[Please stand by for realtime captions.] >> Welcome everyone, you are listening to EDUCAUSE. This is Sue Traxler, Assistant Vice Chancellor for Information Technology & CIO at the University of Wisconsin - Platteville. I will be your moderator for today’s ELive session.

EDUCAUSE webinars are sponsored by Dell. You're probably familiar with the interface webinar we hope you will help make the session interactive and use the chatbox on the led to submit questions. To share resources and comments. If you are tweeting, please use the tag pound EDU live.

If you have any audio issues, click on the link on the lower right-hand corner and at any time you can direct a private message to technical help for support.

The session recording and slides will be archived later today on the EDUCAUSE website.

Now let's focus on today's webinar. Our topic for today is titled top attacks, top attack techniques, top human risks and how to create a cyber aware culture.

This is part of national cyber security awareness month celebrated every October. Today we will learn about the latest scary attack techniques and human risks facing every organization and how you can prepare for those threats to create a more cyber aware culture on your campus. We have three speakers today. The first will be Michael Kaiser, executive director of cyber security alliance, he is going to do a brief intro and then will be followed by Lance Spitzner -- I'm sorry Johannes B. Ullrich, the Dean of research at the SANS technology Institute and lastly, Lance Spitzner director of the SANS Institute. Michael, are you there next

I am. Thank you. I just want to give a big welcome to everyone. Let me tell you that it's national cyber security awareness month, this is our 13th year of doing this in collaboration with our partners who have cofounded and co-led the Department of Homeland security. We are so thrilled, we are already into week two about what's going on for this month, we have seen so many positive things happening. I will say that we so much count on our colleagues at EDUCAUSE and all of your college campuses, you are incredible [Indiscernible] for cyber security awareness all year round but particularly in October we are so thankful for everything that you do. You reach an incredible important audience, you are incredibly trusted source for the audience you reach and that is actually part of the key of awareness. We will see some tremendous things happening in the rest of the month, I see all of you posting all the time the #cyber aware, we love those comments, keep them coming. And I know you have terrific programs today. SANS is one of the most respected leaders in all of cyber security . I know Lance personally, he's a member of the national cyber security alliance board, we are thrilled to have him. He has provided great insight in depth to what we do. I think the blog he posted this week was fantastic. I will turn it over and just say again if there's anything we can do, come to our website, go to stop think connect.org and get materials and look at our most recent website which relaunched with the White House just if you weeks ago called lockdown your login.com. It's an effort to get people to secure their credentials which I'm sure will be talking about today. Happy October and thank you all again and we look forward to the great results that continue to come.

Thank you, Michael. Now I will move on and Johannes B. Ullrich has the first section.

Thank you for the introduction and what I will be talking about here is a little bit what happens if you don't necessarily [Indiscernible]. My name is Johannes B. Ullrich I'm in Jack will Florida and is part of my responsibility -- there tools a very recent events that we worked on over the last couple weeks. This makes it a little bit more real on how this affects the user and follow best practices. One actually what I'm thinking about a paper that was published a couple of months ago about security fatigue. Users are getting sick to being told to pick strong passwords and securing their systems, setting up firewalls, they are overwhelmed by all this. It's helpful to have an example and to show what happens if you don't follow those advice. We make it more real because when it comes down to at the end is when you use your system call you don't want to to be inconvenient, but there's some real risk involved if you're not following the standard advice and I picked two cases because we are a little bit time limited so I figured I will focus on two items here. One item that cost -- it's this case of insecure DVR. DVR have gotten particular a lot of attention because they were used in some of these huge service attacks lately. I have a picture of my little test DVR values for a lot of the testing I'm doing. Most of it is a hard drive and there's led -- very little board that's an extremely stripped-down version of Lennix. One of these tools don't necessarily exist on these DVR. [Indiscernible] are really knew how this particular device I bought this I think two years ago so were looking at the most recent attacks, and then the way they were used is there were used as the chat internetworks. Why are they so dangerous? They hear typically default passwords that are not typically changed by the user. If the user does the right thing, they change it -- the web-based admin interface they may not necessarily change the password that connects to that device but there is a use oversight here from the manufacturer. Years ago and looked at this these devices were used to it attack internal networks. These are DVR, these are not a TV DVR to record TV shows, these are typically used for security cameras so the reason they are easily accessible from the outside is that first of all they come with a very popular feature called universal back and play [Indiscernible - heavy accent] and one thing you know that they often expose some intentionally because they have an outside security monitoring company that would like to have access to these systems. Let's actually just move on here, these are some of the default password, Google and default passwords. Google is very helpful because have that little table the thumbs-up some of the common answers. If you look at that list, they're not that hard to guess. If you don't have a list even, they are easy to guess. There's a couple of DVR that are a little bit more tricky. What they do is they have the six prefix [Indiscernible] and then they are used as web-based pass works -- that prefix is well known and well documented and if you leave your web-based password in default settings then of course it's easy for an attacker to attack you using password.

What we did is an experiment. I took my DVR , I enabled tell net, because by default the -- it didn't have it enabled. I said it all up at 9:30 AM, I open my file -- firewall, that would happen automatically, one is little bit more controlled so at that time I open it up and be much immediately I was being attacks. At 9:38 AM I have the first attempt, they didn't get the password right and then one of the attacks just came in about an hour after I set it up. Someone came in with the correct password, that well-known default password and started to take over the system. This is a little bit about this particular device I use. One problem and oversight by the manufacturer is that they deliver these devices to the consumer with default passwords and services like tell net enabled and exposed. Two years ago we talked to one of the manufacturers that was the big target back then. They actually made a decision after that to produce an updated firmware that was published that longer had telnet enabled. You have to enable it yourself: you can only do that on a specific console that you can attach to the device. You cannot do that via the web haste interface. So essentially someone with remote access would be able -- would not be able to enable telnet. This was a good move by the manufacturer.

Here is a little list of common passwords. Like I said, these are the passwords that I have seen by the users being used, there's about 34 passwords that are commonly used. You will find these passwords and they are by no means a secret. Some of them are actually not documented by the manufacturer that have been been extracted by analyzing the server on these devices. The manufacturer advertises these passwords are certainly known.

After this particular DVR got attacked, what happens next? The attacker uploaded code into the DVR and one interesting thing we saw here -- when we first looked at this two or three years ago, the codes never got [Indiscernible] they were relatively simple. It was somewhat bulky for these DVR's end what was changed since then and its particular the entire code that was used scan for systems and it was only about 1600 bytes. They had a very tight, portion of the code that they were able to upload and the scan rate was about 500 per second trying to scan for new DVR's. In the past we sometimes have seen actually attackers try to use DVR's [Indiscernible] and that was pretty much a big fail because these meteors just don't have the power to actually real -- run real code.

Why do people do that? Lately they have been doing that to assemble these large [Indiscernible]. Hundred 50,000 DVR's were being used and I'm just looking yesterday at one of my [Indiscernible] and a couple weeks I had something like 400,000 different IP addresses that scannedon these particular sensors so very widespread now. Not everything is actually scanned for that comes from a DVR. There's a lot of routers, a ton of these 3G routers, Wi-Fi, Internet access, some the companies that make those in those devices there often the source of these attacks, also little home routers of people using. Often expose because these likely have the ability to monitor the network and make it might while on the road.

With that, let me just move on to the second case. The second case is more about user [Indiscernible] in a sense. I'm going to show how sometimes the technical controls are not always working well but sometimes it's easy to get a sense of security. While we did this experiment I actually picked random malware. This was an attachment, it was obviously malicious, it was a piece of JavaScript , I have not seen any nonmalicious JavaScript lately but anyways, what I did I configured a system up-to-date, I enabled the virus on the system and make sure the virus is up-to-date. I don't believe one tool ran against a particular manufacturer. I could have used another vendor as well and ended up with a very similar result. I set it up, I copied that attachment to the machine and I double clicked on the attachment. The interesting part was I double clicked on the attachment and nothing really happened. So I did noted works. I got pop-ups for my antivirus. They blocked that particular the LR from running, I saw another pop-up that it removed spyware, malware, I saw several pop-ups happening and it took about 15 minutes or so and then when I zoomed out on the screen, I ended up with a picture of perfectly encrypted system thanks to lofty. What happened here? Even though the virus seem to do his job, it didn't. This happens and it's a very common problem that antivirus but not detect the actual JavaScript that does the downloading. This JavaScript is very generic and something I guess you may see an legitimate JavaScript. You have the script call you connect website, download additional software and then run it. This only works if you run the JavaScript on the local machine. This is not work if you run JavaScript on the website with your browser but the JavaScript on the local machine, you run it and as a result able to connect and download the malicious file and then run it. What happened here was antivirus only detects that second stage, it detects that download, that ran somewhere but not perfect. So what happened here is the anti-my water -- anti-malware just keeps trying more and more malicious downloads and eventually one of them will work, one of them will make it past the antivirus and the result is that even though the user kind of did everything right, the only thing the user is running is from the attachment but then again, can we tell you to click on any attachment ever? You probably should of strip that out on the server. Even though there was valid anti-malware running it didn't work, it didn't protect the user.

For years and years I remember way back [Indiscernible - muffled] back then Microsoft [Indiscernible - muffled] but still back then the problem was antivirus is not protect you from the actual [Indiscernible], it only protected you from additional malware being downloaded later and of course there's always some sample that will make it through and if the initial downloader is persistent enough, it will probably figure out what it can download.

In this case it took about 10 minutes, I didn't have a lot of files on that system [Indiscernible - muffled] and that's why it may take a little bit longer to encrypt all these different files. It's actually pretty fast. One thing we run into it often what you will see is that not all the files are actually encrypted. It randomly just goes through and renames all the file, adds some extensions and then encrypt it so some of the files that have that extension, actually still be on [Indiscernible] and that's sometimes a nice thing if you can find some unencrypted files.

What are the lessons? Everybody is under attack. Nobody's really unimportant enough. I think in particular the rent somewhere the attacker have figured out the economics of it. A traditional attack that he yields the data, that data is always valuable to the person that originally had it and people remove the data, they just copy it. And sometimes by copying it they reduce the value of the data. Think about it, all Social Security numbers have already been leaked at some point. So there is not that much money to be made but the one person is going to pay the most of the data, [Indiscernible - muffled] to make money with it.

This is what I have so far. Do you want your questions now or should I wait until the end?

Now sounds great. I think we had one. >> There is one problem about not being able to change these passwords that's certainly true. A lot of these devices is not just one manufacturer. They have these hidden default passwords that are not documented and cannot be changed. Also in the particular DVR I looked at one problem is that the user have ready been prompted and asked to change the password. If you connect the device, you set it up and it just works. The only input you have in this particular case is the mouse. So you have a mouse with an on-screen keyboard and it limits the complexity of the password but by default the keyboard is actually [Indiscernible] only so you have to find a little button, the input field that will turn over to an alphanumeric keyboard but yes, as I mentioned before, the problem is with the manufacturer that delivers these devices. They're typically also wet lab abilities and these devices but actually don't see them exploited much at all. In part because some of the other simpler things with these devices. >> That's used to be most of the questions for now.

Lands is next.

I am ready.

Can you hear me?

Yes. Go ahead.

Okay folks. Welcome to managing your top human risks. For today we are going to take a shift in focus more on the softer human side. A little bit less technical, a little bit more people focus. If you could please go ahead and change the slide. Meanwhile, my name is Lance Spitzner , I am the training director at SANS security Institute so my job and passion is helping organizations around the world built high impact awareness programs. We work with hundreds actually almost over 1000 organizations and I wanted to hear some of the most common lessons learns that we see. First of all what ultimately our goal? Our goal is to help you folks built high impact, mature awareness programs. What you see right here is the security awareness maturity model. This is developed by about 200 security awareness officers about two years ago. This is where you are and where you want to take it. One of them interesting things is I will ask most organizations do you have an awareness program? And they will say yes. Then I will ask do you like it? And they say no. That's where we have a compliance focus awareness program. Programs developed by auditors to check the box. These programs do not change behaviors because they were never designed to. Why is this important? Because I see organizations, institutions, schools, and universities rebooting their programs from the ground up because they want to go beyond just compliance, they want to actually be changing behavior and ultimately long-term, changing culture. And this is having the metrics to change that metrics and behavior. That's what I'm going to briefly talk about today. How to most effectively manage your human risks and move the needle of the maturity of your awareness program just like you see here. So how do we do that? How do we change behaviors? We can't be the only industry out there trying to change behaviors. It turns out we are not. There is a wonderful person out there named BJ Fogg and he is created what he calls the BJ Fogg behavior model . After 20 years of research how to change behaviors, he has created a very simple model. That model is nothing more than right here. Behavior equals motivation, ability, and triggers. With this simple equation for us to change anybody's behavior there is three things called have to be motivated, they need the ability, and they need a trigger for prompt to change behavior. It's not rocket science but when you look at this, it explains a lot and I love the power just because it's so simple. What BJ Fogg is thing is the more motivated somebody is, and or the easier it is to do something, the far more likely to change behavior when they get the prompt. Something that's hard to do or you are not motivated, when it comes time to do the behavior, it fails. This explains a lot for our world and why is he so many awareness programs fail. Problem is this. Most people involved in cybersecurity and cyber awareness proceed security to be very simple. We understand technology, we understand the problem. As a result of the curse of knowledge, what we perceive as easy to do, we then think or perceived easy for others to do. So we are asking people to do all these different things and we think it's easy to do. And then they fail to exhibit those behaviors. For example, passwords. Strong passwords. How hard could this be? All you need is 15 characters, a capital letter, a lowercase letter, a symbol, a number, and then change it every 90 days. This could not be any easier to do. In reality it's very hard. We think people fail. When in many ways it's our community that's feeling because we proceed -- in reality it's very hard. Quite often I tend to find cybersecurity for people awareness is not a motivation ability. People want to be secure, people are smart. The problem is we made it what we think it's easy to do is actually very hard to do. So my talk today is going to be how we can make security simple for the computer user out there?

First of all we really have to engage and ready to start with why? Why is cybersecurity important? What I have found is I worked with hundreds of organizations is to start at the personal level. Think about it pic we use the same technology and universities that we do at home. We have the same risks at schools that we face at home. It's the same behavior. When you focus and remind people how we personally benefit from the training. How not only they're going to secure themselves when they show up for work but also how they're going to be able to secure and create a separate secure home, make the most of the Internet, secure their family and friends. Focus on that personal benefit cost start with the why. Then what we need to do is this, this follows up earlier on what Johannes was saying. We need to make things simple and keep things simple. And we need to keep it short. I find awareness programs fail because we Orwell people with all these do's and don'ts. They cannot remember it all. In fact it busy term for this is cognitive overload. We try to make everybody the ultimate secure operating system and we tried to secure everything as a result we end up securing nothing. So for a variety of reasons what we want to do is identify our top human risks, then focus on just those risks. That takes work. You have to do a human risk analysis. However, fortunately, for you I'm going to give you a starting point. In this webcast we are going to discuss what I feel are the top three most common human risks we are seeing in most organizations today and how to effectively manage them.

It may or may not be the same for you, every institution is a little different but when it comes to the EDU world, these are the three we are seeing the most common.

One of the great ways you can help determine whatever your key risks are is the Verizon DDR report. It's a data-driven report, not emotion driven. If you're not familiar with this call go check it out , it's industry standard in understanding your risk. One of the things they did this year is identify nine different buckets of the most common causes for incidents and then what they did is they broke those down by industry. We take a look at educational, universities, things like that. We see the most common in everything else. These are people like posting data they should not have posted or clicking on things they should not have clicked on. Stolen assets, miscellaneous errors. Do you know what this is? This right here is things like auto complete and emails. Or web apps. Before you start thinking about this you need to have secure developers, that's what they mean by web apps, people will have their logins and passwords compromised and the bad guys are logging in as them. What wonderful here is we have some additional data to support what I'm about to tell you. What I'm about to tell you the three most common human risks we are seeing out there today are Phishing, passwords, and accidental. Let me briefly explain and why are what we should talk about. Once again the whole goal here is we want to effectively manage and change human behavior. BJ Fogg said to do that we have to make it simple. To make it simple we have to focus on a few risk as possible. As we are doing here.

Phishing , to be honest I'm not going to go into Phishing too much. We are all familiar with Phishing, we have all seen it and to me Phishing even includes things like spearfishing, something that prompts you to do something bad. This is a very simple Phishing example, the bad guys once you to click on a link or an attachment to infect your computer or perhaps it is a CEO from base attack where there is no attachment, they're just asking you to do something. Wire transfer, please execute an invoice, submit W-2 form, things like that. In fact, it's actually CEO from technology simply can't stop. There is no URL, there is no attachment, to filter. So in these type of fraud, it is ultimately human. So what can we be doing to address this risk? The key thing is really you want people to identify the indicators of a Phishing attack. What are the most common indicators? A sense of urgency. Getting people to do things they shouldn't do such as bypassing procedures. Something too good to be true. The common lottery. Things like that. We want to make sure they can identify the common indicator and they have to know what to do, what to report and how to report it. Not only to report a Phishing attack, but just as a poorly, if they fall victim to it, do they feel comfortable reporting it or do they feel like there's going to be some type of retribution. Keep -- key things here, we have to make sure they have two know how to protect from a Phishing attack and then what you want them to do. If it's a common one, perhaps just delete it. If it's more advanced, report. Let's shift gears a little bit. Let's talk about passwords.

The Verizon DDR report says that the passwords is one of the key things for incidents and breaches. The reason I'm so passionate about this topic is so many universities do this wrong. This is what a common University will do. Like I mentioned earlier, it's all about complexity. And then not only is about making hard passwords, but then changing it every 90 days. I've never had anybody be able to explain to me why we change the password every 90 days. There's a potential ever so small risk it could potentially mitigate and it's a huge pain and a huge cost to an organization. It's not like I'm the bad guy I'm going to compromise your password and then go oh boy, I have to wait 90 days to use this password. That's not going to happen, they are going to use it right away. So there is a very small amount of changing passwords, small amount of risk that may help mitigate his far overwhelmed by the cost of behavior, the cost and complexity of the cost and pain in people. If you do what I'm about to talk about, changing every 90 days is irrelevant. What we should be teaching people first of all is to protect the password, don't get infected. Things like the ZEUS, malware, that's one of the most common ways passwords get compromised. So to protect your password, don't get compromised. Don't share your password with others. Don't log into an trust systems. This is all about use. No personal questions. People don't realize that's another password. Now where I'm releasing this industry going and I'm so excited is passphrases. We give up on the highly complex passwords nobody can recognize or take forever to typing on your phone, your Xbox, whatever, go to simple passwords, passphrases for going. You have capital letters call you have lowercase letters call you have symbols, you have the question mark punctuation, now you have the most complex password? No. If you had 15 random characters, yet probably it's a little bit better. But remember to change behaviors we have to keep things easy. Far too often people in our world try to create perfect security and that perfect security is extremely difficult. I just scaling it back just a bit and making it easy, we have a huge impact.

Different passwords for different accounts. You're going to need something like a password manager eligibility to write it down. Never write a password down. Well, I can't remember it so what end up happening I set up 184 passwords but I use a password manager and whenever possible dual factor, two-step verification, whatever you want to call it, call it. Michael Kaiser mentioned earlier about a nationwide campaign initiated by the White House and the national cyber security alliance that could not be more exciting. This is the hard job of going what is just one behavior we want everybody in this country to do to be more secure. Think about it. You have the opportunity to ask everyone in the country every university, to change just one behavior, what is going to be? What the White House did and what NCSA did I feel they picked the right behavior. Enable two-step verification. That's part of the lockdown your login campaign that Michael mentioned earlier. Beautiful job of doing the hard work and trying to focus on what's just one thing we need to focus on. Recommend everybody doing that. And then finally I'm always surprised by this. Universities tend to focus on just deliberate attacks and yet it's the accidental that can cause of so much harm also. Trusted employees, staff, faculties, causing harm by simple accidental boo-boos. And an example is auto complete in email. With all the financials for example in accounts payable and he accidentally email your kids soccer coach with all the information. Another thing was losing a device. One of the fascinating things about the Verizon DVI our report is data shows you are 100 times more likely to lose a device then you are to have it stolen. So the awareness programs all about when you're traveling look out for the bad guys. Make sure he doesn't steal your devices. When we should be doing what I call the check. Every time you leave security at the airport, Pat your pockets. You have your wallet, do you have your smart phone, if you have your laptop, check. Leaving the hotel, check. Leaving the airplane, check. We are far more likely to lose that have something stolen so make sure we have those key behaviors.

I really want to start wrapping this up because I know we have limited time. If you are interested more about changing human behavior, and helping really mature the awareness program, here is a couple of resources we have. We have monthly webcasts just an awareness for the awareness community. We have a summit in London, tell your boss you have to learn what the Europeans are doing any to fly out to London. We have also someone presenting from University College of London and then we have a two day course that build on what we just talked about. Lots of free resources including letters and posters at the URL. That wraps things up. Folks, I would like to hand this back over to you.

Wonderful. Thank you very much. Are there questions? Your Highness, I think there is a question in the question box around the Internet presenting many issues about UK government banning smart phones and Apple watches. Any suggestions along those lines?

That's certainly a big issue with this [Indiscernible]. One area that already has become an issue is the fitness -- fitbits. all this data is being collected about you by these devices, and stored in the cloud or wherever, that's a big issue. Now with the article that was more about the possibility of having something like an Apple watch hack and then being used to listen in on cabinet meetings for example. Certainly possible but I have never seen anything like that yet.

We have another question. Regarding the personal questions for authentication big are the questions safe given that they might be easy to guess or find and very hard to possible to change if leaked? With the MSA be safe there for password reset or authentication?

I am not a big fan of personal questions. I think it adds a big layer of complexity and I don't see it as a security. Two-step verification is absolutely the way we need to go. Far more reliable and simpler. And either they asked very simple questions that information is known, what is your mother's maiden name, or some organizations [Indiscernible] if anybody is a United customer, they have questions and they have pre-populated answers we have to choose one of the 10 or 12 preset optional answers. So what I do is this. For my security questions, I make just random answers that the answers are just gibber's, I just type random stuff and I store them in my password manager. So it's just another layer of complexity, something else you have to remember, something that you will most likely forget so in general, let's get rid of them and go to two-step.

Just want to add to this a little bit. One issue I run into with two-step authentication is how do you reset your two-step is if you lose your phone or just update it. You have to update the phone you download the two pack authentication you have to add [Indiscernible]. He had a good two-step reset built into the authentication.

That's a good point. I think one of the organizations that addresses these issues very well Google. You have -- they were the first to adopt two-step verification of the reason I love it is because anybody has a Gmail account. What a great way to introduce people to that whole idea of two-step by starting with Gmail.

Thank you. I think this next question is for Lance. Are there any the differences about how higher Ed approaches information security versus industry sectors?

That's a good question. A couple of challenges. One of the challenges you folks have first of all at university, higher tran15's faculty. You have faculty members that's pulling and $20 million in research and their hearts to touch or maybe you have unions and things like that, the other challenge you have is culture. Culture tends to be not as restricted or let's just say this, if somebody keeps stealing a Phishing assessment in the EDU world as opposed to the fence or government, I would say the biggest difference maybe enforcement. The tolerance for risks for universities maybe a little lower, I'm sorry a little higher, so they make it with a little bit more wiggle room. The other challenge I have higher education tends to have a lower budget, less money, things like that but on the flipside, you can also involve students into helping run your awareness program. So maybe have a graphic design department or an art department in your university, tap into them. Maybe he can vacation department seek and find undergrads who can apply can help you spread the awareness for that. Remember, awareness is not a technical issue. It's really about communication and collaboration.

Thank you. We have a couple more questions. Since so many password resets are done via email, is it a good first step for implementing two factor authentication on a compliant email provider?

Absolutely. We have been talking about this years ago. It's an amazing point. You have all these accounts, you have social media, banking accounts, Apple, I cloud, and they go through what is your email address? And then you have to reset your email address. Well the bad guy compromises your email account, you can then go through and reset all your passwords on your other accounts. So as I mentioned earlier, many of us have Gmail, first thing we should do is enable two-step on our Gmail account because whatever -- whoever asked that question, you nailed it. Our security for different accounts ties back to our primary email account.

Thank you. How safe is it too safe passwords in the cloud with fast pass?

I never used fast lane or fast pass. It really depends on how do you trust them? How do they implement the security of the passwords? In other words, what happens is they don't want you to be able to encrypt anything in the cloud that you. It's encrypted before it ever leaves your computer and goes out into cloud space. That really is a question of how they implemented it. It's just like any other cloud provider for any service but if they have done it right, I was potentially trust it. I use all one password.

In my case one password you can door your passwords database encrypted in dropbox, I cloud, things like that.

Every once in a while he received research Phishing, journals to be pretending to be accredited and researches to send their work with many leads. Which then leads to IP leakage. These are hard to verify and to make our research is aware of it. Any recommendations with this specific type of Phishing.

That one is relatively unique to hire education. It really makes good sense. Remember I talked about earlier Phishing indicators, we want these people to know common indicators of a Phishing attack or in this case , it's maybe not a Phishing attack , but it's a [Indiscernible]. Teach them to specific indicators of one of these emails. I would get some real ones, your institution has been hit with and share them with the faculty and staff. If you can do a Phishing assessment, replicate a real one , use the same words, send it out and then explain to people how their IEP -- IP can be stolen. The millions of dollars of research stolen, the reputation being harmed, things like that. Quite often it comes back to offering -- answering the questions why should I care.

Thank you. Really good feedback. Any last words of wisdom from you guys?

This is Lance. Changing human behavior is simple, we just have to make it simple for people, that's one of the first ways to do that and focus on human behavior as possible.

I actually go back a little bit to the password reset issues and such. If your password reset and there's a lot involved some essential help desk where people have to call to reset the password, realize there almost always [Indiscernible]. It's much better to involve someone like a colleague, a boss, in that process, it's a much easier time authenticating that then someone sitting in another state or other buildings.

Great information. I think we are going to wrap up. We are ending and I just want to thank both of you. On behalf of our attendees, thank you all for joining us today for an informative presentation and conversation. Thank you all to our presenters for joining us from around the web. Before you sign off today, please click on this session evaluation link which you will find at the bottom right-hand corner of your screen. Your comments are very important to us. This session will be archived under the EDUCAUSE website including slides and a complete replay. Please feel free to share it with your colleagues. Share us -- join us for the next live webcast on November 29, 2016. EDUCAUSE is a production of EDUCAUSE higher education technology education. Thank you for joining us today for EDUCAUSE life. Have a great week.

[Event concluded] >>