**Project Completed by:**

**Selections from the**

**EDUCAUSE Security Professionals Conference 2018**

**August 21, 2018|12:00 - 4:30 PM EASTERN**

**Selections from the**

**EDUCAUSE Security Professionals Conference 2018**

**August 21, 2018|12:00 - 4:30 PM EASTERN**

>> Hello, everyone, welcome to our virtual event, encore, selections from the EDUCAUSE security professionals conference 2018. I'm Valley Vogel, Senior Manager of the EDUCAUSE Cybersecurity Program. Information and logistics for today's event. First, we'd like to thank DUO security for the sponsorship of today's event. Student, faculty and staff portals allow for convenient remote access anywhere, any time. The trusted access and multifactor authentication solutions. We'd also like to thank Hunter Ely for joining us today, he'll be providing a brief talk this afternoon on behalf of DUO security. Eight encore sessions from the 2018 security professionals conference, held in Baltimore this past April. The event spanned three days and featured over 50 informative workshops and sessions with networking opportunities for over 800 attendees. For anyone who missed the conference, or found themselves double booked during a session, our online event will reprise this year's most informative sessions. We'll kick things off with the keynote speaker Dr. Jessica Barker, discussing cybersecurity. Fun ideas to create more positive messages for your campus security programs. Following the keynote talk, you'll hear from Linda Ludwig, Joel Rosenblatt, Sarah Brawn and Joe Jody Ito. Now to Adam La Faci.

>> Thank you, Valerie. And thank you all for joining us today. Before we start with the presentation, let's take a few minutes for a brief overview of the online room. In the main window, you will see we have the PowerPoint presentation, and you'll be able to see each individual presentation throughout the sessions today, appearing there. We also hope you'll join us in making these sessions interactive by using the chat box on the left of the screen to share resources, comments and to submit questions. Throughout the day our presenters may be sharing interactive polls, feel free to click on it to register your response. Finally, you'll see an audio issue slide in the lower right-hand corner of the screen, just click there if you experience any audio issues and would like to try some simple troubleshooting steps. The Twitter hashtag is #Security18. And we'll be monitoring the Twitter feed throughout the event. And now, on to a few notes, if you are to encounter any technical difficulties, during today's event, for all sessions, you'll receive the session audio over your computer speaks and most difficulties can be resolved by logging out and back in. If you run into other technical problems, send a private chat message to technical help. Click in the upper right-hand corner of the chat box, and select start chat with. Then click attendees. And at the top of that list, you'll see technical help. And in case of any room wide technical issue, we will be posting updates and advisories here in the adobe connect chat. And with that, I'll turn it back over to Valerie.

>> Thank you, Adam. As always, we are assisted by a terrific group of colleagues to PR E pair for today's event, and I'd like to acknowledge their contributions, our online team of event production staff including Adam La Faci, Jody Tracy, Sean Kennedy and Veronica dice. Our marketing team, including Katy, our corporate team including Carolyn Colman, the security professionals conference committee and our 2019 security professionals conference program chair, Jaclyn Pitter, who will be my cohost for today's event. And now, I will turn it over to Jacqueline.

>> Thank you, Valerie. Hi, everyone, I'm your cohost, Jacqueline Pitter, I'm pleased to be introducing our keynote speaker Dr. Jessica Barker. Dr. Jessica Barker is a leader in the human nature of SIEB you are security, one of the top 20 most influential women in SIEB you are security in the UK and awarded one of the tech women 50 in 2017. Equipped with years of experience running her own consultant SI, redacted firm, working with a variety of organizations from small creative agencies, to multinational banks. Her consultant SI experience, technical knowledge and sociology background give her unique insights and has a talent for translating technical messages to a nontechnical audience. Dr. Barker joined us in Baltimore a few months ago and today, she is joining us from the U.K. to discuss why a better understanding of human nature needs to be a greater priority for the cybersecurity community. Jessica, we are lighted to have you with us again, welcome on behalf of our participants, please feel free to begin.

>> Welcome Dr. Barker, sounding nice and clear now, we'll turn the floor back over to you.

>> Fantastic. Thank you. Well, apologies for that introduction, everybody. We will blame the technology. So which is accurate for my presentation today. Where I'm talking about cybersecurity awareness. What I am talking about today is how we can take lessons from other disciplines, such as psychology, sociology, behavioral economics, neuro science, all of these fields, which have studied human perceptions, human behavior, how we think and why we behave in the way that we do. How we can take lessons from those disciplines and apply them to how communicate and raise awareness of cybersecurity. At the core of my discussion today, is the fact that we often talk about the importance of raising awareness about cybersecurity when we are trying to tackle the human side, when we're trying to get through to people and get them to understand why cybersecurity is important. And the kind of behaviors that we want them to pursue. The problem I have with this is that we can raise awareness about something but not necessarily positively influence behaviors. So I would argue that awareness off cybersecurity is really high at the minute, and has been for a couple of years. But that doesn't mean that are following the kind of behaviors that we would like. So people are aware that cyber security is an issue, aware that it's something that they maybe should be considering, but they aren't necessarily taking those behaviors with regards to password authentication or social engineering attacks, that we would like. So I think it's important that we then consider ways that we can better communicate with people. And this, for me, is about understanding how people think. And what is happening, when we are communicating messages to them internally, how they receive our messages and how they act off the back of them. So for me, a lot of this is about understanding -- known in psychology, essentially, short cuts in the brain, which will really have an influence over how people behave. So these are ways of thinking, these are ways of making a decision that we won't necessarily be consciously aware of. But we will all be subject to, so to get through a day to make decisions, we all rely on these ways of thinking, these short cuts in the brain. My presence today is going to cover the extent to which these are important when it comes to cybersecurity. Before I go on, I wanted to ask you all a question, I wanted to try to do an interactive poll. Where I ask you whether you have considered principles from psychology when planning your awareness-raising training? Have you looked to discipline such as psychology and ways of understanding people to inform what you put in the content or how you deliver the message? And this of course could been from having formal training psychology, could have been from informal learning that you've done yourself, consulting other people, I thought it would be interesting to get a baseline to know at the moment whether most of our participants have considered psychology when planning their awareness-raising training, in the content or in terms of the delivery? So we're getting interesting results coming through and I'm going to ask for the poll to be closed in a couple of seconds. It's showing that most people haven’t, but a good percentage have. We have about 32% of people saying they have considered principles in their awareness-raising training related to psychology. So we will close the poll now. And move along. But thank you so much to everybody who submitted that answer. So I'm going to talk about some of these, which I think are particularly interesting, when it comes to cybersecurity awareness raising. The first one I want to talk about is something we will be very familiar with. Even if we might not know its typical name when it comes to psychology. And this is the idea of social proof. Social proof is a huh Riessic, which is essentially, when we don't know how to make a decision, we will look to how other people behave to lead what we are doing. So social proof is used really strongly in a lot of marketing, and in a lot of Web sites. So for example, it would be trip advisor, Google reviews, AIRBNB, all of these kind of Web sites that look at showing what other people think about something. How they have reviewed it. And if you see that 90 people have given something a four or a five-star review, then you're more likely to give that service or product a try. So social proof is really powerful. And recently, research a number against this, it suggested that when about 25% of the group start behaving in the same way, most of the people in that group will follow that behavior. And this is because we don't want to be wrong. We think other people might know better. So social proof is really fascinating, and it's been explored in a lot of disciplines. But not really in cybersecurity. So one discipline that has looked a lot at social proof and the influence of behavior, the emphasis on behavior of social proof is environmentism and the attempt to tackle climate change. But for example, some research has looked at hotels and the extent to which people will reuse their towels in hotels. And it shows that most people don't reuse their towel, they want a new fresh towel every day. And of course, this has overall a large cost on the environment. So some researchers looked to whether they could influence the extent to which people reuse towels. Using social proof. So for example, in some hotels, they put a sign in the bathroom, and instead of the sign saying please reuse your towel, to save the environment, as we often see, they try to find science that say most people in this hotel reuse their towel to help save the environment, will you please do the same? And what they saw is that of course people who saw this message were more likely to reuse their towel. The research has been tried another message, to see if they could make the social proof even more persuasive and what they found is that messages that said the last person who stayed in this hotel room reused their towel. Will you do the same to help save the environment? They were the most persuasive messages of all. So we really look to people who feel close to us, and someone who feel we can relate to be most influenced by social proof. Asive I've said, social proof has not been explored in terms of cybersecurity, but I think it's interesting to consider how we may be inadvertently use social proof and use it against us. So usually, most of the messaging around cyber security and behaviors is of course very negative. We will generally tell people, oh, everybody has got terrible cybersecurity, nobody is at the timeing up two-factor authentication, humans are the weakest link and here's a list of terrible passwords that most people are using. So from my point of view in terms of psychology, this is causing us problems, because what we're doing is we're saying to people, oh, everybody has got a terrible password. And so, an individual hears, oh, okay, everyone else has a terrible password, so it can't be that important for me to have a good one. If it's good enough for everybody else to have a terrible password, then it's good enough for me. So this is my first lesson when it comes to applying technology to cybersecurity communications and awareness raising, how can we get social proof on side? One simple way to do this for example is to consider if you are doing a Phishing simulation exercise, then what messaging are you putting out around that. Are you saying to people, when it's done, oh, the exercise, and 30% of people clicked on the link and -- [Inaudible] do better next time. Or are you saying, we ran a Phishing simulation and 70% of people didn't click on the link. So next time, join your colleagues in being part of the majority. So another interesting thing to think about in terms of cyber security, is whether we can communicate in an optimistic or in a more negative tone? Research has found that most people actually are wise towards being optimistic. So this is research conducted by a team of neuro scientists over the last ten years, and they have found that about 80% of people are wired towards being optimistic. What they've also found is that optimism is more powerful than -- they saw optism pervades -- that doesn't have much of an influence over how optimistic you are. The optism is the natural way that most people are leaned, most people are wired, and around the world. And no matter what messages we give people, no matter what facts we give them, they will still remain optimistic. So for example, the research has conducted a study where they took a group of people and they asked them how likely they thought they were of getting a disease such as cancer. And individuals were likely to reply, they thought they had a 10% chance of getting cancer throughout their lifetime. Researchers told them the facts, which was that we all have about a 30% chance of developing cancer. And the individuals were reluctant to let go of their optimism. So then, the average response was, okay, so, maybe I've got 11% chance. So what it shows us is that no matter what facts we give people and no matter how much we tell them where hacks have happened, how likely they are to be hacked, the influence that it would have, the impact it would have, people are going to retain their optimism. So this seems like pessimistic views when it comes to trying to communicate about cybersecurity, but the good news here is that optimism actually makes people try harder. So if we can actually use a tone that is more optimistic, that is more empowering, that tells people, you know, cyber security is a problem, the threat is real, but there are a lot of things that you can do that are quite straightforward that actually will bring the threat down to a great degree. Then people are more likely to engage with those behaviors that we are suggesting. So what can we do? For the second lesson. To engage more with optimism. This of course is moving away from a lot of our traditional approach, traditional approach in cybersecurity has been quite rooted in fear and uncertainty and doubt. In trying to scare people into behavior securely. And the bad news about this is that when it comes to the psychology of fear, if we simply tell people something scary, and think that that's going to lead to better behaviors, then unfortunately, that's not how it works. There has been about 5 decades of research into what is known as the fear appeal. So telling people something scary to try to change their behaviors. And what these five decades of research has found is that if you're going to use a scary message, try to influence behaviors on the back of it, you have to communicate that message really carefully. What happens in my brain and all of our brains when we are confronted with something scary or a threat, we will naturally appraise that threat, and we will consider how real it is. Particularly, how susceptible we are likely to be that threat. Only if we think we would be susceptible to that threat, for example, the hacker who want my data, motivated to think about the response of us being promoted, so we would appraise the efficacy. So we need to understand the threat is real and applies to us, before we even consider some of the behaviors that are being recommended. We will then go on to consider the behaviors and to think about whether they actually would work, and whether we are capable of enacting them. So when we're told to have a different password, a different complicated password for every account, when we're told to turn on two factor authentication, not to click on suspicious-looking links, am I able to do that? How am I going to do that? And only if we feel able to do that, will we engage with the actual danger. If we feel that those responses are beyond our reach, or that they wouldn't make a difference, then what we will do is actually just -- the emotion with the fear, and so we will bury our head in the sand or we will try to avoid the threat by not going on the Internet. And so, it becomes a very actually damaging way to try and spread our message about cybersecurity. And a much more empowering and a much more impactful way to communicate about cybersecurity is actually to try to highlight the positives that come from good cybersecurity. We can again look at research in public health to understand why this works and why this is a better approach. There were a set of hospitals in New York state that were trying to address issues of doctors and nurses not sanitizing their hands, and while they were on shift. And so these hospitals attempted to put in a system of surveillance the try to encourage doctors and nurses to use hand sanitizer, wash their hands more regularly. What the researchers found is that when they put in a system of surveillance and they told the doctors and nurses that they were being surveilled and monitored, they found that compliance with hand SAN sayings rose 10 percent, so it was important for the researchers. They then put in an electronic sign above every hand sanitize stand, the electronic sign popped up with a Smiley face and a message that said, good job. They also put in an electronic sign in the common area which tracked hand sanitize sayings by shift and they introduced an element of gain -- with the staff so that the shift that had the most hand sanitizing, the highest rate, they were rewarded. Compliance when they took this more positive approach, that increased by over 90%. These results were replicated in other hospitals. And this shows what we know from psychology already. That people are more drawn to a positive message, than a negative message. We all really like that dope mean fix, this is why social networking sites are so popular, we love to see the likes and retweets and comments going up, it gives us a nice reward and a good feeling. -- [Inaudible] so this quote from the doctor who was behind a lot of this research and neuroscience, really stood out to me. [Inaudible] about cybersecurity at all, but I found it -- how we can consider the research when we are communicating our messages. We need to overcome -- [Inaudible] -- rewards with reaching our goals, this to me, seems to be about the -- [Inaudible].

>> Jessica, sorry to interrupt again, sounds like we're having the audio breaking up at that end. Holding a quick moment to see if we can find an easy fix for it. We're reaching the end of the scheduled time for this event as well. [Please stand by for webinar to resume]

>> give us a quick test now?

>> Sure, I was just -- [Inaudible] the stereotype threat, I don't know if my audio is any better. --

>> Unfortunately, it's still cutting out for us here.

>> Oh, I'm so sorry. I'm on my third -- [ Inaudible].

>> I think we'll do a quick adjustment here, to see if we can clear this up for a brief wrap-up as we near the end of the allotted time. I'll be sure to queue you in a second.

>> Thank you.

>> Jessica, turning the floor over to you again, to see if we have cleared up the distortion. Feel free to give us a quick test.

>> Sure, I was about to move on to talk about the stereotype threat. And something quite different. Hopefully, my audio is a little better.

>> Wonderful, it's nice and clear now. We are reaching the end of the scheduled time for this session, we had technical difficulties, so we'll continue to forward with a little bit of it. But keep an eye on the time as you look for a spot to wrap up.

>> Sure, no problem. I will continue, I will talk really briefly about the stereotype threat, which is interesting when it comes to cybersecurity. The stereotype threat is the fact that if an individual or a group, is the subject of a stereotype threat, it puts such a threat on them, such a pressure on their performance, that they actually end up conforming to that stereotype. So there's been really interesting research done on this with regards to gender and math performance. Some researchers gave two different groups, math exams. And they told some of the groups that they'd been given these exams elsewhere and there was no gender difference. The other groups, we've been giving these exams before and there is a gender difference in the results. And you can see how those different groups performed. The ones who had been told there is no gender difference, they actually, boys and girls, performed about equally. The groups who had been told oh, there is a gender difference before they took the exam, the boys outperformed the girls massively. And this is because the girls knew that in other tests, there had been results, where girls had not performed as well, and so, it put such a pressure on the girls, there was already this existing social stereotype that girls are not as good as math as boys, and this meant that the girls actually under performed. So if there is a stereotype out there, it's so damaging to individuals that it means they actually don't perform as well. When it comes to cybersecurity, one of the biggest stereotypes we have is that people are the weakest link, that humans are the problem. And the difficulty with this is the more we say that, the more we are putting pressure on individuals, the more we are under that -- undermining them and the less able they are, it becomes harder for them to actually engage with what we're recommending. So this notion that users are stupid, we need to stop saying that, when we do it, we make it harder for people to perform. And we know this already from what's known as the pygmalion effect. They feel more empowered, they feel more able and they are more likely to engage with the behaviors and the recommendations that you are purporting. If you speak negatively about people, if you tell people they're stupid, they're less likely to try and they're more likely to perform poorly. If security doesn't work for people, it doesn't work. So what can we do to resist stereotypes? How can we better empower people? Because empowered people are more likely to engage with us. And we know this from research that has specifically been done around levels of empowerment, levels of self-efficacy, levels of confidence in information security. This research has found that people who feel more confident about cybersecurity, are more likely to pursue those behaviors that we recommend. Like doing their updates, having a good approach to passwords, having good general cyber hygiene. That comes from a feeling of confidence and a feeling of being able. So for example, having a report of Phishing in there, when they go to their e-mails, they can see a mechanism, a tool by which they can engage with good cybersecurity. So my fifth lesson of the day is what can we do to raise self-efficacy. People are the problem and instead, be more empowering, and be more encouraging? So a lot of this is actually just about how we frame our messages. With more understanding of psychology, we can actually make our messages so much more engaging and so much more impactful. The move towards better understanding of people and cybersecurity is already being taken. So we saw with guidance from the UK national cybersecurity a couple of years ago, this is being followed by -- last year, for example, to look up passwords, and have a more human centered approach. For example, not asking people to regularly change their passwords. It may be the right technical fix to suggest that people should regularly change their passwords, but from a human point of view, it actually just drives poorer behaviors. So these are my five lessons of the day. What can we do to get social proof on side, harness optimism, spread hope, not fear, and raise self-efficacy. If you want the references for all of the research, I'm happy to share them with you, and if you just want a quick introduction to behavioral economics, psychology, some of the things I've spoken about, these are my top three recommendation, nice, interesting reads. Thank you so much for your time, thank you for persisting with the problems with audio, and I'm delighted to be able to speak with you all today.

>> Thank you, Jessica for such positive and inspiring talk about security awareness. Due to the technical difficulties, we had with the audio, we are going to skip the live QA for Dr. Barker and we ask that people post their questions for Jessica for her to answer and respond to in the chat pod of the online room while we move forward with the next presenter. We're going to reset the stage for our next speaker, we will go silent for a few minutes. [ Please stand by for webinar to resume.]