Podcast Transcript: Cyber Security: Staying Safe Online

Cärin Viertel:

Hello, I am Cärin Viertel, 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 how to protect yourself and your private information from cyber scams. As we've learned, unfortunately, millions of people fall victim to very sophisticated cyber scams every year. We're going to hear from two cybersecurity experts about how to prevent that from happening to you, and what to do if it does.

Joining me are Brent Morris and Brandon Nohr from Success Computer Consulting, an IT firm and trusted business partner of JNBA Financial Advisors. Brent, in the previous podcast, we've talked about what scams are out there and even talked to people who have first-hand experience in encountering a scam. At the end of each episode, we've been talking about three action words that people can use to guide them when they encounter a situation that is suspect. Pause, think, act. Why is this the most important tool for a person to use?

Brent Morris:

Yeah, thanks, Carin. So, the "Pause, Think, Act" advice comes from in part just what's happening in society. We're a very right-now society, we respond quickly, we expect things quickly, and scammers prey on that. They expect they're going to catch us when we're stressed or when we're more vulnerable as a result of what's happening in our family life. And so we just want to encourage people to slow down a little bit. That's the pause part of it. So when you get something, a phone call that you weren't expecting or an email that looks a little suspect or out of the ordinary, we want you to slow down, and then we want you to think about why am I getting this? Why send it to me now? How important is this right now, or how important is it that I take this call or start this call with something that popped up on my screen?

And the act part of things, and we've said this before, sometimes acting means not doing anything. So that means slowing down and maybe giving it 24 hours. Or another best thing to do in the context of acting is to call somebody that you trust. Call a trusted advisor or your bank, call them directly, don't call the number or click the link that they want you to click. Call the actual phone number or reach out to the relationships that you have to validate what you're seeing.

Cärin Viertel:

That's really good advice. So what are some of the things that we should be cautious of today that's happening with scams?

Brandon Nohr:

So when you think about a call coming in or an email you're getting really just be cautious about what's coming in and what it's saying and what it's telling you to do. When you're coming back to that idea of the "Pause, Think, Act" number one is don't panic if something happens. Keep your head. The best thing you can do is stay focused on solving this problem, whether money's left, doesn't matter what happened, or they clicked a link and got into your system. So number one is don't panic.

Number two is really think about what did they have access to? What information did you give them? And really think about what do you need to do to start to secure that? It might be calling

your bank, it might be your credit card company, whatever that is. It might be law enforcement. If it was an IRS attack that maybe you gave up your social security and they got your IRS information, you need to call the government and start those processes. Whatever that may be is really start to think about what did they have access to? And in the corporate world, we think about containment. How do we contain this and how do we react and what are the steps to take here? And really it's just about staying calm and focusing on what do they have access to and what were your next steps?

Cärin Viertel:

That is something that we all probably have experienced, this panic of, I need to do something now, what is this? What are some key actual do's and don'ts about how to protect your information, or if you're interacting with an unsolicited request from somebody, what are some key things that our listeners can put into practice?

Brent Morris:

Yeah, I'll start with, let's take a look at emails or text messages as an example of how they most often reach out to you. Some of the things that you can do is first check the actual email address from whom you're getting the email from. Oftentimes, the domain name will not be from the actual organization that they're pretending they're trying to reach out from, or something will be misspelled, or something might be sent to you at a very odd time. I mean, if you're getting an email from somebody at 3:23 AM in the morning, and it's from a big bank, that's probably not the bank that's sending it to you. So those are some examples of things that you might want to check and see before you react to it.

Brandon Nohr:

And I'll just second that and then don't ever call the number in the email, don't click the link. Oh, if you think this is a scam, click here for more information or whatever that is. Don't follow the instructions in the email or the information. If they leave a number to, "Call us if you have questions." Don't call that number. Go to Google, find the number for the bank or the financial institution or whatever they're trying to get you to connect to. Don't rely on that information and what they've given you.

Cärin Viertel:

So go to the contact information that you've received or you've used before in essence, most likely, with your bank or advisor or whoever it is that they're trying to communicate from.

Brent Morris:

That's the best way to check is go directly to the source that you've always used to validate or verify that information. And I'm a big fan of talking to people, not the people that are reaching out to me, but the people that I trust and know. So that might be a JNBA Advisor, that might be your banker, that might be whomever is handling money for you in some way that you have trust and relationship with.

The other thing that I encourage people to look out for, they prey on our “right now-ness”, if you will. And sometimes instead of if you look at the logos that they use in emails, if you spend just a few seconds longer, it might appear to be off in some way. It could be an image that was copied as opposed to something that truly comes from a marketing department from one of those institutions. So just take another moment just to dig into these things a little bit more, to verify and validate what you're getting.

Cärin Viertel:

What about passwords? I mean, the reality is that we have lots of passwords. If we're operating our lives online, we've talked about that, right? And we have many passwords. What should we be doing with passwords or what's the best way to protect those passwords?

Brandon Nohr:

So unfortunately, your human behavior kind of works against us, right? We want it to be easy. We want it to be fast. We don't want to have to go back to the right now mentality. If I can remember it, I'm just going to enter it in. I'm going to use that everywhere. And that is a bad practice to do. Every site, every application, everything you use should have a unique password, and it should be at least 15 characters. We think in terms of past phrases. So a phrase that you like, and make it things that don't make sense.

Brent Morris loves Justin Bieber. I don't know.

Cärin Viertel:

Do you? Do you Brent?

Brent Morris:

I took my kids to a Bieber concert, I'm a fan.

Brandon Nohr:

But something that maybe doesn't go together so well, don't use common terms, don't use phrases from jingles or advertising. Those are things that can be taken and fished and brute-forced, but make it something longer and the longer the better. And length is important in this. So 15 characters is roughly what we say for passwords.

Now, usually the next question I get here is, "Brandon, that's impossible. Unique passwords every site, every application, 15 characters long. I'm not going to be able to do that." So what they come out with now is this thing called Password Manager. And this is really helpful. It's a password, and a lot of people might even be using it if you have an Apple phone or Android phone, they come with some of these password managers, it will save your passwords for you in an encrypted format and it's protected, but it's just a list of your passwords in a protected vault, they call it.

The Password Manager allows you to, one, keep the password safe, recall them, by knowing one good password, you get access to all of your passwords. And then it also helps you generate those passwords generally, there's a feature in there where you don't have to think about all these weird characters or how long it is. You can generate it there too. These are things that really help secure your environments and your life in general.

Cärin Viertel:

Okay, good advice. That's really helpful. Another thing a lot of us have been exposed to or used, two-step verification, or a two-step verification process. What's that? Share a little bit about should we be doing that? How does it work, just to help educate our listeners a bit.

Brandon Nohr:

Yeah. So yeah, multi-factor authentication, two-step authentication. This is really just what it's doing is you have a password, which is something you know, and then it asks you for something else, something you have, something you are or something else you know, whether it's a PIN code, whether it's a text that has a code in it that you put it in. The site, when you think about multi-factor, it's something you have, something you are, or something you know. And this is just another level to verify who you are versus just the password you remember.

Cärin Viertel:

Okay.

Brent Morris:

Yeah. If there's something to take away from what you're hearing, first and foremost, if your passwords are short or less than 15 characters, come up with a passphrase. That's better than what you've probably got. And we find a lot of people have really easy passwords to crack, and these aren't people sitting behind a computer trying to guess what your password is. They're running software that can test millions of characters in a very short period of time. So the longer it is, the longer it takes them to guess or crack the password. And I'm talking exponentially. So 15 characters means it's going to take years for that software to crack that password. And what Brandon just mentioned with multi-factor, it's just another layer. So passwords these days are kind of considered in the criminal world as a speed bump. Multi-factor is a wall. So you've got more steps that they have to hop through.

And the more layers you have personally for the bad guys to try to get through, the more likely they are to just pass and move on to somebody that doesn't have or hasn't listened to this kind of thing and employed some of these practices. So, what Brandon said with multi-factor, you're likely being prompted to do it by your financial institutions anyway. If you're given the choice to not do it, we want you to choose to do it. And here's another thing that I'll say, you've worked hard all your life to amass this retirement or to build towards retirement. I think we're hoping that you'll just put a little bit of work into protecting it, because the bad guys are working double time to get after it.

Cärin Viertel:

Well said, unfortunately. But that is our reality. So, this is good actionable advice that we can take. But what happens or what are one or two key steps that if you do get scammed, what should you do?

Brandon Nohr:

Yeah, so coming back to this idea of think about, pause, and think about what just happened. Did I give up an account code? Did I give up access? What was that? And step one is, secure your account, secure your environments, whatever it was, a website, your machine, but then also contact the bank. Or if you did a wire transfer, a call for that company, you can report to law enforcement. Nowadays, the law enforcement, it's not going to open a case, it's just going to file a report. And it helps understand if there's a lot of these and there's a lot of similarities to it, they can start linking it to certain gangs or organized crime. So it starts building the case. You're kind of helping that, but then secure your accounts, start changing your passwords. You can freeze your bank accounts, freeze your credit. Those are some of the initial steps to take once you've been compromised.

Brent Morris:

And I'd say talk to people. Talk to people in your network that you trust. Let somebody know who understands this a little bit more. More likely than not, somebody's already gone through this and so they know some things to do, but your trusted network will be able to help you through this. And Brandon mentioned changing passwords. I've got a neighbor of mine, mid-60s, she fell victim to this. I talked to her just the other day, and she's got two retirement accounts for which she hadn't changed her passwords yet. Now I'm pretty sure nothing happened, but that's where I got a little more prescriptive and telling her like, "Okay, we're going to change this right now. We're going to do this right now." Just because once they get in, you never know how long they've actually been in and what they've been exposed to.

And so it's important to not just take a look at the piece or the part that became victim to the scam. You need to consider the entirety of it all. And as Brandon mentioned, change passwords everywhere. You might want to, I have a little more fear about this kind of thing. I don't even want to use the same computer that may have gotten breached. I might just go out and get a new one. Now I know that's not real for everybody, but doing a complete reinstall of the operating system is sometimes what's needed to be done.

Cärin Viertel:

Okay. Well, this is helpful information, and I appreciate you helping us have this conversation to create awareness about what's happening, but most importantly, so that we can take control and we can “Pause, Think, Act”. If we become the targets of any scams out there because there is a way to help solve or mitigate some of these bad actors, we'll call them that. So thank you Brandon and Brent for sharing your expertise and insights, and thank you to our listeners for taking the time to learn more about this and protecting yourself from these scams. If you'd like more information, visit our website, jnba.com and click on the insights tab.

Podcast Transcript: Cyber Security: Staying Safe Online

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.