**_CONSUMER FINANCE PODCAST_: WHAT TO DO WHEN A PHISHING ATTACK HAPPENS TO YOU**
**HOST: CHRIS WILLIS**
**GUESTS: SADIA MIRZA AND KAMRAN SALOUR**
**POSTED: DECEMBER 15, 2022**

**Chris Willis:**

Welcome to the *Consumer Finance Podcast*. I'm Chris Willis, the co-leader of Troutman Pepper's Consumer Financial Services regulatory practice, and I'd like to welcome you to our episode today which is going to be all about how to prevent and deal with phishing attacks when they happen to you. But before we jump into that topic, let me remind you to visit and subscribe to our blog at consumerfinancialserviceslawmonitor.com, where you're going to see daily updates on everything that happens in the consumer finance industry. And while you're at it, check out our other podcasts. We have lots of them. We have *FCRA Focus* all about credit reporting, *The Crypto Exchange* which is of course about all things crypto, and *Unauthorized Access*, our privacy and data security podcast and which has a special connection with my guests on the show today. And if you like our podcast, leave us a review on your podcast platform of choice and let us know how we're doing.

Now, as I said, we're going to be talking about phishing today, and it gives me the opportunity not only to talk to you about that very important subject, but also to introduce you to two of my colleagues and one of the great capabilities that we have here at Troutman Pepper. My guests today are Sadia Mirza and Kamran Salour who are my colleagues who are members of our privacy and cyber group, and they have the distinction of leading our incident response team, which deals with hacking and phishing and other cyber-attacks. And so, I'd like to welcome the two of them to our podcast today. Sadia, Kamran, welcome to the podcast.

**Kamran Salour:**

Thank you, Chris. We are very excited to join you and very excited to talk about phishing, which is a topic that is near and dear to our collective hearts.

**Chris Willis:**

And the two of you are professional podcasters too, because as I mentioned, the two of you are the ones who are responsible for *Unauthorized Access*, which is our terrific privacy and data security podcast, right?

**Kamran Salour:**

You are correct, Chris. I have bias when I say *Unauthorized Access* is a terrific podcast where Sadia and I talk about all things cybersecurity, but we are of course very excited to be on the *Consumer Finance Podcast* as well. And we've heard nothing but great things about your podcast of course.

**Chris Willis:**

Well, let's get right into it. Obviously, phishing has become a major security risk for all kinds of companies and of course, especially for financial services companies. And just to give a little bit of background, phishing is what we have these constant exercises with our IT department with, and I'm sure our listeners do too, where an outsider will send an email to someone pretending to be someone they aren't. A client, a vendor, a regulator, somebody like that, and they'll try to

extract information from the recipient of the email that will permit them access to some of the target company's systems like give me your password or give me this, that, or the other. And it's become an increasingly common sort of threat vector for cyber-attacks on companies including financial institutions. So that's what we're going to be talking about today. Kamran, why don't you start us off, I guess probably to understand how to deal with phishing attacks? Let me ask you first, what is the threat actor's motive when they're pursuing a phishing attack. When they send me these ridiculous emails that I hopefully never respond to, what are they trying to accomplish?

**Kamran Salour:**

It's an excellent question, Chris. I hate to give the traditional legal answer, which is it depends. But when we're talking about a threat actor's motives, especially in the context of phishing, it really does depend. Now, typically when we're talking about phishing, the threat actor has either a financial motive where they're trying to extract money from the organization and they'll typically do that through a fraudulent wire transfer scenario, which we can talk about in more detail. But essentially what the threat actor will do is infiltrate one side of the email exchange and basically tell the company that owes money, hey, we've changed our banking information. Here's some new wire instructions, send the money to us. Of course, the new wire instruction bank is the threat actor's bank, and the money goes to the threat actor. That's typical pattern when we're talking about a financial motivation if I'm a threat actor.

Sometimes a threat actor is interested in just a phishing exercise or more of a phishing campaign. They want to continue trying to get people to click on links and getting user credentials from other individuals. So sometimes a phishing link will just have an ability for the unsuspected individual that clicks on the link to input their username and password, which now the threat actor will use down the road for some other sort of phishing campaign. I would say in my experience, those are the two main categories, the financial motive and also the phishing campaign motive. But I don't know, Sadia, you may have a different view than I have.

**Sadia Mirza:**

No, I completely agree. I think one of the main motives is to lure potential victims into taking some kind of harmful action. Kamran, you kind of mentioned once you get valid credentials, basically infiltrating deeper into the system and causing possibly more significant harm. And I think the one thing to keep in mind with these, when a threat actor is able to get an individual to hand over valid credentials and now, they're in your system using valid credentials, it's hard to spot the threat actor in your system, right? Because they're just operating under the guise of valid credentials, so you just think it's a valid employee that's within the system. To me, I think one of the things we've seen a lot this year is phishing attacks being used to really gain a foothold on the company's network using those credentials and then exploiting it further to cause other type of harm.

**Chris Willis:**

Well, and it seems to me too that for financial institutions, they really have to be concerned about phishing at two levels. On one hand, they may be the subject of phishing attacks themselves directly, which is probably mostly what we'll talk about today, but I think there's probably also a significant threat of the customers being the subject of phishing attacks and then someone basically using that for account takeover purposes. Not harming the institution directly but harming the customer through phishing attacks. Do we see much incidents of that?

**Sadia Mirza:**

Chris, you did your homework coming off of this podcast. Account takeovers, yeah, we see a lot of these type of B2B wire fraud type incidents in what you're describing, and we see it a lot in business email compromise scam, or let's say a threat actor is able to get into the email account of one of your vendors, they basically take over that account. They take over that email and they might send your organization new wire instructions for example, right? And it's tough for humans. They're interacting with someone that they've interacted with before. It's a vendor that they've worked for from the same email address. So, it's tough for humans to be able to catch. Maybe it's just the tone that has changed slightly or maybe it's a spelling issue, but it's tough to catch those types of changes and that's what makes phishing, even though it's the oldest trick in the playbook at this point, but what makes it so successful and why threat actors continue to use it.

**Chris Willis:**

What are some of the things that organizations can do to try to prevent these phishing attacks from being successful, from allowing the threat actor to gain access to the system or cause some other harmful effect?

**Kamran Salour:**

Chris, I think there's a number of things that can be done, and I think what you do or what combination of these things you employ is going to depend in part on the size of your organization, the type of industry that you're in, as well as the sophistication of the companies and vendors and third parties that you deal with. But I think phishing training is something that if used effectively can be very helpful because it gives the email user just an opportunity to get a sense of what types of emails a would-be threat actor would send, but it also gives the individuals an opportunity to test what they learn about how to identify a suspicious email by looking at the sender's address, looking at the headers, looking at some of the content within that email.

For instance, if it's an email purporting to be from the company's CEO but your company has an external email warning on all external emails and that same email that's supposed to be from the CEO says external email, that's a telltale sign that, hey, this is something fishy about this email and let me think twice about it. So, I think if you have appropriate phishing training, that is helpful. If you just have phishing training where nobody reports the results of the training, nobody tells you after the fact here are some telltale signs of why this was a phishing email, ways that you can actually improve your phishing acumen, if your phishing training doesn't have that, then it becomes not a very effective exercise. In fact, it could almost be counterproductive because now people, whenever they get a supposed phishing email, they're less inclined to be vigilant and they're much more likely to click on a link.

I think the other area where training is important and can be effective is with password management. One of the things that these phishing campaigns kind of hang their hats on is, look, if you click on a link and you provide us your username and password, well you may use that same password for a number of other of your accounts. And so now the threat actor has a password, which if it's only good for one account, the threat actor's ability to gain unauthorized access is limited to that one account. But now if I use the same account for work and I use the same password for my personal banking account and I use the same password for some other accounts that the company holds, well now the threat actor has a lot more access to the environment based on just getting that one compromised password.

So, password management is critical. Part of that password management is really not reusing the same passwords and certainly not reusing the same passwords for business purposes, right? You don't want to have the same password be used for multiple accounts within the business because that way the threat actor can get much more access.

**Chris Willis:**

So, you're saying password123 is probably not one that I should repeat in all of my accounts? I'm just asking for a friend.

**Kamran Salour:**

Yeah. Password123, all lowercase too especially is something that you don't want. And I know you're saying it somewhat tongue in cheek, but I've hit a ransomware not too long ago where the admin accounts were admin1, admin2, admin3, admin4, and guess what happened? The threat actor got one password and then realized, oh, well admin1's not going to work, let me try admin2, three, and four, and then got access to various different parts of the environment. So, you always want to balance security and practicality, and you don't want a situation where you have 30-character long passwords that you have to change every week because then it just becomes overwhelming and cumbersome and the likelihood of reusing it is very high. But if you can build it within your password policies, and a lot of organizations have this where you can't reuse the same password within the last, let's say six months or the last six passwords has to be different, that's something that's definitely helpful.

Having long passwords, 12 to 18 characters is definitely helpful as well because it makes it much harder for the threat actor to guess. But certainly, password management is definitely one way to help reduce the scope of the phishing attack once it happens. And I think another piece that's very helpful is an easy way to report suspected phishing emails, right? It goes to that old adage, if you see something, say something. And so, you may get an email and it looks suspicious, and some organizations have a phishing link or a button that you can hit that will send that email to the IT team. The IT team can investigate and if they see that yes, this is in fact a phishing email, they can send a companywide email saying, hey everybody, don't click on this.

I can't tell you how many companies that we have helped, Chris, where they didn't have a feature like that. And so, what happened was the first few people that got the phishing email didn't click on it, but word didn't get around and the 10th person clicked on it and then the threat actor was successful. I think it's important to have safety in numbers and a community of being vigilant against these phishing emails. A very effective way of doing that is having an easy way to report this to your IT and the IT can then spread the word.

**Chris Willis:**

Yeah, I had a personal experience with that recently. We actually had a phishing test in our firm and I forwarded the suspected phishing email to our director of information security and he sent me back a nice gold star for having spotted it.

**Kamran Salour:**

Oh, see, very nice. I didn't know that they would actually reward us with praise, so I will start to do that from now on. I just stop at ignoring it, but I'm going to start to do that.

**Chris Willis:**

Send it to him. He likes to give those gold stars out.

**Kamran Salour:**

Sadia knows how much I love praise, so I will definitely do that.

**Sadia Mirza:**

Kamran, you're on the list to repeat the phishing training at the firm.

**Kamran Salour:**

Is that right?

**Sadia Mirza:**

We'll talk about that later.

**Chris Willis:**

So, speaking about phishing training, what are some things that businesses should be thinking about when they implement that training? You've given a couple of tips already, but is there anything else to add?

**Sadia Mirza:**

The conversation we just had about password management and phishing training, that's interesting to me because I think that businesses should keep in mind that there's not going to be a single control or safeguard that businesses should rely on as the last line of defense, right? None of these things are solutions in and of themselves. It's a combination of tools and technology, policies and procedures that are all aimed at securing the organization and detecting and preventing threats. And so, you can't rely on... Enabling employees to identify phishing attacks is important, but again, it's not a solution in and of itself. So, you have to have other, I don't want to call them compensating controls, the other controls in place to reinforce the phishing training and the other policies and procedures that exist.

The other thing that I think coming out of phishing training that is incredibly important, it's something we talk about when we talk about tabletop exercises as well, and the question is why do we do them? One of the benefits that comes out of these phishing trainings is creating this culture of cybersecurity in the organization, because I think sometimes companies operate with this impression that cybersecurity is just the security team's problem, and the truth is it's not, right? It's everybody's problem. And when you start doing things like tabletop exercises where you're testing your incident response plan, or even simple phishing training exercises, you make employees realize that security is their concern as well and they have a role in protecting the organization.

**Chris Willis:**

Yeah, that makes sense. Let's though shift the podcast into a little bit darker place and let me ask the two of you this. Let's say despite best efforts a business does fall victim to a phishing attack and an employee clicks on the link or provides credentials or whatever. What does the response plan look like for a business that's been the subject of a successful phishing attack?

**Kamran Salour:**

This goes back to the answer I gave you on the first question, Chris, which is, “It depends.” And here's what it's going to depend upon is the type of business, the type of customers that you have and the individual who was victim of the phish. What do I mean by all that? Well, one is let's say you were the victim of a phishing scam. You clicked on an email and as a result, the threat actor is in your inbox. The threat actor is sending out emails to all of your contacts which is a common tactic that the threat actor will use as part of that phishing credential campaign. You can then get an email from a colleague that says, hey, I got this email from you. Is this legitimate? Now you're on alert that, okay, I have in fact been phished and somebody's sending out emails.

You definitely want to preserve that phishing email first and foremost. You want to have your internal IT team take a look at it and depending on what your role is in the organization and to whom this email went out to, I typically recommend that you want to, as a first instance, send out an email basically letting everybody know that, hey, there was an email that went out, it's not from me, don't click on it. Because you want to limit the scope of the phishing attack itself. Then at that point, depending on your job responsibilities, if you're involved in accounting, I would definitely take a look at to whom that email was sent. If that phishing email was sent and it goes to, let's say a third-party changing wire instructions, well now you have some definite action plans that you have to take into place.

You also want to check to see on that email inbox, was the threat actor actually in your inbox or was the threat actor spoofing your email domain? You can check by looking at the actual spoofed email or the phishing email itself, but you also want to check that inbox to see if there's any rules that are unauthorized, any rules set up, trying to send emails out unbeknownst to you and then hiding those emails let's say in your RSS feed. There's a lot of different things that go into play, but a lot of it really just depends on the context of the phishing campaign.

And so probably the most brief and probably most effective answer to your question is if an organization falls victim to a phishing attack, they should consult someone like Sadia or myself in terms of contacting outside counsel that deals with incident response work all the time and we can go through all of these different steps and then from that point we can decide, does it make sense to bring in a third party to conduct a forensic investigation? Do we need to have counsel involved to help resolve a fraudulent wire transfer dispute? All these little different things that come into play. But I think the easiest approach is to contact somebody outside of the organization and then listen to them and follow their advice.

**Chris Willis:**

And I suppose at the risk of being captain obvious here, when one of these incidents has happened, I assume that time is of the essence in terms of contacting outside help to limit the scope of the harm.

**Kamran Salour:**

It is because one, you want to preserve your logs as much as possible because at that point when you've realized you're a phishing victim, you don't necessarily know A, if the threat actor was in your environment, and B, you don't know when the threat actor got into your environment. So, you definitely want to contact outside counsel immediately because they can help preserve all of these logs. But you also, if we're talking about potential money being transferred to the wrong person, usually with the FBI and the Secret Service, they have good

luck clawing back money if it's within that first 48/72-hour window. And so that's really the critical aspect of timing.

Unfortunately, what typically happens in these types of scenarios is you don't realize that you were the victim of a phishing email until two weeks after where somebody says, hey, I thought you were going to send that money to us, where is it? And then your response is, hey, I sent the money. And then you go back and you look at your emails and you realize, oh, we sent the money to this banking account, and the person's saying, well, that's not our banking account. So, it's typically too late in that process, but if you're able to catch it right away, definitely call somebody right away because we can put you in touch with the appropriate people from an FBI standpoint to try to claw that back within that 48/72-hour window.

**Chris Willis:**

Sounds like great advice. Sadia, any parting comments by you?

**Sadia Mirza:**

The only thing I think I would add to that is if you're a business that has cyber insurance, if you suspect a security incident, contact your carrier, contact your broker. They have professionals that are on standby ready to help you. They work with outside council; they work with forensic firms who can get on calls with you quickly to help determine next steps. Hopefully, Troutman is on that outside council panel. If not, tell your carrier you want Troutman on that panel. This is definitely something businesses do not realize. They pay for cyber insurance, and they do not realize that they have the resources available to them. A lot of times we've gotten on calls with forensic firms, the forensic firm won't even charge initially, it's just to hear what's going on. They can tell you whether or not you need forensics, whether or not it's pruning to do it or not. But it's nice to hear directly from an expert so at least you've checked that box. Definitely leverage your cyber insurance and pulling the resources that are already available to you.

**Chris Willis:**

That makes great sense. So, Sadia and Kamran, thank you very much for being on today's podcast and sharing your insight into this issue, but also giving me the opportunity to showcase to our audience what an incredible privacy and cyber and incident response capability we have here at Troutman Pepper. And of course, thank you to our audience for tuning in to today's episode as well. Don't forget to visit our blog, consumerfinancialserviceslawmonitor.com and hit that subscribe button so that you can get all of our daily alerts on what's going on in the consumer financial services world. And while you're at it, go over to troutman.com and add yourself to our Consumer Financial Services email list so that you get notice of our webinars and our alerts. And of course, stay tuned for a great episode of this podcast every Thursday afternoon. Thank you all for listening.