25-039C Fraud Event Meeting - BEC V2-L-Res

0:00
They're basically three different types of business e-mail compromise.

0:04
There's executive impersonation, it's called executive e-mail intrusion.

0:08
So in essence, what this is, is the fraudster is posing as an executive of the company or that trusted advisor, as you mentioned, key that that is going to ask for a payment to be made or a change to a payment to be made.

0:23
And so, you know, it's an authority figure.

0:26
They're saying they're sending an e-mail to the accounts payable department to say we're buying a company or we're investing in something I need for you to send a wire transfer to, to this routing in transit and account number to, to start this process.

0:43
And so, you know, you get an e-mail from the CEO who's asking you to do something and you feel pretty good about that, right?

0:48
And, and so you, you create that e-mail and you send it to the routing and transit and account number that that the executive instructed you to use.

0:59
And so later on, you're walking down the hall and you bump into that person and and then say, hey, I did sent the $1,000,000 wire that you told me to send through your e-mail.

1:10
And they look at you and say, I have no idea what you're talking about.

1:13
And so you can imagine that sinking feeling.

1:15
And your first thought is I got to get my resume together.

1:18
I've got things that I've got to do.

1:20
I need to call my family because this is not going to go well for me.

1:25
So but you're acting on and operating off of the the instructions of that, that trusted partner or that executive.

1:33
The second one is vendor e-mail intrusion works very similar.

1:37
Vendor e-mail intrusion and employee e-mail intrusion are very similar in nature because what what the fraudster is doing is posing as one of your legitimate vendors or they're posing as a legitimate employee and they're asking for you to make a change in the payment that you are that, that you've been to the routing and transit number, the account number that you've been paying in the past.

2:00
The in the vendor situation, it's typically going to say something like or even employee to we changed our banking relationship.

2:11
We're not banking here anymore.

2:13
We're going to bank it at bank B now.

2:16
So here's the new routing and transit and account number for your next payment.

2:21
The other thing on the vendor side is we're not taking checks anymore.

2:24
They've listened.

2:25
They're not going to accept a check.

2:27
They're going to only accept payment through a digital payment channel like ACH.

2:32
So here's the routing and transit and account number you need to use for your next payment and it needs to be through ACH.

2:40
So of course that payment now is going to an account controlled by the fraudster.

2:45
And if you think about the typical collection cycle, business collection cycle is, you know what, 30 days at least net 30, but it's typically going to be 60 or 90 days before your vendor comes back to you and says we didn't get paid.

3:00
So you know, that collection cycle takes a while.

3:03
Well, when that happens, that money's long gone because you it's 30 to 60 days then before you recognize that you that you either made that change on the instructions of the e-mail because you'll tell the vendor, the vendor sure, we did exactly like you instructed us to do and the vendor comes back and goes, that's not my e-mail address.

3:23
And then under really close scrutiny, you look at that and you can see that there maybe was a letter transposed or an S that was added to the end of the the e-mail domain.

3:35
Or because think about how easy it would be to miss if a lowercase L is in the e-mail address to replace that lowercase L with the number one or an uppercase I depending on the font that's used in that e-mail string.

3:51
It's very, very difficult to detect those.

3:54
So it obviously bears paying very close attention to the e-mail addresses because it happens on both cases.

4:02
And it's really, really important that the faster that you notify the bank, whether you bank with us or not, the faster you notify the Bank of of one of these types of situations, the greater the likelihood that we're going to be able to recover for you because we're going to do everything in our power.

4:21
Certainly we are at regions going to do everything in our power to try to recover your money for you.

4:27
But the truth of the matter is we're not always successful.

4:30

And if you look in the AFP survey, 30% of the companies responding to the survey indicated that they were able to recover absolutely nothing.

4:39
So it if it happens and it's a tough situation, it's a tough conversation because you know, it's it's one of those things you acted on those instructions, you emailed that or, or you created that transaction and originated that transaction legitimately and it just went to the wrong party.

5:00
So it's really, really important that you notify us as quickly as you know something.

5:07
As I mentioned, these typically happen as a result of phishing.

5:10
I mentioned the e-mail spoofing where they change the letters creating look alike domains where they add an S or they transpose a letter to it looks like Jeff Taylor Toyota, but maybe Toyota is spelt differently and you don't pick up on it.

5:26
There's a thing that's called nesting and it's where the fraudster through typically through malware has been able to embed themselves in your legitimate vendor's e-mail platform.

5:37
And so when they're they're in there and they're watching that e-mail traffic back and forth and determining just the right time to insert themselves into the conversation.

5:47
And so this nesting process is even more difficult to detect because it's coming from your legitimate vendor's e-mail address.

5:56
And so you have to look at things like sentence structure and, and think about, is this the way my vendor typically talks to me?

6:05
And is it?

6:05
Is it?

6:06
Are these the types of phrases that they use?

6:10
One of the typical red flags and and this is it's not on the slide, but one of the typical flags in this is the word kindly.

6:19
KINDLY.

6:21
You think about it.

6:22
We don't use that phrase very often, do we?

6:24
You don't say something like kindly process this payment by the end of the day, but the fraudsters use that because these are typically nation state actors that don't have the same kind of command of, of English or they don't operate under the same types of phrasing in English that we do.

6:44
And so so kindly you see an e-mail that has the word kindly in it.

6:51
Probably stop what you're doing and we'll talk about stop, call and confirm, but make sure that you pause a little bit when you see that.