Barclay Damon Live Presents *Cyber Sip™*
Season 3, Episode 4: "Money Intercepted! The New Risks of Funds Transfers," With Kyle Cavalieri

Host: **Kevin Szczepanski,** Barclay Damon

[Kevin Szczepanski]: Hey, everyone. Welcome back to Cyber Sip. I'm your host, Kevin Szczepanski. And I am pleased to be joined today by Kyle Cavalieri, who returns to talk today about the risks of funds transfer fraud. Kyle is the president of Avalon Cyber, and he has 15 years of experience providing consultative services, including forensic incident response. Welcome back to Cyber Sip, Kyle.

[Kyle Cavalieri]: Thanks, Kevin. Glad to be back.

[Kevin]: And I'm glad to have you back to talk about an alarming topic that we're seeing occur much too often. And I think it's going to get worse before it gets better, and that is funds transfer fraud. So we're going to talk about what it is, how it works, what are the red flags to watch out for and how, if at all, the audience can prevent funds transfer fraud. Because as you and I both know, once that money goes out of a customer's account, it is very, very difficult to get it back.

[Kyle]: Yeah, exactly right, Kevin. You know, just a little bit about the funds transfer fraud as a whole. Just a little bit of a background on it for our listeners. You know, the actors are essentially able to misdirect funds either directly from the organization that you work for or to any customers or vendors that you have relationships with. And there's a lot of different ways and techniques that they use in order to kind of insert themselves into communication that ultimately lines up, ends up with funds or transfer of funds into the threat actor's wallet. And we'll talk a little bit about that during today's session.

[Kevin]: Thanks, Kyle. No, we definitely will. So, Kyle, how does this work? How does a threat actor position himself to be able to convince an organization to part with its money in one way or the other?

[Kyle]: Yeah, sure. Yeah. So with any attack of varying levels of sophistication, the threat actor is doing what we like to call in the industry "open-source intelligence gathering" about whoever their target might be. You know, so for instance, a threat actor might gain access to personal information or company-related information that they've gained access to through maybe the dark web. So stolen information that could have been placed there from some other previous cyber-attack. And usually what happens in those previous cyber-attacks, that information is kind of packaged up and sold to a bidder on the dark web, which contains a variety of types of information. It's not usually just usernames and passwords. It can be account numbers. It could be just, you know, company relationship information, any little bit of information that they can glean about a particular target is going to be helpful here. Once they have enough information— through any form of research or open-source intelligence gathering that they're doing—they're going to then figure out how they're going to conduct their attack in a common vector in order for these attacks to be successful is through phishing attacks. And when they're creating these types of phishing attacks, they are putting together some bits and pieces of information that seem very believable. And it might get somebody to click on something, download something, or open up an attachment to an email that you maybe wouldn't have normally done. Because again, they're putting bits and pieces of information that looks to be very believable. Outside of the traditional phishing type attacks that you normally see, "vishing" is becoming a very common target or a vector that the threat actors are using. So what is a what is a "vishing attack"? A phishing attack is simply it's a voice-phishing type of attack. Right. It's shortened. And essentially what that means is that you're picking up the telephone and you're contacting, you know, whoever the target might be and giving them bits and pieces of information that looks believable with the hopes that they're going to ultimately give up something that's going to allow them to further their attack.

[Kevin]: So can I interrupt for a second, Kyle, and just ask you a general question? Can you hold that thought?

[Kyle]: Yeah.

[Kevin]: I wanted to ask you about phishing in particular and vishing with a "v," so to speak, because I would think that that is that poses a much greater risk and higher failure rate for a threat actor. You're not just creating an email that looks legitimate and to entice someone to click on a link or open an attachment, you're actually on the phone live with the victim. And I would just have thought generally that is a less favored attack vector because so many things can go wrong, but it's not. In fact, it's on the rise. Why do you think that is? Is it just that there's a bigger pot of gold at the end of the rainbow, so to speak?

[Kyle]: I think once you get somebody on the telephone and you have, you know, a very well put together story that can be told, you're much more likely to get reaction and response, especially if you kind of twist that conversation with some sort of heightened level of emergency. Like, for instance, I might call you and say, hey, Kevin, I'm from XYZ Financial Institution. We're seeing some unusual activity that has to do with your account. Can you verify some information for me to ensure that everything is okay? You might say, well, hey, you know what? I get phone calls and text messages from my financial institution all the time. This seems to be in line with what we would normally expect, only until you get to the point of the conversation where they're asking for things like, can you give me your multi-factor authentication code? Can you give me your mother's maiden name? Can you give me some sort of security code that now the adversary has some additional information about you which they can use to further their attack against whatever they're trying to get after...so that's just an example of the types of things that we see specifically relating to vishing attacks, because they can be much more personable and you're much more likely to get an extension of your activities because of that sort of personal connection right now.

[Kevin]: Right. I interrupted you earlier, and I want to take you back to where you were when we left off. So we have a threat actor who has done some research, maybe use some stolen information on the dark web to create a targeted phishing attack or vishing attack. Spear phishing, spear vishing attack. And should we use the example of someone on the phone? Does that work for you? What happens next? So the threat actor has built this scenario.... What does he (and in most cases it is a "he" for whatever reason), what does he do next and how does he keep the victim on the line, both literally and figuratively?

[Kyle]: Yeah. So, again, it's creating some sense of urgency, making it feel like there is an emergency that requires their immediate attention through some sort of personal connection. Once you have that, you get that bit of information, you're going to be much more likely to further your attack scenario. You know, once they have the access that they need, whether it's through a vishing process, which ultimately gets them access to maybe, let's say, your bank account or your web portal, they can transfer funds, whether it's through ETF or something else like that, or they can move money into another account that you don't have access to. They can do whatever they need. If they're just accessing your bank account. If they're accessing... if they do like a business email compromise where they figure out a way to get into your email system, now they have a whole treasure trove of additional information contained within your email, such as account numbers that you may have or maybe even your clients or vendors are using. They're seeing communication, obviously, through email that you may be talking about an upcoming invoice that's going to be coming due. You may be talking about some business changes that could be happening and they're going to see that sort of info. Once they identify in appropriate time and place, they will insert themselves into that communication through email to make it appear as though that they are somebody working, let's say, in the accounting department of a particular company and they might be reaching out to a customer or a vendor and saying, hey, we've made some financial changes or bank change on our side. We need you to update some information on your system so that when you pay the next invoice that we send you, we're going to need to have that routed to this other bank account. And so, you know, they have very specific rules and behaviors that they follow in order to hide those types of activities going on within the mail system, which the user is going to be continuing to do what they normally do. But unbeknownst to them, there's a side conversation that's being happened through their email account with customers or vendors and trying to get them to divert their funds into the threat actor's bank account or wallet.

[Kevin]: I'm hearing you describe this, Kyle, and I'm thinking we're sitting ducks. What hope do we have? We have a threat actor impersonating us with our own information, communicating with a vendor, trying to divert payment from us to the threat actor's account. Or you had the threat actor impersonating your own financial institution using actual information that it's stolen from the dark web or has gathered from the Internet. And that communication, whether it's by email or whether it's by phone, is designed to sound similar, if not identical to the actual communications that you will have with your vendors or your financial institution. So I don't know if this is an appropriate time to ask, but the question I have then is: what are the red flags that our audience can look out for that might clue them in to the possibility that the communication they think they're having is not legit?

[Kyle]: Yeah, Kevin, that's a great question. And normally I would always say, you know, go back to the, traditional security awareness mindset of being able to detect these types of phishing emails that might be coming into your system. Usually there's, you know, grammatical issues or it doesn't sound right, you know, those types of things that are usually like... jump off the page at you. But with the introduction of artificial intelligence, it's very easy for a threat actor that might be, you know, Eastern European and English is not their primary language, it's very easy for them to go into an AI platform and type into the command lit to say, hey, write me an email that the intention is to get them to change banking instructions related to these types of services. Within seconds, artificial intelligence is developing that that email so that it can be copy and pasted. So that's not really a great mechanism anymore in order to detect this stuff. However, there's other things that, you know, our front lines, or our users can be doing, such as scrutinizing the actual email domains that will be coming in. And so there's ways in which, you know, a user can look at that and look for common misspellings because that's one of the things that we see is adversaries will create doppelganger domains that look very, very similar to the legitimate domain. But it might be off a letter or an "l" might be replaced with a "1"; being trained to be able to detect that type of thing is extremely important. And we need to ensure that our users are capable of doing that type of analysis to scrutinize inbound types of things. The other thing that we're seeing as well, especially in the vishing world, is the introduction of artificial intelligence and deep fakes with voice communication. So some things that you can expect to see in the years to come is using artificial intelligence to make a voice be what you would expect it to be. And so that can be tied into CEO fraud and otherwise, not something that's being... we're seeing a lot of. But it is something that we are seeing a lot of chatter about, and the concern of using AI and that type of thing. Again, how do you how do you detect that or how do you for that sort of type of attack? Going back to the basics and having some sort of a key passphrase that only you and the other party know. So, for instance, Kevin, if you and I, you know, you're a financial institution, maybe I'm a manufacturer, I'm going to, you know, I produce product or whatever, and you call me and you tell me that something's going on or whatever. Maybe I would say I would need to just verify the key phrase to ensure that I'm talking to somebody that I trust. If they can't provide that information, you're a... red flag should probably go up, you know, and then you should probably be reaching out directly to your financial institution with a trusted number that you have. Maybe it's an account rep number that you know, or something like that to just say, hey, I have this interaction. I just want to make sure everything is okay. What steps do I need to take going forward, that type of thing. Another type of

[Kevin]: So. Go ahead.

[Kyle]: Another type of red flag that I would say is just unexpected calls. And I mentioned this a couple of times, especially as it relates to emergencies or urgency or getting you to do something, especially as it relates to some kind of financial transaction. Make sure that you're asking the right questions, and be skeptical. Don't trust and then verify. Verify everything, in my opinion. So that's definitely something that I would do, especially if you're kind of on the receiving end of these types of inquiries or requests.

[Kevin]: So circling back now, that's very helpful, Kyle. And I just want to circle back for our audience. So if you're thinking you get a call from your financial institution and they tell you there's fraud on your account. What we're saying is, if there isn't a passphrase in effect, as you said, you say, well, I would just need to verify the passphrase, which, by the way, those of you thinking, well, they could hack in and get the passphrase, too. We're thinking of a passphrase that is sent to you like your four-digit PIN. It's sent to you by mail. So the threat actor should not be able to access this passphrase. If they don't know the passphrase, then you know there's a risk of fraud. If you don't have a passphrase and you get a call from your financial institution telling you there's been fraud, what I would say, Kyle, is I would hang up and I would say, thank you very much. I'm going to call back on the designated fraud line. And call your institution back on that trusted number. And they will tell you whether there's been fraud on your account and they will be able to help you if there has been. Does that make sense? The extra—I'm thinking the extra two minutes it takes you to hang up and call the trusted fraud line of your financial institution is not going to make a huge difference if it's actual fraud, but it will make an immeasurable difference if it is.

[Kyle]: 100%. In fact, even if it is legit, the inbound communication to you, the folks that are on the telephone will encourage you and be like "totally understand." They're not going to try to keep you on the telephone or anything like that. They know that people are skeptical of these types of frauds and campaigns and they're totally understanding when you say that you're going to be hanging up in contacting the bank directly through a number that you know and you trust.

[Kevin]: Right. And I think with the CEO example and we're familiar with an instance of someone in the United States getting a video call from the CEO who is supposedly in a foreign country saying, hey, you need to send me... you need to wire this amount to this potential new client right away. And the recommendation from here and, Kyle, let me know what you think. The recommendation here is to say, okay, thank you very much. End that call as soon as possible and call the CEO on a trusted number. And chances are and forgive me [coughs] still getting over that cold, sorry, folks. The CEO is not going to be upset with you if you call back to verify a significant transaction. But the CEO might get upset with you if you don't and that money ends up getting wired to a threat actor.

[Kyle]: Yeah, exactly right. Exactly right.

[Kevin]: So very helpful, Kyle. Thank you. These are some of the red flags that we can all watch out for. But in our remaining time, let's cut right to the chase and what you do. Let's suppose that they're... for whatever reason, it's a very difficult attack to spot and you get a call from a client or from me saying that one of my clients has suffered a funds transfer fraud, and we're bringing Avalon Cyber in as the forensic investigator, what are the first things that you will need to do, that the client will need to do once the transfer fraud has been discovered?

[Kyle]: Yep. Yeah. So a lot of times what we recommend and what we see a lot of our clients do is they'll go through and they'll update credentials and making sure that the threat actor no longer has access. If it was a business email type compromise. Even with, you know, maybe, maybe your web content, maybe your web portal credentials for your financial institution were impacted as well—making sure those credentials, anything tied to whatever the target was of the adversary, would be definitely a great step in the right direction. And then, you know, in parallel to that, I would say is notifying your bank. Getting somebody on the phone from your bank, whether it's a relationship partner, you know, or whomever that you have access to, that's a direct relationship to make sure that it's on their radar, that this has transpired. And they'll request some specific information relating to the activity so that they can start doing their investigation and then shortly followed by that, my recommendation would be to contact your attorney if other folks are involved. And so if we're talking about maybe a vendor that maybe… that you work with, or maybe it's a customer where the adversary maybe sent them a fake invoice and said, hey, pay this invoice, but use this new bank account information. Now your client might be a victim of this campaign as well. So having an attorney involved is going to be important for purposes of ensuring that all of the risk is being managed. And those types of conversations can be had between all affected parties. Once that's been done, you know, contacting your insurance carrier or your broker, etc., and to ensure that you have the coverage, to any extent there may be a claim that will need to be made. You definitely want to make sure that you're making those claims early in the process. You don't want to go through the investigation and then later submit a claim to only find out that your claim is denied because you didn't follow the process outlined within your contract that says that you need to notify your insurance carrier immediately that you've had some sort of a cyber incident. So getting those folks on the phone and getting that claim submitted is definitely going to be an important part. With that your attorney should be able to manage that risk management process with you. And then from there, it's, you know, determining whether or not you need to engage forensic experts. There may be specific facts of the case or the matter that would require elevated technical investigative experience. And so you would bring those folks in at the appropriate time and then in consultation with everybody—that would be your attorney, maybe a forensic expert, ownership or senior management within the company, making a logical decision as to whether or not you want to file or pore through IC3 [Note: Internet Crime Complaint Center], which is hosted by the FBI and the IC3 form itself. It's a pretty straightforward process. It asks you very specific details and informations about your about the cyber incident itself. It asks you about any sort of financial loss that may have been incurred and all of that great stuff. And then once that's submitted, that gets pushed out to all the local field offices for the FBI, Secret Service and the like. And those folks will obviously they monitor that on a regular basis. And they do reach out and they do ask you for more specific information. And they may even be able to assist from an investigation standpoint and potentially even recouping some of the funds that were lost as part of this fund transfer fraud scheme. If you get to them quick enough… and like the Secret Service, for instance, has a lot of capabilities as it relates to transactions conducted over the SWIFT Network, you know, they might be able to actually retrieve the funds for you so that you're made whole. And in other cases you might just get a portion of it. But obviously time is of the essence in order to make sure that that happens effectively.

[Kevin]: Yeah.

[Kyle]: And then finally determining exposure. And that's usually done through the attorneys, because obviously you want to get notification out, but you want to make sure that's done, you know, with the attorneys buy-in and support and guidance on that as well. So it's a technical challenge in some respects, but there's a lot of legal elements to this that you want to make sure that you're making the appropriate decisions. And you are you are responding accordingly.

[Kevin]: Yeah. Thank you, Kyle. That is very thorough. And I just want to underscore a couple of points that you made. First, with regard to insurance, you… and I guess just a global comment, everything that you're saying right now, Kyle, you laid it out over a few minutes. Those are all steps that should be taken simultaneously within hours after learning of the fraud. The sooner you act, the more likely it is that the money fraudulently transferred can be clawed back. Contacting your insurance company is critical because you ensure that if you have coverage—and you should have coverage for legal fees and forensic fees—that the carrier is on board and will reimburse you from day one. Cause the longer it takes you to notify your carrier, the bigger the gap there might be from day one in the date of notice. And during that period, in all likelihood, you won't recover your attorney's fees, your forensic costs. Secondly, I wanted to touch on the IC3 reporting, Kyle, because I think you make an excellent point. We had a scenario recently where one of our clients was fraudulently induced to provide information that led to the transfer of a very significant sum of money. The client called us the evening of the day that the fraud happened; it was within a few hours. First thing we said was, you need to go on IC3.gov and report this to the FBI. The FBI responded within 12 hours and while it's true that the FBI is very busy, this fraud happens all the time and they can't get to everything. If the amount of the loss is high enough and the reporting is fast enough, the FBI can either execute a kill chain if it's a transfer to a foreign account, or it can get to the recipient bank and cut off the transfer before the money goes from the recipient bank to the threat actor's account. So it's critical to act as quickly as possible in that scenario. Kyle, the more I see this, the more I think that it's very difficult to stop. It's very difficult to get the money back, and one of your best chances of getting it back is reporting immediately to the FBI so that they can work their magic and try to get that money back before it goes to the threat actor's crypto account or wherever it's going to go overseas.

[Kyle]: Mm-hm. Yeah, exactly. And the other thing to not only the mechanisms they have through like FinCEN [Note: U.S. Treasury Department's Financial Crimes Enforcement Network], you mentioned, like the kill chain in their, in their legal capabilities through FinCEN itself. But they also have really great relationships within major financial institutions.

[Kevin]: Yes.

[Kyle]: So your contact directly to your bank, you might be getting to a relationship manager and you might be bouncing around with, you know, lower level analysts that are kind of dealing with hundreds of these things a day. They usually have access much higher up the chain that can get more attention and allow them to provide you with additional resources and capabilities even within your own financial institution. So there is definitely benefits for engaging law enforcement at the appropriate time. But again, you know, I think those are things that have to be weighed out with counsel to ensure that, you know, it's in the best interests of everybody to file that report.

[Kevin]: Right. There are so many other things we could talk about, the talk of there are insurance coverage issues that come up, there are issues between crime policies and cyber policies. And as you alluded to, there's the negotiating process. If you've been fraudulently induced to transfer money, that should have gone to your vendor or payment to the threat actor, the vendor is going to be coming after you saying, well, I didn't get your payment. And then sometimes it works in reverse where the vendor is supposed to be paying you, but the threat actor diverts that payment. You could be owed money, you could owe money. I think your point is the best contact…involve your lawyer as quickly as possible because we can help evaluate those issues. But that might be fruit for another podcast episode. Kyle, I think we should come back and talk about that. It is a complicated process, but funds transfer fraud is a real thing. I read somewhere that last year alone the average loss was nearly $400,000. We know the frequency of the attacks is going up. We know the amount of the losses are going up. And this is something that I think if you're in the audience and it hasn't happened to you, you need to be thinking very, very carefully about putting the right controls in place. And maybe this is a good place to leave it, Kyle. Having the right training, is there training available out there that business owners can purchase to train their employees up to know what to look for in these types of attacks so that they're less likely to fall prey to them?

[Kyle]: Yeah. So a couple of things just on training, you know, your traditional security awareness platform training, there's a lot of them out there today. They still add a lot of value. The good ones are constantly enhancing their content so that the employees within your company are getting the most up-to-date information. The tactics and techniques that are being used by adversaries. It's still a very valid thing to do and you definitely want to keep doing it. However, one thing that I will say is there has to be internal education as it relates to process and procedure, specifically relating to financial transactions and making sure that you have checks and balances kind of built in. You understand the "know your customer" principles and evaluate that and ensure that those principles are included in the processes that you have. So it's not just about detecting these types of frauds. We know that these frauds are going to continue to happen. It's about your internal processes and ensuring that those processes would be able to flush out some of the things that we're talking about here today. Because if you build in enough layers, and enough checks and balances within that process, you're going to have a better chance of thwarting these types of attacks, even if they're successful in duping somebody to give up a piece of information. Or maybe there's been a business email compromise or something like that, like no change can happen until, you know, these four or five things happen. It may slow down the process for the organization...

[Kevin]: ...a little bit ...

[Kyle]: ...but from my perspective, you have to kind of weigh the risk with the reward. What are we willing to accept as a risk to ensure that we have some sort of security discipline here to prevent these types of things? And that's a conversation that's going to be had with, you know, ownership, senior leadership, finance teams, vendors, customers, etc... It has to be something that not only starts within your organization, but it trickles out across all of your third parties, whether they're customers or vendors.

[Kevin]: Right. And it's the responsibility of the individual organization and the outside actors, the banks, the financial institutions have to have the right protocols in place. But I'm sitting here thinking, Kyle, if the only thing we taught our employees was to independently verify every one of these communications using a trusted email address or a trusted telephone number, we could probably prevent all but a very few of these attacks.

[Kyle]: Yeah. No, I agree with you 100%. And that's why I said, like, the traditional security awareness training is a good start, but it's the internal process.

[Kevin]: Yeah.

[Kyle]: Education, internally, education externally. About that process is going to be the... is going to be the most effective way of dealing with this sort of threat vector. So definitely making note of ...when you're going into, you know, the 2024 period, you know, making sure that your leadership team is aware of this risk and understanding what exists currently to be able to detect it. If nothing exists and it's time to start investigating, how do we improve that process overall? You know, so

[Kevin]: Hear, hear. Well, on that note, I know we are out of time, but I want to thank you, Kyle, for coming back. We always love having you on. This is a really important topic and I'm glad it was you that came on to talk to us about it.

[Kyle]: Well, thanks, Kevin. I appreciate you having me back. And it was a real pleasure to have this conversation.

[Kevin]: It is my pleasure. Will you come back again soon?

[Kyle]: 100%.

[Kevin]: All right. Thank you so much. We enjoyed having you on. And thanks to all of you out there for joining us for this episode of Cyber Sip. We're back soon with another episode.

[Kevin]: The *Cyber Sip* podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share, and continue to listen.