Phishing Programs: Chapter 1 – Getting Your Campus Ready for a Phishing Awareness Campaign

HEISC Webinar
April 11, 2017

Chat Transcript

Joanna Lyn Grama, EDUCAUSE: Thank you for participating in today’s HEISC webinar on Phishing Programs: Chapter 1 -- Getting Your Campus Ready for a Phishing Awareness Campaign.

Joanna Lyn Grama, EDUCAUSE: We will get started in a moment. If you have any technical difficulties, please post a note in the chat area.

Joanna Lyn Grama, EDUCAUSE: If you experience any audio issues, please click on the Audio Issues Link in the lower right hand corner. This page will open in your browser, within a new tab or window.

Tamara Bahr: Can you expand the participant list

_ Technical Help, Jody Tracy: Tamara, you can view the list of participants by scrolling down on the right side of the participant list pod.

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

Joanna Lyn Grama, EDUCAUSE: The audio recording, slides, and transcript will be available shortly from the EDUCAUSE cybersecurity website: www.educause.edu/security

Duquesne University: If opportunity presents itself, I am interested in how far schools go into breach investigations from a compromised account due to a Phish.

ScottF - (UAB): UAB has formalized procedures for phishing scam incident response

Keith: Yes - Flowcharted Sink, SIEM, and Seal processes

Sara - IU: We respond by blocking links in phishing messages that are reported. We also scramble passphrases for anyone who clicked those links.

Antonio Crespo (Barnard College): Barnard has formalized procedures for phishing and communications. We also have a different process if a faculty or staff account is compromised.

Mike Sanker: We blacklist offending links and added the text of the message to our phishing archive

Mike Sanker: UPENN
Patricia Clay - DeSales University: We block phishing URLs and disable & communicate to compromised users.

Duquesne University: We do have a process which is scrambling pw & secret questions, blocking links and submitting take down notice if it has a spoofed login page of ours.

Gary Burkholder (CWRU): We block access to phishing links from campus. If the circumstances warrant, we'll email a warning to recipients of the phishing email.

Patricia Clay - DeSales University: For phishing that are very wide ranging, we publicize on Twitter.

jp anderson: We block phishing URLs (and email addresses), and salt false IDs (honeypeeps) into the forms to see where the actors are coming from. We log all IPs sourcing compromised account usage (or that tried the honeypeep).

Ed Jalinske: As the lead who runs phishing programs for the UW-Madison campus, I've received replies to phishing campaigns that contain salty language or are inappropriate. That's something to expect and have a clear plan for responding to.

Mark Liggett: Publicize on twitter, block DNS, reset passwords, add a few other hand-holding steps for executives/sensitive clients. We do track and correlate findings to block root domains on a regular basis.

jp anderson: We maintain a blog (phishing.it.umn.edu) to publish advisories and present examples of phish hitting our campus.

Susan: We are using KnowBe4 and when a phish is reported and it is a phish we will remove it from all mailboxes.

Valerie Vogel, EDUCAUSE:@jp - Nice! Your blog looks similar to some other institutions' "Phish Bowl" pages – Princeton: https://informationsecurity.princeton.edu/phish-bowl; Brown: https://it.brown.edu/about-the-phish-bowl; Cornell: https://it.cornell.edu/phish-bowl

José A. Domínguez (UO): University of Oregon uses Proofpoint in attempt to reduce the number of phishing campaigns that target the university. For those campaigns that get passed Proofpoint we have a procedure to go through that addresses whether messages were just spam, phishing or malicious payload. Each of those trigger its own set of processes. Users can report suspicious messages. And we also DNS filter names and sometimes IP filter.

Joanna Lyn Grama, EDUCAUSE: Chat with attendees or ask the speaker a question using this chat area or tweet using the hashtag: #HEISC

UD: Need to give users simple, actionable, non-technical advice. Users start tuning out if you speak "techese" to them.

Patricia Clay - DeSales University: Great point about "techese"
Patrick Feehan - Montgomery College: Montgomery College uses Proofpoint. We also use PhishMe including the PhishMe Reporter tool - in fact just had our Phishing campaign for our 1700 repeat clickers (SAD!). Every reporter of a phish gets an acknowledging email. We also publish phishing emails to our "Phishtrap" page.

José A. Domínguez (UO): Agreed. It needs to relate to the user. Many times we miss the point when trying to provide awareness

jp anderson: We don’t discourage duplicate reports - we have an email address (phishing@umn.edu) that puts the reports in a special queue

Patricia Clay - DeSales University: We have a spam@desales.edu account that we use, we don’t ask our users to determine, just forward.

Ed Jalinske: We ask users to report to abuse@wisc.edu

David 2: We use one email address and ask customers to send everything to abuse@ku.edu (though we try to educate them on phishing vs. spam)

Becky Klein @ Valpo: Valpo uses Gmail, so it has excellent spam filtering and not much gets through. Phishing does, so most reports we get are phishing. Thus, we encourage people to report phishing but don’t worry much about spam.

ScottF - (UAB): UAB also uses PhishMe reporter tool to aid in reporting. Automatically goes into our ServiceNow ticketing system. We will do a search and destroy on mailboxes to try to keep the scam out of click happy users. Additionally, if someone is using a mobile device they can simply forward it to abuse@ address and the InfoSec and Email team can pull the sample from a mailbox for Incident Response purposes.

scott: abuse@txstate.edu here at Texas State. One place, one thing to remember.

Patrick Feehan - Montgomery College: We also have an email reporting address for those who cannot use our reporting tool (tool is in development for Office 365) called phishtrap@montgomerycollege.edu

Tim Finley: For our school we only use the helpdesk email address for this, and did not ask the helpdesk or customers to make judgment in defining phishing or spam.

Theresa Semmens: NDSU created a specific email account to report phishing. ndsu.reportaphish@ndsu.edu. We acknowledge the notices and thank the customer and then do some investigation and notification if necessary.

Ed Jalinske: Our abuse reports get triaged through our Cybersecurity Operations Center then usually sent to our IR team
David 2: Question for the group: We use abuse@ku.edu for reporting b/c our ITSO says that is the "industry standard." However, I wonder whether that address is intuitive for customers, or whether it causes confusion with sexual harassment or other types of abuse. Thoughts?

Sara - IU: phishing@iu.edu but it-incident@iu.edu will work also

jp anderson: Our abuse@ works too, but phishing@umn.edu has a custom phishing specific autoreply

Dave Curry (The New School): We also use the helpdesk email address. We ask users to report any "suspicious" emails, which generally gets a good result of phishing being reported and spam not being reported, although a few spam messages slip through.

Susan: We use phishing@mwcc.mass.edu. Abuse covers so many topics, I can see why you wouldn't want to use it.

Susan: When I review phishing emails, it surprises me how many legit emails they send as phishing.

Patricia Clay - DeSales University: It never ceases to amaze me how some people feel that any email they don't want at the moment is suspicious/spam/etc.

Joanna Lyn Grama, EDUCAUSE: Do many of you experience legit messages being identified as phishing messages by the user?

José A. Domínguez (UO): How many institutions have a defined a valid format or identifier for university business communications that they can use to make the university community of what a valid business email looks like?

Susan: Yes - emails from the LMS get flagged all the time Joanna

Ben Woelk -- Rochester Institute of Technology: @joanna--somewhat, but I don't mind that.

Ed Jalinske: Somewhat, yes. But not that frequently. 4-5 times/month at most.

Patricia Clay - DeSales University: @joanna We do see that somewhat, but it's just another opportunity to educate.

José A. Domínguez (UO): @joanna: sadly, yes

Patrick Feehan - Montgomery College: Yes Joanna, but we urge users to err on the side of caution and we get back to them when they send us a legitimate email, to let them know it is legitimate.

jp anderson: We see plenty of badly crafted institutional email reported as spam

Tim Finley: @Joanna Lyn - Yes, often as we are responding (in part due to user education) the customer will identify the validity of the message.
Duquesne University: System generated emails get flagged as spam all the time. Every vendor wants a SPF record, which I don't want to do.

lisa c: Yes, we see legitimate emails being reported as PHISH. Sometimes though, they are written in a way that they do seem suspect.

Will Telfer (Baylor): We try to get folks to send suspected phishing emails to BearAware@baylor.edu (we branded our security education & awareness program as BearAware). However, they sometime email our Helpdesk@baylor.edu account too.

David - KU: Having a "have a defined a valid format or identifier for university business communications" can backfire, because the bad guys only have to mimic that and can, in that case, make the bad email look more legit. My 2 cents, anyway. :-)

Duquesne University: Some vendors want entire class C addresses included in SPF records.

Becky Klein @ Valpo: @Jose - Valpo uses Emma for bulk mailing and all the templates are fairly standardized by our marketing dept. So most messages have that look & feel; therefore spam/phishing really stands out and looks different.

jp anderson: We've seen phishers copy our e-communications template :( 

David - KU: We focus customer education on typical attributes of phishing messages, not how they look different from legit university messages.

Will Telfer (Baylor): Recently we had a phish evolve after we sent a warning out to include our BearAware name in the subject line.

José A. Domínguez (UO): UO = University of Oregon

Becky Klein @ Valpo: We've seen scammers steal logos, but they haven't managed to replicate our templates (so far)

Eric Weakland American U.: Thanks Jose!

Will Telfer (Baylor): Trying to get folks NOT to click links in emails is not proving to be easy even with the phish contains multiple grammar errors, wrong department names, & looks nothing like an official message. We are working on getting them to open a browser & go to the legit site instead...

Mark Liggett: Mouse over - BEFORE clicking

Mark Liggett: When that fails, then look at the URL

lisa c: Agreed, on trying to get people not to click on links.
Erin Fogarty: @jp anderson, CWRU had one also, where the phishers "plagiarized" a phishing awareness email from our CISO. Academic integrity!

Will Telfer (Baylor): The URLs in the last round of phishing didn't match anything - indyracing.com/office/nrn

scott: Does it help to use buttons and such instead of blue text links?

Will Telfer (Baylor): People still logged in & gave away credentials

Esther Silver: No

lisa c: We're working on implementing URL rewrites.

Valerie Vogel, EDUCAUSE: @Erin - Wow!

José A. Domínguez (UO): Digital signatures, anyone?

Joel Rosenblatt: We make the real URL match the apparent URL - Columbia

Ken Connelly: Does your URL rewriting break things like signed messages?

Mark Liggett: Digital signatures are helpful, but fail on internal phishing sources

Joel Rosenblatt: No

James: Any suggestions on a URL rewrite program?

Joel Rosenblatt: Mime defang

Jay: "We make the real URL match the apparent URL" .....how?

José A. Domínguez (UO): Internal phishing sources, eh?

Duquesne University: We are hoping that Advanced Email Protection tools allow us to add our own malicious links

Mark Liggett: Compromised accounts being used to propagate internal phishing

Ken Connelly: Compromised accounts phishing other accounts, Jose

Duquesne University: We are in the middle of an evaluation, which includes re-writes

Will Telfer (Baylor): That has hit us hard since Friday

Tim Finley: Examples of URL rewriting services?
Joel Rosenblatt: If you are using Exchange, there is no way to fix internal phishing - mail is delivered without processing

José A. Domínguez (UO): But, yes, just open more thing. I don't believe there is a silver bullet. Just a collection of tricks, education, procedures

David Sherry, Princeton: "Hover to discover"

lisa c: @James, we're looking at implementing URL rewriting with Cisco IronPort.

Mark Liggett: If your internal clients are sources, look at your email system for multiple accounts being forwarded to a single or duplicate addresses. There is usually more than one internal account that has been popped

Duquesne University: Proofpoint, Mimecast, MS ATP for O365, Cisco IronPort, FireEye

Ken Connelly: Internet skeptics

Joel Rosenblatt: Hover to discover is broken by Proofpoint

Ken Connelly: Utah State guy, now retired

ScottF - (UAB): Hover test is failing the more URL rewrites/redirects become common

Mike Sanker: H2D is also broken by Outlook many times

Patricia Clay - DeSales University: It amazes me that we still have folks that don't know how to hover to discover

Eric Weakland American U.: URL rewrites: Proofpoint, MS-EOP (Advanced)

Tim Finley: Hover to discover on mobile devices?

Becky Klein @ Valpo: But bulk mailing systems don't show you the true URL - it's got all the tracking stuff so users don't know whether to trust even legit links

Sara - IU: It's harder to determine a phishing message on smart phones.

David Sherry, Princeton: On mobile you can teach "press & hold to behold"

Becky Klein @ Valpo: I struggle with whether to include URLs or not in emails when I'm sending them, bc links can often be compromised; but getting a user to manually type a URL to visit a site is just as painful. They want simple, fast, easy.

Mark Liggett: Smart phones often fail on URL reads if the link is crafted properly.

Joel Rosenblatt: David -- do you get paid for these :-)
Eric Weakland American U.: @david - love it lol

Tim Finley: I like it David Sherry, although that does not work on all devices... 'yet'

David Sherry, Princeton: Some is better than none.

Patricia Clay - DeSales University: Clever @david

David Sherry, Princeton: Credit to my former colleague at Brown for the talking points.

UD: By contrast, part of the challenge is getting average employees/community members to believe they're potential targets. "I don't have anything worth stealing" isn't a good defense in the age of SSN-based ID theft, botnets, and advanced intrusions

Cal Frye, CWRU 2: Even if you are only first base, they are on the field

David - KU: With all the issues with the phishing email itself "hover to discover" being thwarted, etc., does it make more sense to focus customer awareness on what NOT to do if they click? For example, if they clicked and sent to a page asking for user id and password, RUN!!!!!!

jp anderson: ? We can't check "all that apply" in the poll

jp anderson: It doesn't work right if we're supposed to be able to click all that apply

Patricia Clay - DeSales University: We use them as-is but send separate messaging to let folks know to expect it. Recently, we had this with a new payroll firm

lisa c: On third party URLs, if we're involved in the message crafting we'll provide some additional guidance on crafting the message. And we discourage using bitlys

jp anderson: Thanks for the fix

Valerie Vogel, EDUCAUSE: Oops! My bad - I created the poll incorrectly. It's been fixed. Please vote again if you don't mind. :)

Dave Curry (The New School): We encourage official messaging senders to make the link contain the URL (as opposed to "click here") so that hover to discover is easier

Valerie Vogel, EDUCAUSE: Thanks for catching that @jp!

Ben Woelk -- Rochester Institute of Technology: We are in that engagement around direct deposits as well. Trying to leverage it to push multi-factor auth.

Joel Rosenblatt: We rolled out MFA to all persons receiving payment for any access to HR portal

Valerie Vogel, EDUCAUSE: Speaking of MFA/2FA... We encourage you to join tomorrow’s InCommon IAM Online webinar (April 12, 2-3 pm ET). Rich Graves (Carleton & St. Olaf Colleges)
will discuss MFA: Duo and Google 2-Step Deployments Compared. https://www.incommon.org/iamonline/

ScottF - (UAB): Having similar issues with SPF/DKIM/DMARC as we have no clue what marketing, ticketing, credentialing systems the various business units utilize.

lisa c: Our biggest issue would be surveys so we ask them to put in the email that they're being sent to x survey site and it will not require credentials.

Ben Woelk -- Rochester Institute of Technology: @valerie Now it looks like I set that up!

Patricia Clay - DeSales University: We created a bulk mail policy so that folks have to contact IT when using bulk mail services, so we can set up SPF/DMARC etc.

Valerie Vogel, EDUCAUSE: Just good timing, @Ben!

Will Telfer (Baylor): Bulk mail has to have approval by certain areas (department, Provost, HR, etc.) before being sent here

Patricia Clay - DeSales University: This is a very good list!

Patricia Clay - DeSales University: We find that it is hard to convince folks of these things, though. People find it very hard to change their ways

Joel Rosenblatt: We filter all outgoing mail through our spam filters -- great for catching compromised accounts

Valerie Vogel, EDUCAUSE: We have 5 minutes left, so if you have any questions for Sandy and Eric, please post them here.

Patrick Feehan - Montgomery College: Even internal email Joel?

lisa c: We don't whitelist vendors/outside sites.

Patricia Clay - DeSales University: Large vendors are terrible at sending out spam and/or not adhering to opt-outs in my experience

Valerie Vogel, EDUCAUSE: And keep in mind we hope to schedule a follow-up to this webinar soon (chapter 2)!

Joel Rosenblatt: Yes .. all mail going in or out of Google goes through our edge

Valerie Vogel, EDUCAUSE: Before signing off, please share your feedback on this event at: https://goo.gl/forms/lZba6XMAIBMDGN3m1

Becky Klein @ Valpo: Valpo also filters all mail, though we do generally whitelist @valpo.edu accounts. But Google has some great tools that help us manage compromised accounts.
scott: Yes, info security's messaging should be like police alerts

Tim Finley: <joke> "Can I click on that link?!"

Valerie Vogel, EDUCAUSE: A recording of this webinar will be made available shortly at www.educause.edu/security

Patricia Clay - DeSales University: haha @tim

scott: Use helpdesk to offer other advice

Duquesne University: Should we hover over?

José A. Domínguez (UO): Thank you Sandy and Eric

Ben Woelk -- Rochester Institute of Technology: Very nice presentation.

Justin: Feb and Nov Links are not working

Becky Klein @ Valpo: Hover doesn't work in Adobe Connect ;)

Nancy - Univ. of Oregon: Will this chat transcript also be saved?

Elizabeth: Great presentation

Tamara Bahr: Thanks great info

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

Valerie Vogel, EDUCAUSE: Yes, chat transcript will be posted!

David - KU: Thank you all!

Nancy - Univ. of Oregon: @Valerie - Thanks!

lisa c: Thank you for the presentation.

Joanna Lyn Grama, EDUCAUSE: Reminder: Please join tomorrow’s InCommon IAM Online webinar -- April 12, 2-3 pm ET. Rich Graves (Carleton & St. Olaf Colleges) will discuss MFA: Duo and Google 2-Step Deployments Compared. https://www.incommon.org/iamonline/

Valerie Vogel, EDUCAUSE: We can fix the broken links in the slides before we post these on the website. :) Thanks for catching that @Justin

Karen McDowell: Excellent presentation

David Stack U of WI System: The links appear to work if you are not in full screen mode.
Valerie Vogel, EDUCAUSE: Before signing off, please share your feedback on this event at: https://goo.gl/forms/lZba6XMAibMDGN3m1

Eric Weakland American U.: Thank you!!

Kamran Raja: Do you think doing monthly training classes or making videos to show the clients how to spot out phishing email would help?

Jay Lin: Thank you!
Eric Weakland American U.: I want to go back and read the chat for tips for myself - so much good stuff!

UD: Thanks all!

Keir Novik (SFU): Thanks!

Sandy Silk (Harvard): @Kamran - always a great idea!

Marie: Thanks!

Jack Suess: Great job, very interesting!

Duquesne University: Thank you

Patricia Clay - DeSales University: Thank you - look forward to the follow up

Joel Rosenblatt: Thanks -- good presentation

ScottF - (UAB): Thank you!

Kamran Raja: Thank You @Sandy Silk

lisa c: Thank you

Karen McDowell: Thanks

Will Telfer (Baylor): Thank you

Lori Henderson: Thank you!

Patrick Feehan - Montgomery College: Thanks Eric and Sandy!

José A. Domínguez (UO): Thank you Valerie, Joanna

Valerie Vogel, EDUCAUSE: Thanks everyone for joining us today!

jp anderson: Thanks!
Jay Lin: Can we get the chat records?

Valerie Vogel, EDUCAUSE: Yes, @Jay. I will be posting the chat transcript, slides, and recording on our security website by tomorrow: www.educause.edu/security

Justin: Thank you!

Jay Lin: That would be really good. Thanks.