PNC C&IB TM Fraud Response Video Transcript

Title: PNC COVID-19 Response – Full Video

PNC Employee: Howard

Transcript: Hi, I'm Howard Forman and I lead the digital channels group at PNC in our treasury management division. Our team focuses on the management and development of PINACLE, which is our online and mobile banking platform, and I also focus on our API development and our file transmission platform.

I spend a lot of time with our PNC cybersecurity and enterprise fraud teams, monitoring the fraud environment and working to help keep our customers' online access safe and secure. And I'm pretty passionate about online security and doing what I can to help our clients protect themselves, because online fraud really is a pretty serious problem for businesses of all sizes. So, I'm here to share some information to help you protect your organization.

The biggest fraud threats we're seeing right now are business email compromise, or BEC, and account takeover. Both of these threats have been around for several years because they are such successful fraud schemes, especially BEC. In fact, the FBI reported that in 2019 there were over 23,000 cases of BEC with victim losses totaling almost $1.8 billion. Pretty staggering amount of money.

A BEC scheme involves a request to initiate payment or a change of payment routing instructions on a legitimate payment. And the request comes from somebody, the victim, that is the recipient of the email, somebody that you generally trust such as a company executive or a known business associate such as a supplier that's expecting a payment. And what makes these requests so dangerous is that the email request comes from a fake email account that is really difficult to identify as fake, or, worse yet, it comes from a legitimate email account that's actually been compromised by a criminal.

Account takeover is a very different type of attack. It typically involves theft of your online banking credentials through the use of malicious software or what we call malware. And that malware gets installed on your desktop, PC, or laptop, and then that malware typically redirects your online banking session to an imposter site that looks exactly like the legitimate site you're trying to reach. So, when you attempt to log in, the imposter site is actually harvesting your security credentials, which the criminals then use to log in to the legitimate site and initiate fraudulent payments. So, both of these are pretty, pretty scary fraud schemes.

There's a few ways the current environment has made things a little bit more treacherous than usual. First, most online fraud begins with email phishing attempts. And phishing, if you're not familiar with the term, is a way in which criminals try to obtain sensitive information or infect the PC, typically by impersonating a trusted entity or by including infected attachments or links to malicious websites in emails that are used to draw the recipient's attention.

Now not surprisingly, we've seen an increase in COVID-themed phishing emails that are either promising information on cases in your geographic area, or even in your specific organization, or maybe COVID cures or potential vaccines. And all of these emails are very tempting to anyone that is anxious over the current situation.

Also, many employees are working in alternate or non-standard work environments where they may not be able to follow their standard procedures related to initiation of payments. So, an email payment request from a business-email-compromise attempt may be less recognizable as fraud.

There are several best practices I think every company should follow to help protect against a pretty wide range of online threats. And I think an easy way to remember these is to think of five E's.

So, first, I would say educate. We have to make sure all of your employees understand the threats posed by phishing attempts and that the employees know never to open attachments or click on links and emails from unknown senders. They should also never respond to an email request for personal information, online banking credentials or any other sensitive information. And as part of the education, let's make sure that employees understand the details of business-email-compromise and account-takeover threats, so that they can learn to recognize these fraud schemes when they occur.

Second, companies should establish policies and procedures for payment and vendor-management processes. For example, you should always verify and validate email payment requests verbally with the requester at a known phone number. Never verify a payment with another email. 'Cause chances are, you'll be communicating with the criminal.

Three, enforce those policies and procedures that you've established.

Fourth, empower employees to question suspicious emails or suspicious payment requests, especially if they appear to be coming from company executives.

And fifth, evolve or enhance, whichever you prefer, your risk controls to scale with the changing threat landscape. Because the criminals are always modifying their fraud schemes.

In closing, I'd once again like to remind everybody that online fraud is a serious problem and it's a serious problem for businesses of all sizes. I hope the information I presented here today helps you protect your organization and keeps you safe and secure. Thanks for listening.