Podcast Transcript: Cyber Security: What is a Scam?

Cärin Viertel:

Hello, I am Cärin Viertel, the Director of Client Services at JNBA Financial Advisors based in Minneapolis, Minnesota. Thanks for joining us for this podcast from the JNBA Studio.

Today we're talking about cyber scams in an effort to help prevent more people from becoming victims of these crimes. So much of our life is handled online today from how we shop to groceries, to clothing, to how we communicate with our loved ones and friends, and to do business affairs via email and/or text. And with an app or a website, you can easily make a deposit or transfer money. And all of these things, no doubt, have made our lives more convenient. But with the rapid changing landscape of technology, it also can be confusing and I think it also opens the door to expose even the savviest people to the risk of cyber scams.

Joining me today are two experts on cybersecurity, Brent Morris, and Brandon Nohr from Success Computer Consulting, an IT firm and trusted business partner of JNBA Financial Advisors.

Brandon, okay, you are truly the expert in this and we're grateful you're here today to share what you know about cyber scams. And there are unfortunately many, many different types of scams out there, and these scammers seem to be getting better and better and getting access or finding new ways to get at us and disrupt our lives with access to our personal information. So if we take a step back and just kind of big picture, tell us what are scams in general, what's going on?

Brandon Nohr:

So when you think about an attacker and what they're trying to go after, it's money, access, those types of things. And who's doing this is generally organized crime. Sometimes nation states, but usually organized crime. So think mob, think the gangsters, they're no longer running the streets anymore, that's more around the cyber crime. And a lot of what they're trying to do is what we call social engineering. So they try to trick you into do something, to give up money or to give up accounts or give up access to something. And those can come in through anything from a phone call an email, a link. And a lot of times they're just trying to get you to click on something or get access to something and the time they're in we call this dwell time. So sometimes they might come in and do something right away. Other times they might sit there and see what they have access to. So if you click on a link and they get access to your computer or your phone, they might just watch for a while and the time they're in there before they make themselves know and we call that dwell time. So those are some of the attacks and at least some of the reasons or how they're approaching it.

Brent Morris:

Brandon, thanks for sharing that. The scams have gotten way more sophisticated than what they used to be when we'd receive emails from the Nigerian Prince or some lawyer from some other continent that says, I've been given access to millions of dollars. What are the scams like these days and how much more sophisticated have they gotten?

Brandon Nohr:

Well, what's interesting is some of those scams still exist, and the reason those kind of work is they're almost litmus tests. If you respond to something like that, they probably found an

unsophisticated user. And so those stunts still happen, but they are getting more sophisticated. They're going after more sophisticated users after bigger dollars and things like that. So it's really around, the term in the industry's OSINT or open source intelligence, they really start to try to understand their attacker and go after them, especially the bigger dollar ones. It takes time and energy, and there's usually teams of people coming after. I always equate this to it's not the hooded mystery figure in their mom's basement going after it is organized crime. So they are getting sophisticated. There's people that are really good at crafting emails. There's people that are really good at finding data on people. Think of a business, you have different people in your organization that are good at certain things, and that's kind of how they're organized.

Brent Morris:

And I've kind of cut my teeth in sales and marketing. And so a lot of what I try to do is script what we want our salespeople to do. And what we're seeing in these sophisticated businesses is that they're scripting exactly what to say and exactly who to say it to and they're passing things off as though they are operating a legitimate business. And in many ways they act like legitimate businesses, right?

Brandon Nohr:

Exactly. So think about marketing. We have ideal client profiles. We understand who our clients are, we understand their needs, we understand what they're willing to buy and how we engage with them. These attackers start to understand that too. They understand the people they're going after. They understand if they're going after a corporation. They understand if they're going after a CFO. They understand if they're going after someone who's retired and maybe not as sophisticated with certain technology. So they understand this stuff. They really kind of tailor the story, they tailor the attack around that.

Cärin Viertel:

They know their audience, unfortunately, and it is an industry to the point earlier, it's an organized effort to pull off these scams. And I think, Brandon, you were sharing earlier, do you remember a stat you shared about GDP?

Brent Morris:

Yeah cyber crime, if compared to a nation would have the third-largest GDP behind the United States and China, that's how big this cyber crime thing is. And so when we use the word sophistication, we're talking about it in the context of bad actors who have grown businesses around the legality of stealing, and they prey on those of us that aren't as sophisticated. So they hope to find people that might be tricked easily. And when we say tricked easily, we mean they're using tactics that trick the best of us, the smartest people have been captured or have been stolen from. And so the thing that we try to convey to people is, no, you're not dumb. No, you're not wrong. No, you're not bad. You got tricked and now we got to figure out what to do about it.

Cärin Viertel:

Yeah, I did see on the FBI shared that the former director of the FBI and CIA, they had a public service announcement that he himself had been a target of cyber scam. So I mean, it unfortunately does not discriminate or they do not discriminate who they're going after. So with that context, what are some of the common scams that you're hearing about or seeing about right now?

Brandon Nohr:

So there's many different, there's phone calls, emails, those types of things. There's also IRS scams where they poses you and try to get your tax returns. When we think about the social engineering where they're actually calling you or reaching out in some way, think in terms of there's a sense of urgency to it and there's a whole bunch of different scams around sense of urgency, but they're trying to make you to take action and make you feel that if you don't take action, bad things are going to happen. And these are the gambit of asking for money. Law enforcement could be after you, there's a warrant for your arrest. All the way down to kidnapping, we've kidnapped your child and the child's fine, they're at school or whatever that is, but trying to get you to take action and not think about what to do.

Brent Morris:

Yeah, it's like if there's a message that you get regardless of how it comes in and it prompts you to react emotionally, that should be a trigger that it could be something that is suspect. So whether it's love or fear, those are powerful emotions and they try to hook you in that way. And there's many different forms. It could be a romance scam. We've seen those at infinitum. There's many things that just... Like your money, we have a lot of fear and a lot of protection that we feel around our money, and they appeal to us in that way.

Cärin Viertel:

And I know malware comes in on people's computers or iPads or whatever it is, that if you don't act now, we're going to take everything off your computer, you're going to lose access or just creating, to your point, Brandon, that fear and urgency like act now and creating this strong emotional state, which gets to people.

Brandon Nohr:

And that's a big one that you just talked about, is they'll get on your computer and then say, something's wrong with your machine and if you don't let me in to fix this... And they'll even say, I'm from Microsoft or I'm from Apple, and here's what you need to do. Now I need access to your accounts because we need to be protect you. Again, that sense of urgency. Kind of take a second and think about it, is this really how they would reach out? Especially with law enforcement or IT support.

Cärin Viertel:

Right. What do you think has changed most recently with... It feels like that there is obviously an increase in cyber crime, that's one of the reasons we're talking about this today to create

awareness. What do you think has changed and just your thoughts on an increase of that kind of activity we've seen?

Brandon Nohr:

Yeah. I think the way that things have changed is the use of AI and we talk in terms of deep fakes and faking people's voices making a phone call. And it really sounds like the person on the other end because they were able to mock that up from a social media post that they spoke on. It is really the use of those types of tools that allow to amp up the sense of urgency, amp up the realism that something's really bad has happened. The AI piece has just been really huge.

Brent Morris:

The bad guys are always looking for an advantage, and to a certain extent, they pioneer new methods of which the security community has to react to. And we don't have an opportunity to react to it until it's happened. AI represents that new kind of pioneering way of gaining access to people, whether it's through faking a voice or being able to create something on the fly that might've otherwise taken somebody with design skills in the past. And it tricks us. And so the important thing is just to slow down a little bit and take a moment to consume what's happening to us and think about it in a way that gives us an opportunity to react in a more thoughtful way.

Cärin Viertel:

That's a really good point. And I think with everything that's going on to what you're talking about, Brandon, what can we share with our audience today? What can we do knowing that this is happening out there? How can we take control back? And you started talking to that a little bit.

Brandon Nohr:

Well, I'll talk a little bit. We have a mantra that we have followed for many years now is the pause, think, act. If something is coming in and it's a sense of urgency trying to get you to act quickly, just pause, take a moment, try to think about is this how this person or entity would reach out to me? And then really start to understand, it's okay if I take a minute here, the world's probably not going to end, but they really try to make it feel that way. So if you kind of just take a moment that pause, think, then act, it really will eliminate and reduce that kind of surface area, we call it surface area of attack or response that people have dramatically. And a lot of times if you just take a moment, the IRS probably isn't coming after you and asking you to go get Target gift cards.

And that's the one we kind of say, because it's kind of funny, but people fall for this. And because they're put in this state where they're really responding and oh my gosh, I don't want, don't want to go to jail. I don't want the IRS after me. But at the end of the day, if you just take a moment, ask, reach out to somebody, "Does this sound normal to you?" Those are the things you can do to kind of litmus test also that, am I going to react the right way to this?

Cärin Viertel:

Right.

Brent Morris:

Yeah. We're in a “right now society” where we have access to things today that we didn't have access to 10 or even 20 years ago. And so we tend to act faster on things than we may have otherwise in the past. And I think what Brandon is saying is, the best thing you can do to protect yourself is just slow down a little bit. And that's hard to do when you've got pressure or you're feeling this urgency from somebody on the other end of some kind of technology. But if we can slow down for just a minute and think, "Should I be receiving this? How real does this sound? What things might I be able to do to validate or verify what I'm hearing or seeing? And then who else might I be able to check on that can help me with this?" So slow down in the moment of right now, think about what's happening and get some help. And oftentimes the act part of this is, do nothing.

Cärin Viertel:

Yeah, no, that's a good point. Hang up the phone, delete the email that might be okay too in some cases.

Brent Morris:

Right. If it's truly important, they'll get back to you again. And if it's something that you feel the need to act on, some of the best advice we can give is, independent of whatever you received or whomever you're talking to, hang up, call the institution, call people, call your trusted advisors. Sometimes that's the best way to validate what's being asked of you and gives you an opportunity to lean on some trusted advisors that have a different perspective and can maybe think about it objectively.

Cärin Viertel:

Great advice. Thanks so much to both of you.

Next time on our podcast from the JNBA Studio, we'll be hearing from people who have unfortunately encountered some of these sophisticated scams we're talking about, and we're grateful they'll be willing to come on the podcast and share their story so that we can learn from it, but also so that we can feel like we aren't alone in this. Thank you Brent and Brandon for teaching us more about the ever-changing cyber scam industry. And thank you to our listeners for taking time to learn more about this and protecting yourselves from these scams. If you'd like more information, visit our website JNBA.com and click on the insights tab.

Podcast Transcript: Cyber Security: What is a Scam?

DISCLOSURE:

The previous presentation by JNBA Financial Advisors, LLC, was intended for general information purposes only. No portion of the podcast serves as the receipt of, or as a substitute for, personalized investment advice from JNBA or any other investment professional of your choosing. Different types of investments involve varying degrees of risk, and it should not be assumed that future performance of any specific investment or investment strategy, or any non-investment related or planning services, discussion or content, will be profitable, be suitable for your portfolio or individual situation, or prove successful. Neither JNBA's investment adviser registration status, nor any amount of prior experience or success, should be construed that a certain level of results or satisfaction will be achieved if JNBA is engaged, or continues to be engaged, to provide investment advisory services. JNBA is neither a law firm nor accounting firm, and no portion of its services should be construed as legal or accounting advice. No portion of the podcast or video podcast content should be construed by a client or prospective client as a guarantee that he or she will experience a certain level of results if JNBA is engaged, or continues to be engaged, to provide investment advisory services. Please Remember: If you are a JNBA client, please contact JNBA, in writing, if there are any changes in your personal and or financial situation or investment objectives for the purpose of reviewing, evaluating and or revising our previous recommendations and/or services, or if you would like to impose, add, or to modify any reasonable restrictions to our investment advisory services. Unless, and until, you notify us, in writing, to the contrary, we shall continue to provide services as we do currently. All services provided by Success Computer Consulting are separate and independent of JNBA Financial Advisors, LLC. JNBA providing a professional referral could present a conflict of interest because the professional may, on occasion, make a referral to JNBA which could result in an economic benefit despite the lack of any revenue sharing agreement in place. You are not obligated to engage the services of any such JNBA recommended professional, and the firm's Chief Compliance Officer, Kimberlee M. Brown, remains available to answer any questions that you may have. A copy of JNBA's current written disclosure Brochure discussing our advisory services and fees is available upon request or at jnba.com. Please see important disclosure information at jnba.com/disclosure.