THE CREDIT TIMES

CCC of New York
Serving the Credit Industry's Professionals

March 2022

A Publication of The Commercial Collection Corp. of NY, Inc.

Business Fraud And Cybersecurity Best Practices in the Office or While Working Remotely

By: Wanda Borges, Esq.
Borges & Associates, LLC

Since the onset of the coronavirus pandemic, the majority of businesses have employees working from home. In the midst of many businesses reopening their doors to full-time office work, the rise of the variants caused those businesses to reconsider and maintain a remote work environment. While this new "normal" has been beneficial to most people and companies, the door has been opened to cyberattacks. The advantage of enabling employees to work remotely allowed businesses to continue to operate. But, with those advantages, along came cyber-risk. Home computers or other remote locations are more vulnerable than ever to cybercrimes. Business email compromises ("BEC") became the number one cybercrime in 2020. In 2020, the FBI Internet Crime Complaint Center ("IC3") received nearly 20,000 complaints about BEC, with reported losses due to the attacks increasing to $1.86 billion from $1.29 billion in 2018. The FBI defines BEC as a sophisticated scam targeting both businesses and individuals performing a transfer of funds, and its website states that the scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques resulting in an unauthorized transfer of funds.

Credit professionals can be exceptionally vulnerable to cybercrime, which can be defined simply as Internet fraud. The five elements of fraud that exist in any cybercrime scenario: 1). the criminal is lying to you and trying to convince you that what they are saying or offering is true all the while 2). knowing that its statement is untrue and 3). using the statement ["click here"] to deceive you into opening an email or clicking on a link and you 4). justifiably rely on the statement believing it to be true which 5). causes harm to you (or your company) as a result of the falsehood.

The most common cybercrimes today are: Malware (includes Phishing, Ransomware, Trojan Horses, Crypto Mining) – generically – Hacking, Debt or Credit Card Fraud, Data Breaches, Compromised Passwords, Business Email Compromises, and Social Media Access.

Companies need to create people-centric cybersecurity strategies to protect against these cybercrimes, particularly Business Email Compromises and Ransomware. In that this article is just a snippet of information available to the credit professional on cybercrimes and cybersecurity, it will focus on these two areas of cyberattacks.

continued on next page...

In this Issue

Management Team

Congratulations to Lisa Erce from Wuxi AppTec on winning an Echo Show 5 in our drawing.

Make sure to enter this month's drawing by using your Special Placement form. For every claim you place you will be entered for a chance to win an Echo Show 5.

Certified By CLLA
Endorsed By IACC

con't

Business Email Compromises ("BEC")

The chart below is a prime example of an attempted BEC. This is a copy of an actual email received by a corporate business account.

Click on Release, to free these messages to your inbox and to Verify your Mail Account : Deliver Messages

Quarantined email			
	Subject:	Subject:	Date:
Release	Re:Enquiry/Consultation	RE: Send PI Asap for payment	10/12/2021 5:19:49 p.m..
Release	Re: Balance Payment	RE: T/T Payment Copy	10/12/2021 5:19:49 p.m..
Release	Re: Account Statement	RE: New Purchase order	10/12/2021 5:19:49 p.m..
			Deliver all messages (3)

Within this one email, there are five separate places which will open the door to the cybertheft. By clicking on any of the four words "Release" the door will be opened. Or by clicking on the phrase "Deliver all messages (3)" the door will be opened.

Ransomware

Ransomware is a type of malicious software, or malware, designed to block access to a computer system until a ransom is paid. Ransomware is generally downloaded inadvertently. You may visit a website and suddenly a message pops up on your screen. These are some of the common messages that we see:

"Your computer is infected with a virus. Click here to resolve the issue"

"Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a $100 fine"

"All files on your computer have been encrypted. You must pay $500 within 72 hours to regain access to your data"

Ransomware may even be hidden in a link from a company or person that you know. Always use caution when opening a link even from a person you know. If you suddenly receive an email that you weren't expecting from a friend or a client or a colleague excitedly telling you to open the link because it is something you are going to want to see, DON'T. Call your friend, client or colleague (Yes – pick up the phone and call) and ask if they did, in fact send something to you. The odds are you will be told that they were hacked, that nothing legitimate was sent to you and that you should not open any link contained in an email because it did not come from them. Clicking on the link will immediately infect your computer.

More important than anything else - NEVER PAY THE RANSOM!!!!!!! Paying the ransom doesn't work and will likely cause more damage to your computer.

For more information on any of CCC's services...
3rd Party Collections
Business Process Outsourcing (BPO)
Preliminary Notices/Mechanic's Liens
UCC Filings
Credit Reports
Please contact Chad Haynie at 1-800-873-5212 or Email chaynie@commercialcollection.com

The Commercial Collection Corp. of NY, Inc.
PH: 800-873-5212 / Fax: 800-873-5211
www.commercialcollection.com