**RedZone Podcast Episode #55: Phishing Dark Waters, Social Engineering, Hacking, Human Vulnerability – with Chris Hadnagy**

\*\*\*

\*\*\*

Chris: Why did your employees click on this phishing email? Why did they answer all the questions on the phone call? Why did they not follow security policy and let someone through the door un-badged, and why do these things occur? For me, because this wasn't a natural thing, I wasn't born an SE, I had to learn these skills, I said, 'I need to understand why, because if I understand the why', this is the whole hacker mentality, 'if I understand why, if I understand how it works, and the it is the person, how the human works, how we make decisions, what controls decision making processes, then I can not only use that as a social engineer, but I can use it as an educator.

\*\*\*

Chris: There's a ton of really great, talented people in this industry. You put something in front of them and they're going to find the hole, they're going to hack it. The success ratios were super high and the failure ratios from the companies were super high. That is not an argument at all, but one of the things I saw lacking was people with the ability ... why these attacks worked.

Why did your employees click on this phishing email? Why did they answer all the questions on the phone call? Why did they not follow security policy and let someone through the door un-badged, and why do these things occur? For me, because this wasn't a natural thing, I wasn't born an SE, I had to learn these skills, I said, 'I need to understand why, because if I understand the why', this is the whole hacker mentality, 'if I understand why, if I understand how it works, and the it is the person, how the human works, how we make decisions, what controls decision making processes, then I can not only use that as a social engineer, but I can use it as an educator.'

[00:09:00]

[00:10:00] For me, for my very first book, there was a chapter in there about non-verbals, because it was something I felt very passionate about, that our non-verbal body language and facial expressions communicate so much more than our words, and that first book launched me to try to get a relationship with Dr. Paul Ekman, who's kind of the grandfather of non-verbal research, and we got him on the podcast and after that, he really ignited in me a passion for learning more and more about that, which, again, is another crazy story, because it kind of turned my whole life into an SE thing, where I sat back and I said, 'I'm going to write a book with this guy' and it took a 2 year process of talking to him and meeting with him and showing my concepts and my ideas and my 2nd book, "Unmasking The Social Engineer", was co-written with Dr. Paul Ekman and was basically a diving into facial expressions and non-verbal body language, and not only how we can understand them and decipher them, but as an attacker, how they are used to put the target in the right frame of mind and the right emotional context to be compliant with the request being made.

Bill: Do you think attackers are aware of these non-verbal signs when they go into ... are they consciously trying to take advantage of these non-verbal signals, in your estimation?

Chris:

[00:11:00] If I had to estimate, let's say the large majority of attackers don't understand the psychology or the science behind non-verbals, but what they do understand is that when I'm nervous, I'm tense, and when I'm tense, my muscles are tense and my face is tense, and when that occurs, I create tension in the target. Great con men throughout history have learned that a smile, a head tilt, open ventral displays, they make people warm, friendly. They make people feel trusting, and when people feel trusting, they're so much more easier to bend and flex. They're so much more compliant in the requests that are being made. They may not understand like 'oh, this is the science behind why when I open ventrals that people react this way', but I think that they do understand how important non-verbals are, and then they learn to master that and control that, but as a security industry, we sometimes don't, because we're so nervous.

I know people that I work with, the people that work for me, and they get themselves so worked up during an SE pen test that that tension comes across and it creates fear and anxiety in the target, as opposed to empathy or compassion.

Bill:
[00:12:00] Interesting. Can you give me an example of how maybe you or your team has used this when you've gone into to do SE-when I use the word SE, you're talking about the social engineering, someone engaging you for an SE pen test, correct?

Chris: Yep.

Bill: Do you have an example of where you've used this to some success?

Chris:

[00:13:00] Yeah, so in one of the stories that I talk about in that "Unmasking" book with Dr. Ekman, to me it's a classic story, because it was when I first started to understand the non-verbals and then I said, 'I'm going to try to practice this and see how it works', and I had this whole pretext built in my head about how I was going to go to this company for an interview and I was going to show up and my storyline was going to be 'I'm driving here for the interview, I'm running late, an animal ran out in front of me, to avoid killing it, I slammed on my brakes, my coffee fell out of my hand, it went all over my car, and it soaked my last, remaining good resumes, so can you please help me with ... USB key and that computer that says, in a big sign, do not put USB keys in it, and print one out for me?'

That was my pretext, right? My preparation for it, of course, was having the right clothing and then having soaking wet resume folder, so that way it was visible, but then I knew that if I went in nervous or afraid, it wasn't the right emotion. The right emotion would have been sadness, because 'man, I may lose this job, and I almost killed an animals and I really love animals', so I walked into the building with my storyline, with my wet resume. Secretary turns around and says, 'Hey, how can I help you?', and she sees my hand holding wet resumes. I quickly scan her desk and I see she's got a picture of looks like a couple of little girls, probably her children, and they're playing with a cat. She's got a couple cat pictures around her desk, so I'm like 'okay, she's a cat lady.'

[00:14:00] I go up, and I have to show all the proper signs for sadness, so normally, even right now as I'm talking to you, I'm standing up in front of my desk, my chest is out, my chin is up. I'm using more what you would consider Italian-American gestures, big gestures, this is my normal way of talking. I knew that my normal way of talking would definitely not [see 00:14:22] this story, so I had to lower my shoulders. I had to lower my voice and my tone, and then I had to display proper sadness in my face.

[00:15:00] Now, this can't be grief. It can't be extreme worry and anxiety, because I didn't kill the animal in the story, right? It's just 'I have these wet resumes', so you have to show slight sadness and controlling that facial expression and then going 'yeah, I was supposed to be here in 5 minutes for an interview and this cat ran out in front of me, and I love cats, I didn't want to kill it, so I slammed on my brakes and my coffee went all over my car. It's all over me, it's all over my resumes, and I just don't think I'm going to be ready for this interview', and right away, the woman came helper-mode.

'Well, what can I do to help?', and I'm like 'I don't know, I don't know. I think my appointment's in 5 minutes and I don't even know what I'm going to do' and just showing some stress now at this point, and then she's like 'well, maybe we can make a pho-' and I'm like 'no look, the resumes are ruined, they're covered in coffee. I have this USB thing, I don't even know what you call them, what is it? USB thingy, maybe can you print one for me, maybe you can do that?' She takes the USB key and literally bends down to put it in her computer and there's a sign on the computer that says, 'No foreign USB devices'.

[00:16:00] She looks up at me, and I'm showing all the classic signs of sadness. Not fear, which would be the normal emotion at this point. All the classic signs of sadness and I'm kind of looking down at my watch like 'oh, about to be late for this appointment', and she just puts that thing right in. Puts it in. A minute later, I get a little text message from my partner saying, 'We have shell', which is the indicator that the remote exploit had worked, because she had clicked on the documents in the directory and one of them was a malware document that had a shell.

I get a text message and I just tell her 'oh, I'm sorry, that's just my notification about my appointment' and she prints out the resume, because we had a real one in there, she puts it in a binder for me, puts it in a little folder, hands it to me, and then she says, 'So, who's your appointment with?' I say, 'Oh, it's Mrs. Smith from ABC company.' She says, 'ABC company? Oh, this is XYZ. ABC is next door.' Now, I had done that on purpose, because they were really my target but I didn't ... I knew if I made a real appointment, things would be bad if I'm in the building. I didn't have an appointment.

[00:17:00] I'm like 'oh my god, I can't believe how bad of a day this is' and 'well, you probably saved my life, let me go over there.' Well, now this woman is in full helper mode because the job had been done so good that she is taking me by the hand and walking me over to the other company. I'm like 'oh, man', I'm trying to think of a way to get out of this, because if she walks me into ABC company and says, 'Oh, he has an appointment with Mrs. Smith', they're going to be like 'we don't know what you're talking about.' I'm like 'oh, you know what? You've been such a good help', I said, 'But I just need a few minutes to compose myself. This has been so stressful. I'm just going to take a minute, stand out here, get my thoughts together, and then go in. Is that okay?' She's like 'that's a great idea' and she gave me a hug and she left.

That's just one of the stories that I like to use to describe how it wasn't just non-verbals, so I won't say that non-verbals was the only reason we succeeded there, but it was a key factor in making the story believable and showing her that I'm not a bad guy and I'm somebody she can help.

[00:18:00]
Bill:
Yeah, I find that story so interesting. Then, in your book, the latest one, "Phishing Dark Waters", you talked about the Amygdala as well, kind of talking about the neuroscience of this a little bit more. That was the human piece of coming in and inserting a piece of technology in, bypassing policies and procedures that are probably in place, but what about clicking on-maybe you could talk about the Amygdala as it relates to where you see the importance of educating people about our responses to situations that would trigger the Amygdala.

Chris:

[00:19:00] Yeah, so this is an interesting piece of research, right? When I was writing the book with Dr. Ekman, one of the things, in chapter 8 actually, I started writing all about mirror neurons, and Dr. Ekman had read that chapter and he said, 'Look, there's very little research.' At that time, there was very little, now there is much more, but he said, 'There's very little research that scientifically proves mirror neurons, you may want to come up with a different topic.' I said, 'Well, I had this research here on Amygdala hijacking, what do you think about that?' He's like 'yep, that's a good one.'

I started reading all these papers he sent me, and it ... work by a very, very talented researcher, Daniel Goldman, about Amygdala hijacking, and they did a study where they took college students and these college students had to have a decent GPA, they were able to do complex mathematical equations. A part of it was it wasn't difficult for them, they had to be able to do it, so it wasn't super easy but they'd have to struggle. They put them in a EKG machine, where they're scanning their brain, and they give them these complex math problems to solve, and they timed them and they come up with an average, okay?

[00:20:00] These students can complete these problems in an average of 17 point something seconds per problem. I don't remember the exact time, so I'm just giving you an example, where they can complete these problems in x factor, 17 seconds per problem. Then, they took the same students and they showed them an emotional video, something that either was sad or angry. Something that had triggered heavy emotions, and then gave them not the same exact math problems but similar, so the same difficulty level math problems, and in every case, it took the students up to twice as long to accomplish the same math problems.

[00:21:00] They did this over and over and over, saying, 'Well, why is this happening?' When you look at the EKG scans, you see that certain parts of the brain were triggered after the emotional video that were not triggered during just the math portions previous part of the study. That led them to realize that the Amygdala, this little walnut-sized piece of gray matter in the brain that processes all of our external stimuli and then feeds out emotional responses to our body and other parts of our brain, that piece is translating the emotional stimuli way faster. Sometimes as much as 150 seconds faster than our brain is processing it. Things like auditory or visual modalities, things that we see, the senses, we see something or we hear something, our Amygdala's processing its response to that faster than our brain has the ability to process that response.

Bill:
[00:22:00] For me, that makes tons of sense though. Just as a species, I don't know the exact date, but we're well over hundreds of thousands years old as a species and I would imagine that ... I just saw some latest research that we're actually have a much more peaceful world nowadays than we have in the past. I know some people take objection with that, but I actually have the research study that shows that, but just as a species, we would have to be able to decipher threats very, very fast from just walking up to people, understanding the landscape, understanding the micro-expressions. I would imagine this is a capability that we've developed over millennia.

Chris:

[00:23:00] Yeah, so we're definitely built-in, with an internal radar. At least in my understanding, that's the way that we were created, to have this internal radar, and, sometimes, what happens is we force it to shut off because of society, right? I've seen this in my own family. Not with my children, but when I was growing up. You meet somebody who gives you the creeps as a little kid, and maybe you don't want to talk. You hide behind your mom or dad, and what do they do? They smack you and say, 'Be polite! Come out here and say hello.' Well, what is it about that stranger that made that child feel creepy? Well, maybe there's no exact answer to that, but whatever it is, there's an internal radar that said, 'Hey, I don't feel good here', right?

[00:24:00] This happens more with children and with women. They have this internal radar where they feel it but then they're told 'well, you're just being silly. You're not really thinking through this', but we do, we have this radar to determine threats. If we didn't, like you said, it would be much more difficult for us to determine those threats. From a science point of view, understanding that certain emotions, emotions like sadness and fear and anger, can trigger the Amygdala, which will make the reasoning centers slower to respond.

This is a very, very terrible analogy. I'm going to tell you that up front, and it's only because I am not a neuroscientist, I'm not a researcher. I'm not even a psychologist, so for me to understand that in my very simplistic mind, I consider it like way back in the day with co-processors, and you had an old machine and if you did one process that was too heavy, the processor slowed down and it couldn't do other processes, right? If you were scanning something and you tried to open up Word, Word would take forever to open up. Why? Because it was first scanning this.

[00:25:00] In a very simple analogy, that's the way our brains work. While it's triggering these emotional responses the Amygdala is, the reasoning and logic centers cannot trigger as fast. As a social engineer, I [ripped 00:24:52] this research, and I said, 'That means if I can trigger the proper emotion in a target, I can actually disable their ability to think reasonably and use logic.' I correlated that with Dr. Ekman's research where he said that non-verbals are 2 way streets. Not only do we make a facial expression when we feel an emotion, but by actually making the facial expression, we can create the emotion. This is a powerful piece of research, because-

Bill: That's the mirror neuron part, so you just have ... someone mirrors your empathy or mirrors your fear or whatever, is that what you're saying?

Chris:

[00:26:00] Exactly, but you also create the emotion in you, and that's the amazing part, right? If I can master the proper facial expression for sadness, then I will create sadness in me. Now, that doesn't sound too popular and happy, but from a social engineer standpoint, that means that I will do all the things that are not natural for me as a guy who's confidently standing with his chest out and his chin up, but if I can create sadness, then I will have the slumped shoulders, the softer voice, the lower head tilt, the closed body language that mirrors sadness, and like you just said, when someone else sees that facial expression, then they will begin to mirror the emotion that they are now seeing.

This means that I can create in you a feeling or an emotion that you didn't feel before, and if I can create a strong emotion like sadness or fear, which fear would be terrible for social engineering, from a positive side, not from a malicious side, but if I can create those emotions in you, I can shut down your reasoning and logic centers, which means that once that emotion is triggered, then if I make my request at that point, then you are more likely to make the decision on that request based purely on emotion and not on reason and logic.

[00:27:00] Now, that is a lot to consider, and some people go 'wow, that's too complex', but it's really not. It really is a fact of if you mirror the right emotional content on you, you will create an emotion in your target and that emotion will make them respond the way you want them to respond. In essence, it is like a buffer overflow for a human.

Bill:

[00:28:00] It also gets back to an earlier point you mentioned about why, and I think understanding why, you might not need to be a social psychologist or a neuroscientist, but just understanding why gives some meat and legs to the motivation, and the motivation to even engage on a program to educate people, but so how do you talk to people if-so we've just gone into a neuroscience, psychology from a high level perspective, how do you translate that into ... I'm thinking of it as from a Taekwondo, I have a black belt in Taekwondo, and so you're watching your adversary coming in but then you have to counter, so how would you train someone in a company ... you're not necessarily going to make them interested in the neuroscience of it, but how would you train them how to be aware of an exploit?

Chris: That is the piece that this research really helps with, because back to Dr. Goldman's research, what he found was that if they showed the students an emotional video and then they gave them 30 seconds in between the video and the math problems, that their ability to solve the math was back to normal time.

Bill: Oh, a delay. It was a little bit delay.

Chris:

[00:29:00] It was a delay. All it took was for the ... for up to 30 seconds for the brain to return back to its normal processing power. We teach people that when you feel an emotional trigger, like you get a phishing email that says, 'Your accounts have been hacked, you better click here', or you get someone on the phone who says, 'This is the IRS, you owe back taxes, I need your credit card number', or you get someone who's telling you that they have to get into the [CE's 00:29:06] office to fix the computer because he was called and someone's going to get fired. When you feel that trigger of emotion, find an excuse to pause for 30 seconds. Think about what's being requested, and then return to making your decision, because what happens is is we're too busy. I don't know about you, but I probably get somewhere in the range of 200 to 300 emails per day, no joke. That many emails, it's not my job to check email. It's not my job. Even if you're only getting 100, 150 emails in a day, and we know that at least 1 or 2 of them per day are going to be phishing emails or spam or something terrible on your computer.

[00:30:00] We don't have the time, we tell ourselves. When we feel that emotional trigger, it's best to get up, stand up for even if it's 5 or 10 seconds, think about what you're being asked to do, and then respond. You don't have to respond right in that second, and that simple task alone can save so many people. Now, the 2nd thing that we tell them is you need good policies in place that are actionable and usable by companies. I'll give you an example of a horrible policy. Don't click on bad stuff. That's a horrible policy. Why? The person has to translate. 'Well, what's bad stuff, and what if I don't know what bad stuff is? What if I don't think this is bad stuff?'

[00:31:00] You can't do that. You can't put a policy that's not actionable and the person has to figure out. You make a policy that a person can take action on, but that also is clearly understood, like 'do not click on links that do not come from trusted sources', but then you have to tell them-how do you figure out if it's a trusted source? You got to give them the steps. Now they get a phishing email, and they clink on a link from a non-trusted source and you can now go back and say, 'Well, did you follow these 3 steps we told you to figure out if it's a trusted source? No? Well, this is why you failed on this particular assessment here.'

We educate people to have critical thinking and good policies, and those things can save people. I tell you this, anyone who says they're going to make you hacker-proof, they're full of it. There's no such thing as hacker-proof, but they can make you not the low-hanging fruit. These 2 simple steps can make you not the low-hanging fruit, which can really decrease the amount of attack vectors inside your organization.

Bill: That's interesting, so that pause-actually, I can use that with my 15 year old, that 30 second pause, that's good parenting advice, Chris, as well as-

Chris:

[00:32:00] It is. It's life advice, because this is a human thing, right? This is not just a security thing. This is the way we work as humans. As humans, we get triggered emotionally on a constant basis. Think about it, half of media, and probably more, 90% of media is designed to do just that. To trigger emotions like anger, when you hear things about terrorism. It triggers things like lust, because they're showing you more and more sexually provocative images. To trigger things like fear, when they talk about the latest plane crash or the bombing.

The media is designed to make you trigger emotional responses, and then what's right on the side of your browser bar when your emotions are triggered? ... ad, because every company on Earth has followed you and collected all of your cookies and they know everything that you've looked at, and they're ... you up the very thing that you may have said no to originally, but now you're saying yes to it because of that particular emotion that you're triggered into. Marketing people know it, right? Scam and con artists know it. Hackers know it, so it's now time that the regular, everyday person knows it, so they can start using it to be protected.

[00:33:00]
Bill:

[00:34:00]
Well, I think this is great advice, because I think there's the tyranny of efficiency and the tyranny of the grind and everybody has experiences where they've just got to grind it out at work or they're grinding through work and then have to grind it at home, and it can you dull you down and there's a ... I think all of us are empathetic to that, and I think the only sad part is you get stuck in that too long, but being aware and taking that break, it's almost like a get out of jail free card. Just hit that button, stand up, and don't react, because what's interesting is I find, at least in our security practice, that clicking on something ... there's a powerful problem we have right now, which is you click on something inadvertently and it could take the company out for ... it can make the company limp for days with malware, with all of the sudden files being zipped up. What are you seeing today as being the single most biggest problem that can present itself from clicking on something that you shouldn't click?

Chris:

[00:35:00] Well, phishing is the biggest problem, right? Phishing is the biggest vector right now. If you look at all the latest breaches, phishing was involved at some point, and maybe not 100% but you can see that in a large majority of them, phishing was involved in so many of these breaches. It's a problem, because we live on email, and we get email everywhere. You get email on your computer, your laptop, your phone, your tablet, you're getting email everywhere, and attackers know this, so they're inundating us with exactly what you said, links to click. We're seeing a massive increase in BEC scams, so that's Business Email Compromise scams. I think the FBI reported that there was something like a 300% increase in just 6 months in the amount of BEC scams just in this country. Their whole goal with that is basically to infiltrate an email account and then search through the sent mail to find ACH data and then do wire transfers out of your account into theirs. Just cleaning businesses out with wire transfers.

Bill: Can you explain that again, that's called a BEC-

Chris: BEC scam. Business Email Compromise.

Bill: White listed email, that wouldn't take care of this because these are normal, valid accounts?

Chris:

[00:36:00] Yeah, it's like sending you an email and saying, 'Hey, this is Paul down in accounting. Look, I need you to check this invoice because it has your name on it and we have no clue who the vendor.' You double-click the invoice and it's malware. Now, I'm on your machine. I'm the attacker. You email back and you say, 'Look Paul, I can't open this, it's crashed.' 'Oh, okay. It just deleted, I'll send you a new one after lunch.' You delete it, you move on with your day, because you think I'm from accounting. I'm on your machine now with malware and scraping through tons of email looking for ACH data, looking for your wire transfer data. If you're in accounting, you're going to have it, right? Now, I'm scraping, looking for bank accounts, looking for SWIFT numbers, and all with the goal of doing transfers out of your account and cleaning businesses out.

[00:37:00] It is a huge problem right now, because they're not shutting down the network, they're not ... when that happens, you know it. You know you've been attacked, right? When ransomware is on your network, you're not going 'yeah, I wonder if we have a problem.' You know you have a problem. Sony, when they got hacked last time, they knew there was a problem. There was a giant flaming skull on their screens, that you don't have to worry, but the normal BEC scam, you don't know what's happening. You move on with your day, right? I think it was just 2 years ago, Coca Cola had that. President of Coke says, 'We're going green', a group of Chinese attackers sent a high level VP in the company a pdf saying, 'This is all about green initiative, please read it.' He opened it, it crashed, he deleted it, didn't think anything about it. 6 months later, FBI's knocking on Coke's door saying, 'Hey, you guys know you're sending gigs of data per day over to China?' They're like 'what are you talking about?' Check the network, they had been compromised for 6 months. 6 months they were in the network just scraping and exfiltrating everything they could.

Bill: Unbelievable. What is whaling? How is whaling different than phishing?

Chris: The terms like whaling, the difference is really just in the target. Whaling is a big target, right? You think of a whale being a big fish. It's someone who is pretty higher up in the company, and-

Bill: The CEO of Coke would fall into that?

[00:38:00]
Chris:
Yeah. That would fall into that. Then, normally what they're doing when they whale is they're looking for specific info, so what they call "doxing", looking at open source intel online and [giving 00:38:07] all the information they can on the target and then using that information to develop a couple key phishing attacks or ... attacks or combination attacks that they feel would work based on the information they found.

Bill: Okay. I wanted to clarify that, and so it's really a variant, it's really just a play on words more than anything else, but it's targeting the top level person who would be potentially offer the most vulnerability to an organization.

Chris: Yeah, you have phishing, whaling, spearfishing, you have all sorts of different terms. They keep coming up with them.

Bill:
[00:39:00] Vishing, V-I-S-H, I don't want to assume everybody's on the same sheet of music when it comes to this, but I realize some of the audience may understand these terms but I want to make sure everybody does. Vishing, that is phone confirmation of a spearfishing attack?

Chris:

[00:40:00] Not necessarily. Vishing actually stands for voice phishing, so it could be linked to an actual phishing attack, but vishing is also being used now to collect credentials, to collect credit card data, to collect other pieces of intel that will help the attacker attack the company. Sometimes, it's as simple as just information gathering, calling and finding out who your vendor for trash removal is or who your vendor for your soda machine is, and those particular pieces of data can be used for an on-site attack. Finding out the name of the girl in accounting. All of a sudden, that becomes a use in an attack. Finding out the type of email nomenclature you use, is it first name dot last name at company dot com. The vishing is used for all sorts of information gathering in addition to attacking now.

Bill: Is that the old fashion-would the other word, would that be pretexting? Would that be similar?

Chris: Yeah, pretexting is part of both. Phishing and vishing and it's actually part of on-site, too. Pretexting is your story. Pretexting is who are you pretending to be? Whether that's in a phishing email, whether that's on the phone or whether that's in person, it's the act that you're saying you are.

Bill:

[00:41:00] Excellent. As far as having a program, there's different levels of programs that an enterprise can roll out here, and assuming the human attack weaknesses is the ... everybody here listening, it's human error is the biggest issue, is it human error, so how do you scale education of hundreds and thousands of employees? How do you attack that type of a problem, Chris?

Chris: This is going to sound very self-serving, because this is what I do for a living, but I have an analogy that may work, especially with you since you have a martial arts background. If I wanted to learn your art and I came into the gym and you were the teacher, and I said, 'Hey Bill, I want to learn how to box. I want to learn how to fight. I want to learn how to use Taekwondo', and you sat me down in front of a 20 minute CBT all about Taekwondo and then said, 'Okay, here's your black belt. You're done', I would be like 'this guy's nuts.' It wouldn't work, right?

[00:42:00] At the same vector, if you took me into the gym and you put me in the ring day 1 and put me up against a black belt and said, 'Okay, spar', I'd also think you're nuts, but what I would expect is that you take me into the gym and you show me the moves. You show me the stance, you show me how to hold myself. You show me how to deliver a punch to a bag. Then when you feel that I'm ready, you put protective gear on me and you put me in the ring and I spar with a person that doesn't want to kill me but wants to teach me how to take and give a punch. Eventually, I'm at a level where if I was in a real fight, I'd be able to use those skills.

[00:43:00] We say that is no different than educating your people and social engineering vectors. You can't show them a CBT that's going to make this make sense. You have to phish them. You have to vish them. You have to show them what it feels like to be phished, to be vished, on a consistent level. If I came into your gym once a year and I said, 'Hey, teach me something', you would think 'this guy's not serious about his education.' It has to be consistent. We recommend monthly phishing programs. We recommend consistent vishing calls, and all with a person who doesn't want to kill you and humiliate you. With a company that wants to help you with education, teach you why these are such dangerous vectors, and then use that information to continually build educational programs inside your organization to help protect.

Bill: I love your analogy. I love that analogy, because I think that the way we use language is so powerful. Otherwise, we turn people off, so I love the way you just linked that to essentially a very physical thing that everybody can relate to.

Chris: Thank you.

Bill: Are there ways that you see, like the top way, programs fail? I love that analogy, I think it's going to light up people to look at taking on a social engineering program in a different way, but is there 1 reason why you see most of these programs not gaining velocity, or failing?

Chris:
[00:44:00] Yeah, there's actually a few, maybe 3 I can give you. First, it's no support from the top down. If your C level does not support you, your program will fail. You have to have a top-down buy-in. This program is going to tick people off. It's going to make people mad, because they're just going to feel like it's a waste of their time until they see it working. If you don't have the big C support up top, you're just going to get hammered from every manager between you and the CEO. You have to have top-down support.

[00:45:00] 2nd is using shaming and embarrassment as opposed to positive reinforcement. Too many programs I see want to basically punish people for failing. Punish people for being human, right? Let's think about this. Last year, I sent 3.5 million phishing emails. That's how many phishing emails I sent, okay? 3.5 million, and my 3rd book was written last year all about phishing. I think I'm a subject matter expert without being too braggy and sounding arrogant, but I'm a subject matter expert on phishing. I clicked on a legitimate phish last year. I clicked on a phish because I'm an Amazon junkie and I got an Amazon email and it looked legitimate and I clicked on it. Fortunately, I caught myself before anything bad really happened, but I clicked on the phish, so if you're going to tell me that anyone who clicks on a phish is stupid, then that means I'm stupid, and I don't want to believe that. I don't think that's the truth.

[00:46:00] I think that what happens is if you find the right emotional trigger for the right person at the right time, anyone can fall for a phish. Using shaming and embarrassment, it doesn't work. Positive reinforcement. You have, so far, C top level down, positive reinforcement, and then the 3rd thing I would say is lack of consistency. I've seen people who-companies who are like 'we only want to phish everyone once a year.' Well, great, so that's like, again, I come into your gym and give me one lesson this year, and then I say, 'Okay Bill, I'll see you next year for my next lesson in Taekwondo.' I'm not going to learn anything, and I'm definitely not going to retain it, right? I'm not going to go home and what, I'm going to practice the 1 lesson you gave me for 1 whole year? It's not going to work. No-one's going to do that.

Bill:

[00:47:00] Last year, one of the CIO masterminds that I'd been running for about 20 years, last year, one of the-this often happens, but one of the CIOs says, 'Is anybody using-', it was one of the self-phishing tools from the cloud, he said, 'Is anybody using [Nobe 4 00:46:34]?' Nobody was, and he explained it and subsequently, everyone went out and started using it, but his story was interesting because he's like 'listen, the first time I used this tool to self-phish myself, I had 25% percent of his users clicked it.' Clicked on the link. As he's been going along and educating and educating, he's been driving that percentage, driving it down, driving it down, and there's very few things in security that you can actually show measurable improvement on that actually has a massive impact. That one, you can get really excited about, because the negative consequences are just so deleterious. Interesting story that my group popped up there.

Chris: Yep, I'm with you. I'm with you. Sometimes the best recommendations are those that don't come from the person supplying the service.

Bill: Do you ever use gaming? Can you turn it into a game, where-go ahead.

Chris:

[00:48:00] I want to say, I'm for gamification, but at a limit. For example, I'm all for ... we have one client that what they did is they're huge, so they have this 1 division that's maybe a couple hundred people in this division, and the division manager bought a plush fish Nemo doll with a crown on it. Every month, when they get their phish, the first employee in that division to catch it by not clicking it and reporting it properly gets the fish at their cube for the next month. Now, it's something so simple and so silly, but you see 200 grown adults lobbying and fighting for this plush Nemo doll. Why? It's a game. It's a game. I've seen other companies who, if you successfully catched a phish for 3 months or 6 months in a row, you get a gift card to Amazon or Starbucks or something.

[00:49:00] Gamification to that level, I agree with, right? Even if it's recognition, even if it's just like 'hey, every month, if you catch it, you're going to go in the employee newsletter intranet or something', I'm all for that, but sometimes, gamification go too far. After you click the phish and you're on this page and now you're playing a reel in the fish game. It's company wasting time, and it's not really educating the person what to do next time. I'm for gamification, as long as it gamifies and motivates them to take the proper action and doesn't waste company time and resources.

Bill: I love it, I love it. Well, look, I just have 2 questions, 2 followup questions for you, Chris. One is related to the C level top-down buy-in. If you had to give some resources for ... if you had to-and again, this is if a CEO doesn't get this, there's a problem, but some of the CISOs, CIOs, [inaudible 00:49:28] here are going to need to have some ammo, so what resources would you point to that could help someone build an investment case around this, either the cost of being hacked or ... how would you help someone and where would you point them to to build an investment case around it?

Chris:
[00:50:00] 3 resources I would give you. First, on both of our sites, the social-engineering.org and .com, we have infographics and blogs that constantly are analyzing recent attacks and talking about the cost of them. 2nd, the Verizon DBI report. It comes out once a year and it talks in this last year, again, phishing is in the highest marks for attack vectors, and then, there's a website called the APWG.org, and it's the anti-phishing work group, and all they do is collect phishing data. That is all they do, these people are amazing. They collect phishing data from around the globe and they issue a quarterly report showing the largest kinds of phish, the volume of phish, the cost of phishing, and it really outlines very clearly the results of phishing as an attack vector.

[00:51:00] So far, there's not really a lot of data out there in relevance to vishing, so we're working on some of that, but there's not a lot out there, but I would focus on the phishing and show the dangerous aspect of that with those 3 resources, and a lot of times, the CEOs, if they can't see it after that, then there's probably little hope that you're going to convince them of it. Most likely, this is sad to say, what will convince them is an actual attack on their people.

Bill: Yeah, right, exactly, something used to trigger their Amygdala, they haven't been triggered.

Chris: Yeah, exactly.

Bill: My last question to you is from a non-business point of view, what kind of books have you most read that you find would be, they're interesting to you, that some part of our audience may be interested in reading it themselves.

Chris:

[00:52:00] I love Paul Ekman's books, right? My favorite one of his is called "Emotions Revealed". To me, it's a phenomenal book, if you're interested in all at non-verbals. Really is a tremendous book. Let me see. There's a couple others that I would recommend, and it depends on how many you really want.

Bill: Anything related to neuroscience, related to any hobbies that you particularly have or any genres that you like?

Chris: Okay, so definitely then Paul Ekman's books, on that. Then, oh boy, I should know the name of this book off the top of my head, shouldn't I? Yes. Amy Cuddy's book, her book "Presence". First of all, she's a phenomenal, phenomenal person. I had a chance to meet her and interview her on our podcast. She is just amazing, and her life story and her work is just amazing.

Bill: Her TED was excellent too, by the way.

Chris:

[00:53:00] Yeah. I think it's one of the most widely watched TED talks ever in the history of TED. Life-changing stuff with Amy. That's really a wonderful book that I recommend to a lot of people. Thirdly, there's another psychologist, Dr. Ellen Langer. She wrote a book called "On Becoming An Artist", and it's all about her research into the state of being mindless. It's about mindlessness, and how these people go through their life performing their job and their duty in life mindlessly. They don't really think about things as they're doing them, and that state of mindlessness is what causes a lot of problems in life today. Some of her research is literally life-altering and changing. Those 3 books, I'd say I recommend those 3 books as ones that I keep on my bookshelf and I use as reference points all the time when it comes to just personal hobbies and things that I like.

Bill:

[00:54:00] Well, I think it's an interesting theme to your interests, which developing presence and developing awareness and developing the ability to become more aware of your reactions, your unconscious reactions to things, so really, really fascinating. Well, I want to really let you know that I'm going to put all the [show nuts 00:54:06] to this on our site, so all 3 of your books I'll link up. "Phishing Dark Waters", your latest one, relates to social engineers, what's the best way for people to reach out to you if they want to pin you and say hello?

Chris: Twitter is probably the best way. As scary as this will sound, my Twitter ID is HumanHacker, all 1 word, so that's me. Then our websites, like you said, you'll put them up there, social-engineering.org and .com. Both of them have all our other contact details. Anything from Facebook and email and all of that people reach out. I like to say as a company and myself particularly, I'm pretty good about reacting to people if they email or if they talk to me over Twitter and trying to make sure we can have good conversations about this stuff.

[00:55:00]
Bill:
This has been super fun Chris, I appreciate your time coming on the show and sharing very pointed suggestions for people to be able to leave and implement within their organizations, and I'm sure people reach out to you and say hello or engage with you.

Chris: Yeah, thank you very much, it was a lot of fun.

Bill: Okay, talk to you soon.

Chris: Bye.