Phishing: Chapter 2 – Too Legit to Quit: How to Avoid Making Legitimate Campus Messages Look Phishy

HEISC Webinar
February 21, 2018

Chat Transcript

EDUCAUSE Help-Joanna Lyn Grama: Welcome! As we wait for today’s session to begin, please feel free to introduce yourself in the chat.

Will T. (Baylor University): We also have Microsoft's ATP for Office365 turned on for links that arrive from external sources.

Lisa Ross: Ditto Will, but we try to word messages with instructional info as well, when we can.

EDUCAUSE Help-Joanna Lyn Grama: We will be starting in just a moment.

Mark O'Black: We also use ATP at Duquesne University.

Jenny P. (Longwood): Some URL's are filtered to Quarantine if the message also contains a key word

Ken Connelly: We use STUPID Lyris tracking links

Joe D.: Hello. This is Joe Darkoh from NC State University. I work in Business and IT Continuity. Looking forward to today's webinar.

EDUCAUSE Help-Joanna Lyn Grama: If you have any technical difficulties, please post a note in the chat area.

Ben Woelk (RIT): Hi Everyone! Go Awareness and Training!

Cathy Ullman (University at Buffalo): Greetings! A&T rocks!! :)

EDUCAUSE Help-Joanna Lyn Grama: Chat with attendees or ask the speakers a question using this chat area. You can tweet this event using the hashtag: #HEISC

EDUCAUSE Help-Joanna Lyn Grama: The audio recording, slides, and transcript will be available after today’s event from the EDUCAUSE Cybersecurity Program website: www.educause.edu/security

D Dexter: Helps us if we have to change or update hard links behind the scenes.
D Dexter: Helps to market other items on the page containing the link.

EDUCAUSE Help-Joanna Lyn Grama: Have questions for the speakers? Post them here and we will address them during the next Q&A break.

Shawn Cosgrove: At the University of Delaware, we have a website up with guidelines to help users make official University email campaigns more verifiable by recipients, for both official University emails and third-party emails. Here’s the link (it’s safe to click, promise): http://www1.udel.edu/it/help/email/campaigns/safe5.html

EDUCAUSE Help-Joanna Lyn Grama: Thanks Shawn!

Scott Emery (Oregon State): Thank you, Shawn!

Ken Connelly: Here's a BIG difference - When I read an email message, I presume it's fake until proven otherwise. Most of our users take the opposite view, real until proven fake.

Patricia Clay - DeSales University: Great point, Ken

Cassandra Bizzaro: Is anyone else hearing a beep every now and then? Sounds like someone "joining" or something...I turned on/off "chat sounds" and that didn't work. Maybe it's on the presenters end? It's not happening with any pattern that I can tell.

Patricia Clay - DeSales University: How do we move the needle so that users are more skeptical?

Ken Connelly: practice practice practice

Valerie Vogel, EDUCAUSE: @Cassandra - Apologies! It's people joining/leaving the phone line. We will be sure to disable that before the next webinar.

Cassandra Bizzaro: Ah ok - yes, it's very distracting. Thanks.

Dan Deter - NC State DELTA: +1

Ken Connelly: I make it a point to congratulate people on their skepticism when they send me a phishing message. Eventually, that trickles out to others. No other great ideas though.

Patricia Clay - DeSales University: Yes, I agree with your suggestion of practice. We will talk about one way to help them practice later in the webinar :)

M B: We do this ("Verified Messages") at Cornell. However, it becomes a challenge having communications groups across campus to submit them to us prior to sending the messages! :)
Taylor UIUC: Is the UC Davis registered message page available? and/or procedures/setup around that?

D Dexter: Like our campus police notifications, we summarize a message and then direct them to read more at the designated area on our website.

Bryan C. Andregg - UNC-CH: Has anyone A-B tested different techniques like links vs. directions?

D Dexter: So the details are not in the message, they're on the website.

Katie Santo: Hey Cassie, I hear it as well - I think it's people joining

Jenny P. (Longwood): +1 for Ken’s congratulatory approach

Cassandra Bizzaro: @katie santo! Thanks for making me feel not crazy ;)

Sharon: I post detailed security alerts on the Portal in the Security Channel. I send a generic email to all telling them a new alert has been posted:

David Sisk: Ken C, I fully agree. It's slow, but makes clients feel appreciated (and reinforces their skepticism).

Dave Simmons: We use the a phish alert button in outlook to forward messages to us, and thank them for recognizing a phishing email

Valerie Vogel, EDUCAUSE: The Global Cyber Alliance has more information about DMARC: https://dmarc.globalcyberalliance.org/

Patricia Clay - DeSales University: We have not A B tested the approach, just heard the complaints when we do not include links!

Frank Furnari - Boston University: I have to say I have an issue with giving people navigating information to links. We have had enough time to get people to open our messages and click on what we’re saying, that adding more layers makes me worried that fewer people will go there. Also, at a large school, we're not going to get buy-in from everyone at the school, so people will be less likely to follow what we say.

Mckenzie: @Frank, we definitely face the same challenge here at NYU

Bryan C. Andregg - UNC-CH: FF - I share that concern about directions. Everyone wants a TL;DR these days, which would be a link.
Frank Furnari - Boston University: The two things we try to do - never send them a link that goes directly to a login screen and always give them a link that goes to our official "TechWeb" page and then it might be a link to the login page or to a vendor's site.

Patricia Clay - DeSales University: Buy-in is critical on all of these approaches, M B. I love that Cornell has "verified messages"

Shawn Cosgrove: We use SANS as our phishing awareness vendor for monthly test campaigns. Unfortunately, they do not offer DMARC/DKIM signing for their test phish. :(

Ed Murphy (UW Colleges & Extension): DMARC has a heavy technical debt

D Dexter: @Frank, we use multiple channels and check analytics for which is most effective. Our emails are not as effective as some other channels, like social media and word of mouth.

Bill 2: We implemented DMARC on inbound only, see benefits

Shawn Cosgrove: Agree with Ed

Tom M. - Skidmore: +1 for Bill 2

Sharon: I also have tag lines in my email signature: "Security is Everyone's Responsibility" "Verify, then Trust"

EDUCAUSE Help-Joanna Lyn Grama: Don't forget to Tweet your reflections! Tag your Tweets with #HEISC

Sharon: We limit to a very few who can send out mass communications.

Amy 2: haveibeenpwned

Sharon: We use Proofpoint email firewall services

Micki Jernigan: Inbox to report suspected phish mail

michael m: I think O365 does DMARC by default on inbound

Will T. (Baylor University): Mass communications require approval here.

Amy 2: This is used for our security team to identify if email addresses have been used on other company websites that have been compromised.

Jenny P. (Longwood): We’ve got a list of known bad URL's that have been included in phishing. They’re blacklisted on our campus (so if someone clicks they get a specially crafted...
"oops" page - similar to what I've seen phishing simulators use -- we just don't have the buy in to "test" our users

Mike - MSUDenver: It doesn't help when campus departments go out on their own and sign up for marketing tools that spoof our domain.

Adam Arrowood: aka "phish bowl"

Mike - MSUDenver: https://www.abuseipdb.com/

Will T. (Baylor University): Couldn't get buy in for a phishing simulation from our retiring CIO previously...

Sonja - NDSU: Phishing quiz with correct answers if you answer wrong

Sharon: With our security assessment/penetration test we will perform Phishing tests with the users

Tom M. - Skidmore: If you have a web site to look up known phishing, do you put a link to it? :) 

David Sisk: We use "reliability clues." Messages from IT tend to come from me or 2 others; we use a standard footer text; we archive messages on our blog, and we try to put out warnings when we see widely-distributed phishing.

Dave Simmons: One problem we have is campus and hospital use cloud services so telling users to check the link does not work for all services

Sharon: Will soon deploy SANS security training modules for the users

EDUCAUSE Help-Joanna Lyn Grama: @Tom: It's a security riddle!

Mike - MSUDenver: :-)

Julie Goldstein, University of California: We offer some guidance for how to create less phishy emails.

Scott Emery (Oregon State): We're developing a set of best practices and guidelines as part of an email communications security standard for email comms sent from central IT out to the wider university.

Patricia Clay - DeSales University: Mike - MSUDenver, exactly our trouble here

EDUCAUSE Help-Joanna Lyn Grama: Have questions for the speakers? Post them here and we will address them during the next Q&A break.
Bryan C. Andregg - UNC-CH: We're always learning to make legitimate emails just read less phishy.

Patricia Clay - DeSales University: We developed a mass email policy that helped, somewhat, anyway.

Valerie Vogel, EDUCAUSE: UCOP's system-wide guidance – Prevent Emails from Looking Phishy: https://security.ucop.edu/guides/create-less-phishy-emails.html

David Sisk: We will NOT do phishing simulations. No matter how effective they may be, we are worried that they will erode the trust our clients have in us. We need that trust more than we need better phishing education.

Shawn Cosgrove: Here at UD, our phishing simulation program is VERY popular. We ran a contest with prizes during NCSAM with a lot of positive feedback.

Ed Jalinske: Executive support is irrelevant if they're not notifying users that these campaigns will be running at some point.

M B: At Cornell University, we've made it an opt-in, where units/colleges can opt in -- framing it that way and presenting the features made it seem more alluring for leadership -- they ended up coming to us to try it out. Great success so far.

michael m: Not sure real benefit...I think education and examples are good enough as opposed to running a campaign

Shawn Cosgrove: We are able to target units with repeat clickers for additional phishing training.

Mike - MSUDenver: We also do not do phishing simulations, based on concerns about trust. We have very good reporting on spam/phishing and use our incident response process to identify users who need training.

David - Univ. of Kansas: We do quarterly self-phish exercises. We inform ALL recipients a day or two before that the self-phish is coming!

Michael Davis (LETU): David, I had the same concern. My CIO overrode me, did a great job at outreach to other execs and offices, and has helped with follow-up training to the departments that had employees who fell victim to the self-phish

Becky Klein - Valpo: No phishing tests at Valpo. My colleagues have the same concerns about sending links, but we also have users who prefer links over instructions.
Shawn Cosgrove: Our click rate has dropped from ~15% to ~2% after 12 months of phishing simulation.

Becky Klein - Valpo: I'm the sole message-bearer for IT and that seems to help people, because there's one name they know and trust for messaging.

Ken Connelly: Might have buy-in but don't have $$ nor time to do the self-serve choices

Dave Simmons: Using knowbe4 for monthly phishing sims, then got approval for sec awareness training, took almost a year to get approval, could not make mandatory, just consequences for sec failures

Charlie Kulins - Adelphi University: Adelphi has combined self-phish campaigns with informational messaging, tutorials and workshops.

M B: It's all about providing a safe space to learn and encouraging that

Tom M. - Skidmore: Until somebody spoofs you @Becky

Becky Klein - Valpo: @Tom - trust me, that's my biggest professional fear these days

Mike - MSU Denver: It's not about negative consequences for clicking on links. It's the concept of Security trying to "trick" the campus.

Jenny P. (Longwood): fish food ice cream! I like it

Shawn Cosgrove: We gave out Swedish "phish" :) 

Mike - MSU Denver: We are very focused on rewarding those that forward spam and phishing emails to our spam@msudenver group.

JT @ SFSU: When I sent the first simulation exercise I was prepared for negative feedback -- After 6 month there has only been one person complain out of 4,000 and many people have sent messages indicating they really like the training. I do not reveal the names of those that are susceptible.

Tom M. - Skidmore: @Becky - it happened to us

David Sisk: Phish food ice cream and Goldfish crackers - now that's pretty clever!

Becky Klein - Valpo: One question about phishing simulations, how do you control for new patterns and styles of phishing? The scammers are always a step ahead

Tom M. - Skidmore: +1 on Becky's?
David - Univ. of Kansas: By "self-phish" I don't mean looking like an internal message, but rather mimicking a real external phish message.


michael m: Mike-Denver - what types of rewards?

Dave Simmons: KnowBe4 constantly updates their templates, I add new templates into each campaign

Becky Klein - Valpo: @Tom - that's awful that it happened! I do tell people that it's my fear, and I always tell them that it's good to be skeptical.

Mike - MSUDenver: When a phishing campaign hits us, we analyze the response rates, check outbound logs to see who clicked, replied, etc. We get much the same information as a phishing test, with real world data.

Bill 2: Phishing intensify during breaks and holidays

Shawn Cosgrove: Our phishing sim platform allows us to create custom phish messages, so we can design our own phish based on trends we monitor in the news.

David - Univ. of Kansas: WARNING: Don't do a parking related phish message...we found that "parking" is a hot button, third rail issue. :-D

Keir Novik (SFU): There are lots of good comments in the chat window, but it's too hard to read.

Shawn Cosgrove: Agreed David!

Jenny P. (Longwood): +1 Mike - MSUDenver

Bryan C. Andregg - UNC-CH: Parking! Of course that's a hot button. See also: medical benefits, legislative pay increases, paid time off.

Katie Santo: If you click the paragraph icon in the upper right-hand corner of the chat, you can customize the text size in the chat.

Dave Simmons: Also be careful of eviction, sheriff, law enforcement simulations

michael m: Off topic...is anyone using security awareness software [SANs etc.] or home grown on an annual basis
Valerie Vogel, EDUCAUSE: @Keir: We will make the chat transcript available after today's event.

Lisa Ross: We disable and have our clients reset their password before we unlock again.

D Dexter: Does anyone find any correlations with language barriers?

Shawn Cosgrove: We use SANS at UD, Michael.

Shawn Cosgrove: For both training and phishing.

Bryan C. Andregg - UNC-CH: Our CIO spent a good year talking about phish statistics to anyone who'd listen, so people were prepared to trust Security really is trying to help them.

michael m: thx

Dave Simmons: We have noticed some of our users that fell for real phishing emails gave away credentials, they did the training, but were foreign, not sure how much they got out of the training

Shawn Cosgrove: Agreed Bryan, senior leadership support is critical

Janice G.: I'm dealing with this right now. How do I re-roll out the SANS securing the human training without providing link in email? Also I find the automated messages from SANS to be rather spam/phishlike...

Keir Novik (SFU): That's better, thanks!

Mike - MSUDenver: Agreed, Janice.

Mark O'Black: A lot of our users report the SANS email as phishing!

Rose: Janice - I completely agree. The SANS emails are terrible!

Mike - MSUDenver: We dropped SANS STH because of the number of complaints about their email formatting.

Becky Klein - Valpo: So a couple years ago, we had a bizarre phishing scam go around, where there was no link to click, but if people replied to the email, their accts were compromised. We have no idea how it happened, and the email seemed like an innocent "babysitting request"

Shawn Cosgrove: You should be able to customize the SANS emails...

Lisa Ross: My motto for most is if in doubt, delete. No, you did not win a free iPad!!! ;)

9
Becky Klein - Valpo: Our campus is good at recognizing the styles that have happened before, but when a new one comes out, that's when we end up with people who fall for it.

Mike - MSUDenver: The enrollment emails included login information, and links, and raised more complaints than compliments.

Janice G.: We have customized. They still make me uncomfortable...

Scott Emery (Oregon State): Adding a brief instruction above the link might help. Something like, "<- Copy & paste the link below ->

Will T. (Baylor University): We have tons of users say they NEVER clicked a link, but their account still ended up compromised...

Joel Herbert-Edwards: Towson University uses PhishLabs and SANS

Becky Klein - Valpo: No - no one requested acct info at all, it wasn't like any other scam we've seen before.

Sharon: Our SANS training will be available through our Portal so they only need to log into the Portal and we don't have to send out a link in an email.

Patricia Clay - DeSales University: Oh, very strange Becky!

Rose: I would be very interested in the UC Davis Registered Email site & how it works.

Lisa Ross: In the end it takes a combo of technology AND training. Sadly, that is time consuming for a large audience.

Scott Emery (Oregon State): +1 to putting your standards/guidelines behind auth!

Janice G.: Sharon do you have single sign on for SANS? I suppose we could put SANS on our portal even without SSO ability.

Becky Klein - Valpo: I was taking a class and my prof fell for it. I saw the email, it was only text, no links. It was something about "I'm moving to the area, need a babysitter for my kids, can you help?" She replied to try and be helpful & refer them to the "right" person, and ended up with a compromised acct. She provided no personal info whatsoever.

Patricia Clay - DeSales University: We have seen a few applications which *must* send links, like our new payroll application, unfortunately

EDUCAUSE Help-Joanna Lyn Grama: Have questions for the speakers? Post them here and we will address them during the next Q&A break.
Shawn Cosgrove: @Becky: also "tutoring request" phish

Petr Brym: Rose, can you send me a brief e-mail to prbrym@ucdavis.edu about talking more about registering messages so I have your contact info?

Valerie Vogel, EDUCAUSE: Need materials for your campus security awareness campaign? We have 12 months of content developed by our HEISC Awareness & Training volunteers! [https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns#securityawareness](https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns#securityawareness)

Will T. (Baylor University): We have recently seen a job opportunity scam that wasn't phishing but turned into a money laundering scheme...that was "fun"

Bryan C. Andregg - UNC-CH: Our forthcoming challenge is more and more emails from hosted solutions which employee their own URL's and service email addresses. We teach users not to fall for phishes but then ask them to trust an outside service.

Stan - NC State: @Will T. - we've been hit with the same one here in the last several weeks.

M B: How are other universities dealing with third party email services (Constant Contact, Mail Chimp, etc.)?

Will T. (Baylor University): Interesting - it was a personal assistant & a Monster Energy Drink car wrap here

Dave Simmons: Pres of univ and deans use constant contact, still having problems with users submitting as phishing

Jenny P. (Longwood): @M B: Those external messages come in tagged with [Possibly Spoofed] if they attempt to put their Longwood email address in as the "sender" instead of defaulting to the generic Constant Contact/ Mail Chimp/etc.

EDUCAUSE Help-Joanna Lyn Grama: How prevalent is spear phishing against your campus leadership?

Becky Klein - Valpo: We use Emma, and of course all links are masked for marketing data tracking. Makes my job a lot harder, since hovering over those links is useless.

Will T. (Baylor University): Spear phishing seems to come & go, but the president, provost, & VP of HR seem to be popular targets here

Jenny P. (Longwood): and the CFO
Sharon: I tell users when they forward an email to me they are uncertain about - I tell them if you are not expecting it then I would consider it spam and possibly phishing email.

EDUCAUSE Help-Joanna Lyn Grama: Before signing off, please share your feedback on this event at: https://goo.gl/forms/JZ4sDULkJ0SVrxoL2

Shawn Cosgrove: Spear phishing is more prevalent for our researchers, presumably due to their work with CUI and ITAR data.

Katie Santo: Our IT dept has an awareness campaign focused on device security, phishing, etc. They do videos, have quizzes, and they have digital signage across campus. Some content is available here: https://www.nyu.edu/life/information-technology/it-security-and-policies/security-awareness.html

Sharon: We've seen more spear phishing but not just to executives but to all staff.

Will T. (Baylor University): We are trying to get folks to follow our security education social media accounts so we can alert them to phishing emails

Frank Furnari - Boston University: How many of you have started using 2-factor for at least some of your systems? We implemented it on our SAP system a few months after a spearfishing attempt a few years ago.

Will T. (Baylor University): @BearAware on Twitter & BearAware on Facebook

M B: At Cornell University, we have 2FA enabled everywhere for all staff

Will T. (Baylor University): We have over 50 systems behind Duo now & are working on putting on our email

Jen Bellenger (UC Berkeley): We're in the process of rolling out mandatory 2FA for faculty/staff

Mike - MSUDenver: Our execs aren't targeted as often as they're spoofed. A number of recent spear phishes were spoofing the president, asking for information or financial transactions.

Shana Bumpas: We are rolling out Duo at UR, starting with VPN

Joel Herbert-Edwards: We have 2FA for almost everyone

David Alexander: We are thinking about a Phish of the month, or PhisherMan or PhisherWoman of the month to encourage users to report phishes they find. Do you post phishing attempts somewhere where all can see recent exploits?
Katie Santo: We have multi-factor authentication required for all administrators and *I believe* current students. We need it for email and any of our secure services.

David Sisk: Frank, we're a Google school, and we push people hard to enable 2-factor authentication. We are preparing to roll out Duo 2-factor in the coming year.

Dave Simmons: Duo on some systems, trying to get approval for off365, etc.

Mike - MSUDenver: 2FA is coming for us. Testing Duo as well as the Microsoft suite.

EDUCAUSE Help-Joanna Lyn Grama: EDUCAUSE CDS research in 2016 showed that 10% of respondents used MFA for email.

Will T. (Baylor University): We gave them a date to have a device registered, provided video tutorials online, & had tables where they could walk up to get assistance

Kathy Frederick: At Lehigh U. We offer a security awareness video program (SANS Securing the Human), which includes a phishing module and much more. It's incentivized through our employee wellness program, which makes it more appealing to many. [https://ltsnews.lehigh.edu/securing-human-e-security-training](https://ltsnews.lehigh.edu/securing-human-e-security-training)

Mark O'Black: We are in the process of implementing DUO as well.

Will T. (Baylor University): Giving away t-shirts got the students interested

Lisa Ross: Tested MFA, DUO will be better, in my opinion.

Sharon: I've discussed a recent ransomware attack where someone lost all their data due to no back up at an all managers/supervisors meeting. There was an audible gasp in the room. Unfortunately not all managers and executives were present

Bryan C. Andregg - UNC-CH: FF - We're rolling it out across systems now. It's in front of W-2, VPN, Student Financials. Coming soon to O365 - all. First for students, then staff and faculty by Fall.

Patricia Clay - DeSales University: We are just piloting Duo at DeSales

EDUCAUSE Help-Joanna Lyn Grama: Keep an eye out for July 2018 when CDS opens and there will be new a new infosec module!

Katie Santo: To be specific, we're using DUO for our MFA.

Bryan C. Andregg - UNC-CH: We're doing DUO in front of everything but O365 and using Microsoft MFA for that space.
Rose: Is anyone using Microsoft for 2FA?

Sharon: I can only get messages out to students when I'm interviewed by their newspapers.

Scott Emery (Oregon State): We're using DUO as well

Will T. (Baylor University): [https://www.baylor.edu/its/weduo](https://www.baylor.edu/its/weduo)

Shawn Cosgrove: We're using Microsoft and Google for 2FA for all faculty and staff at UDel.


Bryan C. Andregg - UNC-CH: Now, we're looking at MFA settings like device remembering and length of time remembering.

Mike - MSUDenver: MS 2FA is a challenge unless you're using EMS suite and Azure AD.

EDUCAUSE Help-Joanna Lyn Grama: Before signing off, please share your feedback on this event at: [https://goo.gl/forms/JZ4sDULkJ0SVxol2](https://goo.gl/forms/JZ4sDULkJ0SVxol2)

Mike - MSUDenver: The "free" MS 2FA is problematic.

EDUCAUSE Help-Joanna Lyn Grama: A recording of this webinar will be made available after today’s event at www.educause.edu/security

Mike - MSUDenver: Or at least was for us.

Will T. (Baylor University): Some folks in IT tested Microsoft Authenticator but we wanted one single MFA so we waited for Duo to work with O365

Frank Furnari - Boston University: We're using DUO as well, been using it 4(?) yrs

EDUCAUSE Help-Joanna Lyn Grama: If you have questions about future events or suggestions for new topics, e-mail us at security-council@educause.edu

Lisa Ross: MS MFA will be awful for most here. DUO is a more familiar solution.

Will T. (Baylor University): We are not going to go forward with MS MFA Lisa :)

Mike - MSUDenver: Thanks, everyone! Have a great afternoon.
David Williams: If you do determine email accounts are compromised, how deep do you perform forensics? e.g., Is the entire email account history reviewed to determine if confidential information is in mailbox?

Charlie Kulins - Adelphi University: Thank you for a great discussion.

Tom M. - Skidmore: Thanks!

Scott Emery (Oregon State): Thank you!

Nan N: Thank you!

Mark O'Black: Thank you!

Rose: Thank you!

David Alexander: Thanks, great content

D Dexter: Great job everyone, speakers and coordinators!

Lisa Ross: Yes, I heard.

Ed Legaspi/SDSU: Thank you

Shawn Cosgrove: @David depends on the malware analysis

Patricia Clay - DeSales University: Great question David Williams

Neal Fisch (CSU Channel Islands) 2: Thanks Everyone! Great Job!!!

Mary Veres: Would love to get a list of higher ed institutions using MFA across the board

Tom M. - Skidmore: Is this link valid? :) 

Lisa Ross: Great info! Good job!

Janice G.: Thank you.

EDUCAUSE Help-Joanna Lyn Grama: Thank you everyone!

Jenny P. (Longwood): @David Williams: Yes, we run Spirion against mailbox for breach notification
Keir Novik (SFU): Thanks!

Sharon: Thank you!

Joe D.: Thank you!

Linda Ludwig - Grinnell College: Thank you

Shawn Cosgrove: Great presentation, thank you!

Will T. (Baylor University): Thanks

Katie Santo: Thank you

Valerie Vogel, EDUCAUSE: Please feel free to contact security-council@educause.edu if you have further questions!

David Williams: Thanks for the feedback.

José A. Domínguez (UO): Thank you

Valerie Vogel, EDUCAUSE: Thank you all!