21st Century Crime Prevention:
How to Protect Against Cybercrime

It has been called “the crime of the 21st century” and even ranked by the Director of National Intelligence as the top national security threat — ahead of terrorism and foreign espionage. We’re talking about cybercrime.

The most recent statistics bear out this concern. In the 2018 U.S. State of Cybercrime Survey, published by IDG, cyberthreats continue to be most important, as two out of three respondents (66 percent) are more concerned with cybersecurity threats in 2018 than they were in 2017. And in the 2018 Internet Crime Report published by the Federal Bureau of Investigation, cybercrime cost businesses a collective of $2.7 billion in 2018.

A Prime Target: Mid-sized Companies

Much of today’s cybercrime is being perpetrated by highly organized cybercriminals based overseas. Many of them are specifically targeting mid-sized U.S. companies that are in the cybercrime “sweet spot”: large enough to have significant corporate bank accounts, but not big enough to possess and deploy sufficient cyber-security controls.

Their goal is to obtain sensitive information like user names and passwords that gives them access to corporate bank accounts. With this access, cybercriminals can make unauthorized banking transactions and steal tens (or even hundreds) of thousands of dollars straight out of corporate coffers.

“The CEOs and CFOs of middle-market companies today need to be especially vigilant when it comes to guarding against cybercrime,” says Cadence Bank Treasury Management Executive Katrina King. “It’s almost impossible to ensure 100 percent cybersecurity, but there are steps businesses can take to significantly reduce the risk of a cybercrime breach.”

Cybercrime security starts with recognizing the biggest threats. One of the most common ways cybercriminals break into corporate bank accounts is through business email compromise (BEC), a catch-all phrase for several
crimes that leverage tactics – like phishing, targeted email spoofing and other forms of credential theft – to facilitate the fraudulent transfer of funds. Cyber thieves continue to hack or spoof email accounts of C-level executives to initiate wire payments to fraudulent beneficiary accounts. In recent years, the scam has extended to personal email compromise, vendor email compromise, and targeting of the real estate sector for both buyers and sellers. BEC attackers rely heavily on social engineering tactics to trick unsuspecting employees and executives. They also carefully research and closely monitor the potential victims and organizations.

Educate Your Employees

While cyber thieves also use other more sophisticated techniques to launch cyber-attacks, middle-market companies can go a long way toward reducing cybercrime by simply educating employees, particularly those in finance and accounting, about these kinds of phishing and spear phishing scams. Train employees to never reply to an email like this with sensitive account access information, never click on links in emails like these, and never make payment changes without verbal confirmation.

Also urge employees to use caution with social media. Increasingly, cyber thieves are trying to trick social media users into downloading malware or giving out account access information. Establish policies that define what types of social media use in the workplace are and are not acceptable and consider restricting access to some popular social media sites.

Today, mobile devices have become a primary target of cyber thieves, since they represent relatively easy points of entry. So, employees need to be vigilant in protecting their work-issued smartphones, notebooks, tablets and laptops. Many of today’s mobile devices can be protected with mobile device management software that enables protections, like locking down browser access and limiting downloading of third-party applications by employees. The key is to balance cybersecurity protection and employee productivity.

In addition, Trusteer Rapport™ is a security software application that protects users from financial malware and phishing attacks. It is available at no charge to Cadence Bank clients.

Contact Us

To learn more, contact your local Cadence Treasury Sales Officer or Treasury Client Support at 1-800-329-0289 or treasurymanagement@cadencebank.com.