Don't be held hostage by ransomware.

One wrong click and you're out $146,900.*

What starts as just a single click by one employee could jeopardize your company's entire future. At any time (even as you are reading this article), one of your staff members could be opening a phishing email. If they click on the attachment or click through to a website containing encryption malware, the malicious software will immediately take control of their device and begin encrypting your data. Within minutes, you will be blocked from having access to your own computer systems and information. Soon, the cyber criminals responsible for the attack will contact you asking for a ransomware payment to decrypt your data and restore your access.

SMALL-TO-MEDIUM SIZED BUSINESSES ARE BEING TARGETED

You might think, "This will never happen to me; this only applies to large companies." Not true -- ransomware is wreaking havoc on small-to-medium-sized businesses (SMBs). The average cost of ransomware for a SMB is $146,900, more than a 200% increase over 2018.* Unfortunately, many business owners do not realize the severity of this digital threat.

> The average cost of ransomware-induced downtime for a SMB is $146,900, a more than 200% increase over 2018.*

Phishing emails are the main cause of ransomware attacks and ransomware is the fastest growing type of cybercrime in the world. According to the Federal Bureau of Investigation's 2018 and 2019 Internet Crime Reports, there was a 37 percent annual increase in reported ransomware cases and a 147 percent annual increase in associated losses from 2018 to 2019.**

Many SMB companies today are totally unprepared for a cyber event, especially if they do not have an information technology (IT) resource. Even if they do have an internal IT function, many teams are overextended and are not able to stay ahead of the cyber-threat curve. They may not be aware of the significance of phishing and ransomware risks.

WHAT'S THE BEST WAY TO SECURE YOUR BUSINESS?

Today's cybersecurity threats target your people, not your systems. While many technology solutions will identify and block phishing emails that can lead to a ransomware attack, your employees will always be your best prevention.

If you think your business is safe with a firewall, think again. Typically, perimeter security only manages 30% of cybersecurity risk.

By implementing a **user awareness program** and educating your employees who are the ones receiving the phishing emails, you can help to secure your business. They can learn to recognize phishing emails and handle them appropriately, instead of clicking on a link that can lead to a cyber-attack in your company.

In addition, a **ransomware preparedness service** can identify weaknesses in your business that could be exploited and harmful to normal operations. This service typically includes diagnostics to pinpoint key controls and technical issues that can make your company more susceptible to a successful ransomware attack. You can also receive recommendations to guard against significant and costly disruption.

THE FIRST STEP IS TESTING YOUR EMPLOYEES

Through a targeted phishing campaign, you can get a baseline of your employees' current level of awareness and then begin to educate them on phishing schemes. Your staff should understand the severity and long-term impact of cyber and social engineering attacks and be able to recognize the red flags.

Your staff is your first defense against phishing. They can be your "human firewall".

Your people need to practice regularly to become adept at recognizing and dealing with phishing emails properly. Some training campaigns can be executed quickly and the results can be leveraged to improve the overall effectiveness of your information security program and reduce the likelihood of an effective cyber-attack.

A CASE STUDY THAT IS CLOSE TO HOME

In late 2016, when UHY Consulting was being flooded with phishing emails and malware, we started an active phishing campaign with our own employees. Our security team ran an unannounced phishing test to our entire employee base and our results were typical.

UHY Consulting employee phishing test results:

- 30% clicked on embedded links in the test emails.
- 16% supplied personal information on the linked phishing pages.

We reviewed the results with our staff and explained how the firm could have been negatively impacted. They were surprised by the results – that by simply opening an attachment and clicking on a link could result in a malware or a data breach.

UHY Consulting now deploys a program that mimics the most prevalent and successful real-world phishing emails to provide practice opportunities. Over time, UHY Consulting's risk rating for phishing-related cyber-attacks has decreased from 30% to less than 3% due to the regular training provided to our team members.

A study by the Ponemon Institute found that training can reduce employee click-throughs on phishing emails between 26% and 99%, with an average improvement of 64%.

TIPS FOR GETTING STARTED

First, recognize that your existing IT resources are already overwhelmed. They need help, even if they indicate they don't need it. Give them permission to ask for help. Assist them in identifying allies in the battle against cybercrime who have experience in designing and implementing phishing and awareness campaigns. Talk to them about creating a comprehensive user awareness program for your employees that will include internal phishing campaigns.

Second, with your allies' assistance, arrange for an initial phishing campaign to test your staff. The fees associated with conducting the phishing campaigns may depend on the number of email addresses, email templates and landing pages.

Third, ensure that this partner has the tools and training necessary to educate everyone at your company. Remember, to be able to recognize and deal with phishing emails properly, employees will need to practice their skills.

Fourth, each campaign should report results and highlight risks to help you implement a more effective training and awareness program for your business going forward.

DON'T LET YOUR BUSINESS BE HELD HOSTAGE

The UHY Consulting Cybersecurity team can design and implement a **comprehensive user awareness program** to decrease your risk of phishing attacks. In addition, **ransomware preparedness** can help make your company less susceptible to a successful ransomware attack.

We understand the challenges and resource constraints of running a small-to-medium-sized business, so **our cybersecurity programs start at $2,500**.

Contact us directly at 630-288-6992 or email cyber@uhy-us.com. uhyconsulting.com

[*] Fourth annual Global State of the Channel Ransomware Report, published by Norwalk's Datto Inc. 2019.

[**] Compare Federal Bureau of Investigation, Internet Crime Complaint Center, 2018 Internet Crime Report, at 19, 20, available at https://pdf.ic3.gov/2018_IC3Report.pdf, with Federal Bureau of Investigation, Internet Crime Complaint Center, 2019 Internet Crime Report, available at https://pdf.ic3.gov/2019_IC3Report.pdf.