on the phone.

Double-Down on Email Security: Security pros say employee email remains one of the most common ways hackers use to penetrate a business network, so you'll want to shore-up your defenses in this risk vector, according to Cybriant Managed Security Services.

The coronavirus has triggered a new set of hacker penetration schemes, including malicious emails disguised as info requests on your business' economic stimulus payment request. For an employee, that's a tough email to ignore. Delete a legitimate email and you could be on the hook for the business loss of Paycheck Protection Plan money. Click on a fake email link and you could open up your employer's network to malware, ransomware or another kind of unwanted penetration.

Similar hacker emails are also arriving offering fake advisory news about an employee at your business who's been infected with the coronavirus. And hackers are also having fun spoofing employees with fake notifications regarding a fake shipping problem or fake shipping delay caused by the coronavirus.



Still not enough? Hackers are happy to send your employees emails featuring PDFs and other attachments that promise to detail your business' coronavirus policies. The boldest hackers also demand that your employee click a link inside the email confirming that they've read the policy. That's another easy way to download malware or ransomware.

Pictured: Hackers are piggy-backing on coronavirus fears to break into computer systems.

All told, more than 27% of employees and managers surveyed during the early months of the coronavirus epidemic said they'd received malicious, coronavirus-themed emails while working from home, according to the Kapersky Report.

As always, the best defense against email hacks is to continually refresh employee awareness about the problem. Some security consulting companies specialize in providing ongoing education for your employees—including remote testing of employees by email—on the latest email hacks.

"I believe it's a very good idea for businesses to educate employees about cybersecurity by introducing a trusted and respected resource into the conversation," said Craig. "This helps to better frame the narrative around cybersecurity, why it's important and how individuals can contribute to overall safety."

(For more info, simply Google "Employee Email Security Education.")

More Protections

Beware Cloud-Jacking: With increasing numbers of businesses moving to cloud services, it was inevitable that hackers would follow them there, according to the 2020 Sophos Threat Report. The hacker trick here: These days, even novice hackers can buy automated scripts on the Dark Web that enable them to take complete control of the cloud infrastructure for your business.

Once inside the cloud, a hacker is often able to steal the ID credentials of your cloud's system administrator. Those are essentially the "keys to the kingdom" and can be used to further penetrate your cloud network, steal business data or wreak other havoc.

The move here is for businesses to review the security agreements they have with their cloud provider and ensure

the provider is holding up its end of the bargain. Giving your cloud provider representative a call to ask about special precautions the provider is taking against the latest hacker cloud tricks should help, too.

“Cybercriminals have adapted to capitalize on misconfigured or mismanaged cloud environments,” says Greg Young, vice president of cybersecurity for Trend Micro. “We believe migrating to the cloud can be the best way to fix security problems by redefining the corporate IT perimeter and endpoints.

“However, that can only happen if organizations follow the shared responsibility model for cloud security. Taking ownership of cloud data is paramount to its protection. And we’re here to help businesses succeed in that process.”

Stay Vigilant Against Ransomware: The scourge that keeps on giving, you’ll know you have ransomware on your business’ computer network if a message pops-up announcing your system and/or files are frozen. That message is usually accompanied by a demand that you pay a cash ransom to regain control of your computer network and files.

Ransomware is expected to generate damages to the tune of $6 trillion annually by the close of 2021, according to Jordi Botifll, senior vice president for Cisco Americas. During the past year, ransomware attacks have become more personal, according to a 2020 Trend Micro report, “Securing the Pandemic-Disrupted Workplace.”

Essentially, more hackers are purchasing log-in credentials to specific business systems on the Dark Web and then loading in a ransomware program once they’re inside, according to the report.

Consider Passwordless Authentication: Despite years of admonishments, employees still insist on using passwords that are simple to crack. For hackers, it almost seems too easy. In 2019, for example, the most common password in use was “123456,” according to a report from Splash Data, an Internet security firm. Employees looking to be a bit more clever employed “123456789.” And the next most popular passwords in descending order were “querty,” the ever-imaginative “password” and “1234567.”

No wonder an increasing numbers of firms are turning to password alternatives to secure their networks. Popular techniques include Touch ID, Face ID, ID using a call or text to an employee smartphone, and one-time passwords that are generated and sent to an employee’s email address after an employee ID is entered.

Forget Zoom-Bombing: Early on in the epidemic, web video meeting software firm Zoom got a bad rap from pranksters who began popping into business video meetings to cause trouble. They screamed expletives, exposed body parts and generally acted-up like 6 year olds. To be fair, Zoom always had privacy controls, but they were a little tough to find. Fortunately, Zoom has since updated the security on its video meetings and made its security controls much easier to find and use.

Like Skype, GoToMeeting, Cisco Webex Meetings and BlueJeans, Zoom has become a staple among companies looking to put together meetings on-the-fly.

Consider an AI Upgrade: As with virtually every other aspect of business software, some of the newest network security systems come with an artificial intelligence component. These new AI systems often lurk in the background, watching hackers as they poke around business networks, taking note of tricks and techniques hackers are using and then auto-building scripts to frustrate those same hacker moves the next time they pop-up. (For more info, simply Google “AI computer security” or “AI cloud security.”)

In the end, when in doubt, ask a professional.

“I think investing in the protection of your network is a no brainer,” says Marisa McTiernan, office manager at The Garden Factory. “The stakes are too high to be flippant about web security. We decided to look to an outside IT company instead of trying to do it in-house, which was the right fit for us.

“We are able to focus on growing our business—with the peace of mind that our network is protected.” **GP**

Joe Dysart is a speaker and business consultant based in Manhattan with more than 20 years of experience writing about tech-related issues. He can be reached at: (631) 438-1142 or joe@dysartnewsmedia.com.

FYI

Here are links to a few of the reports mentioned in the story, plus some company websites:

- How COVID-19 Changed the Way People Work: tinyurl.com/mdummzpm
- Securing the Pandemic-Disrupted Workplace: tinyurl.com/aaz8z4n9
- 2020 Sophos Threat Report: tinyurl.com/4zstt2s5
- Gartner, a company specializing in tech consulting: gartner.com
- Cybriant Managed Security Services: cybriant.com