CYBER CREEPS AND COVID-19

BE WARY

OF THESE

I.T. THREATS

N-LINE
TECHNOLOGIES

INTRODUCTION

Business owners already have enough to worry about with COVID-19 sending everyone home to work. Too bad cybercriminals are such opportunistic creeps: they are even taking advantage of the global health pandemic to scam the unsuspecting. This eBook highlights many coronavirus-related scams. Be aware, so you can educate employees and best protect your business.

Email remains the number-one means of cyberattack. Cybercriminals are increasingly sophisticated and always motivated. Today, companies from any industry of any size can face a targeted threat.

Whether it’s a phishing attack or a malicious attachment, these bad actors prey on human nature. They will target your staff’s heightened fear and desire to help or tap into the near-Pavlovian response to urgency or a "steal of a deal.” Right now, they are looking to benefit from worldwide anxiety about the coronavirus pandemic. While businesses grapple with remote work processes, cybercriminals find new weaknesses.

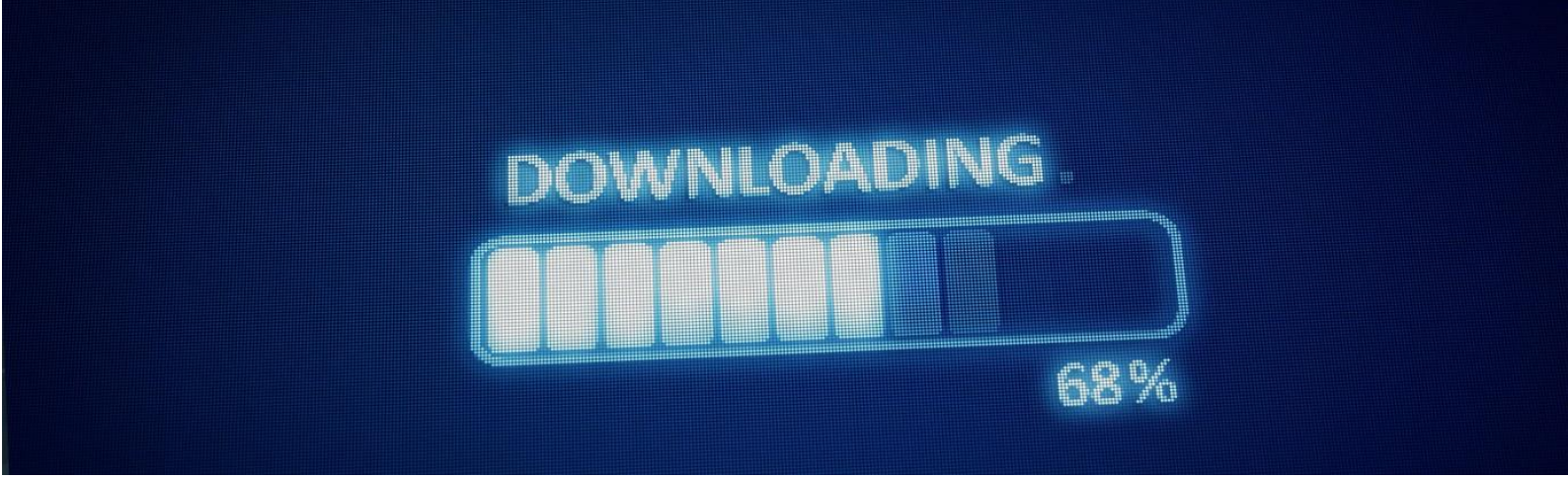
This roundup of known threats related to COVID-19 can help an IT team ramp up cybersecurity. We will also discuss the need to educate employees, then we'll suggest a top solution for protecting business email communications.

COVID-19 SCAMS OUT THERE

Cybercriminals are nimble crooks who capitalize on current events. As soon as there is a fresh news story or angle for their attacks, they adapt quickly. Right now, they are taking advantage of the coronavirus. As businesses change the way they work, bad actors see an opportunity to find new entry points. They will try any means to phish for sensitive data, breach systems, or deliver malware.

Scams aren't new; it is a matter of how they're packaged. In the past, a Nigerian prince wanted to send you millions. Now, many governments are giving out money in the form of economic stimulus payments. The scammers leaped right in. Scam emails ask for bank information to pay relief funds directly, or the emails request other personal data you do not want to reveal to a criminal.

Fake bank, telephone, or insurance company phishing emails are another problem. These ask for personal and financial information, lure the user into opening malicious links or attachments, or seek remote access to the user's device. Emails impersonating healthcare organizations are also common. The CDC, WHO, and other healthcare organizations are not reaching out directly.



Downloading a “Safety Measures” pdf or the like could introduce malware or take an employee to a malicious site. A fake virus tracking app is set up to deliver malware. The ”COVID19 Tracker” app infects a device and demands $250 in Bitcoin. Emails offering fake news about someone infected in the area are another tactic. Sometimes, cybercrooks target a business with a communication saying there is a shipping problem caused by COVID. Saying a package is held up, the email encourages clicking on a malicious file or link to remedy the problem.

Hackers are even gaining access to corporate email addresses or relying on a close approximation to fool the busy reader. Then, they send links or attachments promising to outline company coronavirus policies. Often, these will ask the user to log in to view the necessary documentation. If the user does not question the communication, bad actors capture employee access information.

Your IT team does not have to look at flexibility and security as a sliding scale. Digital technology balances both the need to accommodate work from home, and to protect business systems and networks.

EDUCATE YOURSELF

People are the foundation of your business success. At the same time, they can also represent a real security threat. According to Experian, only 45% of companies have mandatory cybersecurity training.

Yet your staff needs to understand the many ways in which they can put your business at risk. IT cannot be the only team making cybersecurity a priority.

In educating employees about potential cybersecurity issues:

- Impress the importance of caution and questioning the source of any communication with links or attachments. Hovering over URLs can show where the link leads. Grammatical and spelling errors are often a red flag, too.

- Require installation of the latest malware, antivirus protections, and security patches.

- Explain why you have an acceptable-use policy. Talk about what could happen if they decide to download that one app from the Web to their work device.

- Warn them about installing random USB drives hoping to connect the stray device to its owner. Dropping thumb drive devices is a common way cybercriminals gain illicit access.

- Emphasize the importance of physical security, too. A stolen unencrypted laptop or someone accessing an on-site computer can lead to a breach.

- Provide them with a way to report suspicious emails, communications, and potential compromise.

PROTECT YOUR BUSINESS

Even after you have taken the above advice to educate employees, there are still risks. Some of these emails are very convincing. People are busy, working fast, tired, and overly trusting. Additionally, these particular scams are targeting our preoccupation and fears around the coronavirus.

IT can do its best, but it only takes one bad click to breach your system.

An email gateway is the best defence against email malware. This solution removes malicious files or links before they reach your employees' inboxes. A gateway scans all business emails for signs of harmful content.

This can include scanning outbound and internal emails. Why would you want to do that? To protect yourself from data loss or compliance risks. For instance, gateway email archiving stores communications for later audits.

PROTECT YOUR BUSINESS

Secure email gateways provide protection by offering:

- Spam Filtering
- Virus and Malware blocking
- Phishing Protection
- Admin controls and reporting

The email gateway collects different cloud-based technologies working together to block threats. Working as a firewall, the gateway enforces rules about what email can enter or leave the network. As this is done on a network level, it also means the protection works on all devices, whether your staff is on-site or working remotely.

WE CAN HELP

Installing gateway email protection may be one more thing to add to an already extensive “to do” list. IT has had to adapt to a lot of changes lately, and with some businesses reopening, there are more transitions to accommodate.

N-Line Technologies

Phone: **(432) 279-0671**

Email: **nathan@n-linecomputers.com**

Web: **www.n-linetech.com**

Facebook: **facebook.com/NLineTechnologies**