Barclay Damon Live Presents *Cyber Sip*™ Season 3, Episode 6: "Don't Get Hooked! Tips to Prevent Phishing Attacks," With Bill Haber

Host: **Kevin Szczepanski**, Barclay Damon

[Kevin Szczepanski]: Hey, everyone. Welcome back to *Cyber Sip*. I'm your host, Kevin Szczepanski. Today we're joined again by our favorite friend of the pod, Bill Haber of TEKRiSQ. Welcome back, Bill.

[Bill Haber]: Thanks, Kevin. Good to be here.

[Kevin]: It's great to have you. Today our episode is "Don't Get Hooked: Tips to Prevent Phishing Attacks." And for those of you that don't remember—and you should—Bill Haber is the co-founder of TEKRiSQ. TEKRiSQ is an experienced cybersecurity firm with strong domain expertise in networks, data security, software, and health tech. TEKRiSQ is business development assets will help you grow your cyber opportunities, including, right Bill, the opportunity to obtain and maintain your cyber liability insurance.

[Bill]: Absolutely. Very important part of a defense.

[Kevin]: All right. So today we're going to talk about tips to prevent phishing attacks. But I appreciate that there may still be some in our audience who aren't up on the latest and trickiest attacks. So why don't we start from the beginning. Bill, tell us, what is a phishing attack?

[Bill]: Sure. So, Kevin, phishing is a very successful technique used in the form of modern social deception, right? There have been con men around with different scams forever, and the latest of them is "phishing." It's very easy to fall for. It's essentially a fraudulent way of either sending emails or other electronic messages posing as a reputable company to hook people to give up personal information like passwords, credit card numbers, etc. And it's really, today, one of the primary mechanisms used to try to get company... to hack companies. It's very common and it's again, easy to fall for.

[Kevin]: It is very common. I think we were talking before this episode, some 74% of breaches involve the human element and phishing is still the primary means that threat actors use to hack into a system. Which tells me that it's a very successful method. Why would they keep using it if it weren't?

[Bill]: Yeah, that's right. You know, this can occur on your email, on your phone, through a number of methods and, you know, it's mostly carried out in constantly refreshed new websites or domains that are being used in the process. Today, over 60% of all the domains used in a phishing attempt are 10 minutes old or younger. So think of it as an arms race. These guys or folks who are deploying these phishing schemes are constantly setting up new domains and new infrastructures to try and catch people off guard and avoid being detected. So yeah.

[Kevin]: So the threat actors are getting better and more creative. And so we have to get better and get stronger at recognizing what these attacks look like and avoiding falling into the quicksand that can lead to a data breach or a ransomware attack, or other cyber incident. So, all right. You want to talk about some

examples. I know you have some in mind. And when I was when we were talking about some examples and you sent me some, what struck me is that we're in a new era. Yes, it's a sign of a phishing email if the language doesn't sound quite right, if it says Dear Sir/Madam instead of Dear Bill or Dear Kevin and if there are grammatical mistakes. But increasingly we're seeing better attacks where those common mistakes aren't there, it's getting harder and harder to find. Can you run us through an example or two so that our audience can appreciate how much more sophisticated these attacks are getting?

[Bill]: Sure. Yeah. I mean, not long ago, we saw a lot of those phishing messages that were improperly worded or the grammar was strange and it was easier to detect. Now they're getting very clever and using more informal terms. Oftentimes, you know, a link that you're... that people are being trained to scrutinize or recognize might be italicized or used with a Cyrillic alphabet where some letters look incredibly similar to what we use in the English language, like a standard A versus a Cyrillic A, is hard to distinguish, but people need to be aware of those things and be thinking about them before they click on links or decide something's legit. You know. And this can be very complicated because it's just as common on a mobile phone as it is on a large desktop. So, you know, your limited screen, real estate can be an issue, especially because people are often distracted when on their phone. You know, there's a number of examples that I can think of that are scenarios that happen all the time. Think about being out to dinner and you're having a cocktail with your significant other, enjoying yourself and you know, you don't want to look at the phone. So anything that might happen, you might want to, you know, minimize the time you spend on it. Maybe your spouse heads to the restroom and you check your phone and, you know, quickly click on a link to provide information that you think somebody is looking for in a flash. And unfortunately, it's a cybercriminal's email and you were just phished. So there's examples like that. And they come in different ways. You know, there are things like "smishing," which is, you know, via text message, someone masquerading as another person. And you have to be careful to look at the dialed number because people can change the numbers and names associated with an SMS. You know, there's social engineering attacks that are called "spear phishing," where the hacker has targeted information tailored specifically toward you. Maybe your company won a new client and the CEO sends you a message saying they need immediate access to your development system. And can you please click on the following links and they'll set up the rest. Maybe you, you know, feel compelled to respond to the executive. But you have to take a minute, make sure these requests are legit.

[Kevin]: Right? So you, in this era of social media and in the era in where "fast is best" or so we think, if you have you... your organization has something out there on social media about a recent employee or a recent award or a recent job that you've won, you've got to be thinking that threat actors are looking at what you post online and are going to try to use that in order to get you to click on a link, open an attachment, enter your credentials. So when you get an email or a call or a text that involves something that looks like it involves your business, you've got to stop and wait. And maybe that's our cue, Bill. Let's run through some of the... unless you have something, something else to add about different types of attacks, we can talk about those, too. We're talking about tips...

[Bill]: Yeah, I'll just mention, Kevin...

[Kevin]: Yeah.

[Bill]: One of the one of the common causes of breaches today come from "man in the middle" phishing. This is like when someone sets up an environment in a, in a Starbucks or in the lobby of a hotel and you know, maybe they've got a fake Wi-Fi hotspot, you know, 100 bucks and they can get a pineapple device to set this up and be in business. And so maybe click on, you know, free high-speed Starbucks or, you know, complimentary hotel access or whatever. And then anything that you're doing online, once you connect to the network, even with your corporate credentials for your email or your Google authenticator codes can be captured. So it's not just the method, but you have to make sure that you can entrust the networks you're connecting to. You might be just connecting to a criminal site and have no concept of that. And that's another thing that people have to be careful of...

[Kevin]: That's a great point. And I'll add one, which is, excuse me, it's that season and I wish this were Theraflu. It's only water, but I could probably use it. One of the other attacks we're seeing, it's increasingly common, is what we call "funds transfer fraud." But it's essentially an event where a threat actor will use and more often than not, phone. So this is a phone phishing attack and will impersonate or try to impersonate your lender, your bank, and either convince you or steal your login credentials to be able to transfer funds out of your business account to an account controlled by the threat actor. We're seeing that... we're seeing extensive losses arising out of fund transfer fraud. We've seen anywhere from $100,000 to over $2 million. So it happens. It happens to the best of us. And so why don't we spend our remaining time, Bill, just talking about tips for how to prevent these attacks. And the one I want to start with is one that may seem simple, but it is: slow down. Don't be sitting in that restaurant, as you mention, thinking, oh, my spouse just went to the restroom. It's time for me to quickly check my texts or emails and oh, I can respond to this one quickly. Don't do that. Take a breath. Think carefully about what you're seeing and doing.

[Bill]: Yeah, absolutely. In fact, I think "slow down" is probably one of the least addressed issues. But the urgency that a lot of these messages are sent with—the call to action. We're getting so used today to responding to things quick and trying to knock things down very quickly. And any time there's a request to provide any kind of sensitive information, people need to be suspicious of it from the get-go and have their defenses up. And what you just talked about with financial fraud, we have a client who's a great guy and otherwise pretty careful, but he connected through a man in the middle account at a hotel lobby and had a $400 K loss connecting to his cryptocurrency company because ultimately he connected through the wrong login and he wasn't using a VPN or anything. And so his credentials were discovered. Someone took that money out and when he reached out to the cryptocurrency company, they even had the audacity charge him for the transaction, kind of a kick in the backside on the way out.

[Kevin]: But no, it's true. Let me... we've got a lot to unpack there. Let's take a few minutes and do it. So you talked about slowing down and just generally slowing down and thinking carefully. If you feel if you're saying to yourself, let me quickly do this or let me rush through this so that I can get to the next task, you're probably not in the right framework to spot a phishing attack. The second one you mentioned is the sense of urgency and that is a very common means of attack. Right. And there are different types. Generally it comes in...well, let me say: generally it's a couple of different varieties of urgency. Right? It's either financial, you're going to lose money or you have an opportunity to gain money if you act quickly. Second, it might be some deadline: you're about to miss an opportunity. You've missed a deadline. You're going to lose something if you don't act quickly. And third, could be danger. Now, this goes beyond the financial vector. There are threat actors out there who are using generative AI to impersonate voices of family members. And so we're seeing attacks where you may think you're getting a call from your spouse or a child, and it sounds like that person's in danger, and you need to quickly transfer money. And we've seen this work. We've seen innocent victims transfer funds thinking that they're talking to a family member who is the victim of a crime. And it turns out the threat actor has impersonated that person. So, Bill, what are you seeing when it comes to that sense of urgency? Those are the three that I have seen most frequently over the last couple of years. But the threat actors are getting better and better, aren't they?

[Bill]: Yeah, we see that, too. And in fact, you know, there's a lot of young people that put very emotional messaging on social media and that can be used to target their grandparents for, you know, different fraudulent attacks. One that you may not have mentioned there, Kevin, is power. You know, when a message is directed from a CEO or when the message is relevant to a new customer who needs something, employees often feel like an immediacy, an urgency to respond with the right information quickly... becomes critical or you're going to upset somebody or aggravate a new client. And that's, of course, part of the "slow down." But that's, you know, kind of connected to, oh, there's more powerful forces that need me to do something right away.

[Kevin]: No, that's a great point...

[Bill]: Got to escalate the importance of proper cybersecurity procedures, because, frankly, your boss is always going to love when you slow things down. And your client will understand when you're careful with money that you exchange with them. And that's never an issue that people should be overly concerned with.

[Kevin]: No. Agreed, Bill. And that leads me to another point, another tip to prevent phishing attacks where all... you have to beware of the email from someone you don't know, that you're not expecting. So that is a very common vector of attack. If you don't know the person, if you're not expecting the email, if you don't recognize the subject matter, don't click on the link, don't open the attachment, close it, and forget about it. But there's another problem that comes, because sometimes you get an email from someone you do know or you think it's from someone you do know and your guard drops because you think that this is someone in your organization or this is a friend and you're more likely to click the link or open the attachment. And the advice I always give in that situation is all right, if I get an email from Bill Haber and he says, Kevin, I've got this great opportunity, or just click on that link and you can join my chat. I'm not going to do that. I'm not going to click on the link, I'm not going to open an attachment. But if it's from Bill Haber, I'm going to contact Bill using the contact information I had for him yesterday. In other words, I'm not going to use the contact information that's in this suspicious email. And as you said, you're not going to be upset if I call, say, hey, Bill, just got an email from you. Just want to verify that it's you who sent it to me. And you're going to say, yes, I did. That's the link. You jump on my calendar, we can make an appointment to talk about the next Cyber Sip episode. Or more likely than not, you're going to say, no, I didn't send that. And then I'm going to look at your email address and I'm going to see that instead of an Arabic A, that normal A that we use, there's a Cyrillic A in Bill Haber's email address course your email address a little different. We're not going to give it out here, but you don't have As in your email. But you get the point, folks, that your... it is going to be harder and harder to suss out suspicious email attacks. And it's critical that when you get an email—even from someone you know—you don't respond to that email. You don't contact that person using any of the information in that email. You use your own contact information to reach out. Bill, that sounds fine, but how are we going to get people to do that? Because I don't always do that. Maybe you probably always do that. I don't know many people that are that careful. How do we change the mindset that we all have that enables us to slow down and be as vigilant as we need to be in order to avoid these attacks?

[Bill]: Sure. Well, there's some things you can do. And let me get to that in just one second, because you made me think of something with your description. You know, sometimes..

[Kevin]: Oh good.

[Bill]: Sometimes people are very well trained to spot something fishy in an email. And it's always good practice to make sure that you look at the email, who it's coming from, look at any links that anyone's wanting you to click on and consider all those issues before taking action. But a new trick that a lot of people are doing is a second layer of phishing. Maybe they'll send you an email and everything looks legit and there's a link that appears proper to a document in Drive or Box or something like that. Right? And then embedded in that document will be a phishing link. So there's there can be multiple layers where the first layer gives you a false sense of security and they catch you on the second layer. So it's important to keep that top of mind. In terms of how you can protect yourself? Look, everybody should, be through their work or personally, you know, getting cybersecurity awareness, training, real basic, simple, and oftentimes entertaining training that doesn't take a huge time commitment, but particularly accompanied with phishing exercises. These are kind of preparatory educational exercises where, you know, a friendly force, someone inside the company will be trying to phish employees to help test their knowledge and to get people to, you know, report when they see them, or if they do accidentally click on them, help them to understand what went wrong. And that's a really important thing to help people do.

[Kevin]: Can I break that down, Bill, into two steps? I want to ask you first about the training source, and then I want to ask you second about something you and I have talked about, which is the quality of the phishing, the internal phishing attack. So first, if an organization wants to, they say, I really, this is a great idea, I want to

set up employee training with phishing examples, are there sources that you know that you recommend that our viewers, our listeners can go to in order to set that up for themselves?

[Bill]: Oh, yeah. There's a lot of different training companies that have different curriculum. We work with a couple of them who we find that's really good rather than to do like one cumulative hour of training once a year, rather to do, you know, 5 to 7 minutes once a month and have, you know, kind of spread-out cadence that's just part of your daily routine. But there's a lot of big names out there. You know, I'd rather not endorse one over another. But...

[Kevin]: There are many to choose from.

[Bill]: Yeah, you can do a search for "cybersecurity awareness training." And many of also often also offer phishing exercises, which is very important to include given the frequency with which people are phished. And I think it's important to make sure that when you conduct phishing exercises across your employees, to make them relevant. The idea is to try and phish the employees and, gradually get more and more successful and fewer and fewer people click on them and they learn through the exercises. But you got to make them relevant. You know, if you're sending out a phishing example, that's, you know, for a blood drive or something, no one's going to click on it because they probably wouldn't even click on a regular one. But, you know, if it's Thursday night and you're doing a DoorDash campaign, well, you might have a whole lot of people wanting to take advantage of that. And that's a great way to make sure people have their guard up. So, you know, keeping them relevant to the audience is a great idea.

[Kevin]: One of the strategies that we at Barclay Damon use internally, I should say, our IT team uses internally are phishing attacks purporting to be from the IT department. So the only advice I would give our listeners and viewers out there is: if you see something suspicious coming from, appears to come from your own IT department, don't click on it. Don't enter your login credentials, shoot your email, shoot an email to your IT department. If you're a larger organization, you may have a dedicated IT email address. If not, you know who the person is in your organization. Forward them the email you got, say hey, I just got this. Is this legit? I've done that and I will tell you that three quarters of the time it's not legit. There was one time that I sent the email back and they say, yes, Kevin this is a legitimate email and I felt a little silly about it, but you know, I think if I'm an IT person, I'd rather have a suspicious employee that doesn't click on the link than I have someone that's just clicking, clicking, clicking and rushing through the day and, and inevitably clicking on a malicious link or opening an attachment that he or she shouldn't.

[Bill]: Yeah, absolutely. And part of establishing good cyber hygiene and a proper cybersecurity culture inside a company is to eliminate the fear of reporting and make reporting something that nobody is reluctant to do. And I've seen really good companies do things like reward people with, you know, a Starbucks card or other simple incentives for reporting things or escalating things when they see something that doesn't quite look right to them. And that's really important to do. I'm glad that's going on inside of your company. You asked about some other things that companies might do, and maybe we might talk about what business owners or executives should do beyond training employees, because these things often get through even inside the best trained companies. And there's some important tools that you can deploy that are simple and don't break the bank and are good practices, especially given that so many of the folks who are phishing and smishing are setting up domains very quickly. And so, you know, obviously email filtering and spam filtering tools are great to be able to eliminate a significant percentage of those suspect emails, which is where most of them come from. I think also today, post-pandemic, we're all working from everywhere and it's difficult to secure every endpoint, but good old-fashioned VPN services that are really easy to install in your machine and you can have them always on. That's going to eliminate a lot of those "man in the middle" attacks and mask some of your credentials so that you operate much safer. There are tools that do—they're often called DNS blockers or DNS filtering—and those tools simply can be deployed by tech administrators in the company very easily to make sure those brand-new domain names, where a lot of attacks are coming through, are never allowed

through any of the company assets. So those are some real simple ways to just cut down on the traffic and complement the efforts to train the employees to do the right thing.

[Kevin]: We've covered a lot of simple steps. And to borrow from you, they are they are not "break the bank" steps, but they are steps that every organization should take. And just to close on this thought, Bill: if you are taking these steps, it's going to make it more likely that you'll be able to transfer your cyber risk through a cyber liability or cyber risk insurance policy.

[Bill]: Yeah, absolutely. Nothing looks better on an application or a risk profile that might complement an insurance application then "these are the defenses we have to be able to minimize our exposures." And if you don't have anybody helping you with those things, that can be very effective because it's increasingly necessary, whether you're applying for insurance, whether you're doing business with new companies, to make clear that you're a company with good cyber practices, taking steps to improve your cyber hygiene and developing a culture of cyber wellness. And, as we talked about, whether it's with clients or executives, there's nothing wrong with slowing down, taking time to make sure that we're not making mistakes or giving the wrong people access to the right systems.

[Kevin]: Oh, that's a great point and that's a great place to leave it. Always appreciate having you on.

Bill: Thanks, Kevin. Pleasure to be here.

[Kevin]: My pleasure to have you. Thank you so much. These are our tips to prevent phishing attacks as we get started in 2024. Thanks to Bill Haber and TEKRiSQ. And thanks to all of you. 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.