KnowBe4

CASE STUDY

Achieving Real Security Behavior Change at the University of Oklahoma

Ensuring a small city's worth of people know the value of sound cybersecurity practices is no small feat, but IT veteran Randy Moore takes it all in stride.

Moore runs IT cybersecurity training, education and awareness for the University of Oklahoma (OU). Across three campuses, Moore is responsible for deploying security awareness training content to 4,000 faculty, 8,000 staff and 36,000 students; almost 50,000 people in total.

"Using KnowBe4 Smart Groups has helped us introduce cybersecurity training into the academic culture using a phased approach for each audience"

Creating a Security Culture

Moore started his IT and security awareness work with OU at the university's Health Sciences Center and was eventually assigned to run the training program for the entire university starting in 2019. The shift in audience meant a shift in the way he had to think about what, and how, training was delivered to a varied population of faculty, staff and students.

"We collaborate with three different campuses, all in different cities. Each campus has a different business focus and culture," Moore says. "Our biggest challenge has been academia culture."

Close to 50,000 email inboxes, with people of all cybersecurity skill levels and ages, meant he needed a robust approach to security awareness and risk education. Moore had successfully implemented the KnowBe4 security awareness training and phishing platform at the Health Sciences Center to train 5,000 employees and 4,000 students. Once he was tasked with training the whole university, continuing with KnowBe4 was an easy choice because of the depth and quality of the training materials and integration with simulated phishing.

"Using KnowBe4 Smart Groups has helped us introduce cybersecurity training into the academic culture using a phased approach for each audience," Moore says.

From the beginning, Moore's goal was to create a positive cybersecurity culture university-wide. Moore says he sees such a culture as one in which all faculty, staff and students are aware of cyber threats, trained to identify and respond to them, and are motivated to fulfill their respective role in protecting university information and systems from cyberattacks.

Success with Phishing Security Tests

Moore began by deploying a baseline Phishing Security Test (PST) to gauge the Phish-prone™ Percentage (PPP) of the main campus faculty and staff. Initial results of a 13.9% PPP were respectable, with the average baseline for large educational institutions sitting at 28.4%, according to the 2022 Phishing by Industry Benchmarking Report.

After the baseline test came monthly, biweekly and weekly training based on how often users failed phishing tests. Moore also incorporated "just-in-time" training into the phishing tests, which shows users training content as soon as they click on a phishing test. He also had the Phish Alert Button (PAB) installed in the university's email client so users can easily report suspicious emails when they see them.

"Having just-in-time training, if they fail a phish test they immediately receive training, linking those two are really important because they are at risk of becoming victims of real phishing attacks"

KnowBe4, Inc | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com
© 2022 KnowBe4, Inc. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

After several months, Moore saw the PPP for the main OU campus staff drop to the mid 4%, achieving his 4.3% target.

"Having just-in-time training, if they fail a phish test they immediately receive training, linking those two are really important because they are at risk of becoming victims of real phishing attacks," Moore says.

Training Variety Makes It Personal

The variety of content available in the KnowBe4 ModStore makes it possible for Moore to tailor training to different audiences of faculty/staff and students. Moore has delivered specific training based on job roles to faculty and staff while providing general lessons on social engineering to students mixed with vital acceptable use requirements. Moore credits his KnowBe4 customer success manager with providing expert advice on which training content works best for a given situation.

"The ModStore is very large, so it helps to have someone who is familiar with that content and can point me in the right direction," Moore says.

The KnowBe4 platform makes sharing these successes easy, Moore says. He's used the KnowBe4 reporting API to feed phishing campaign results and the organizational risk score into a single dashboard he shares with his CIO and university leadership.

"That's really been a great way to provide transparency to everyone to show specific increases in awareness based on decreased PPPs," Moore says.

PhishER Proves To Be a Time Saver

Ever the innovator when it comes to security awareness and risk reduction, Moore recently worked with his security incident response team to incorporate KnowBe4's PhishER platform into his overall strategy. PhishER is a lightweight Security Orchestration, Automation and Response (SOAR) platform that prioritizes user-reported emails based on threat level.

The OU incident response team uses PhishER to sort through thousands of emails users report using the PAB. PhishER's machine learning capabilities, PhishML, allow emails to be automatically categorized as threats, spam or legitimate, saving Moore's colleagues precious time to address actual threats.

"We have 50,000 mailboxes, [so] whenever we're under attack, it just happens really fast, and speed in our response is really important," Moore says. "Automation was essential because of the volume that we deal with."

Over the initial six-month period after PhishER was brought online, the platform ripped nearly 150,000 malicious emails from users' inboxes before they even had a chance to click on them, Moore says. PhishER's PhishRIP™ email quarantine feature looks at any user-reported message, searches for similar messages across mailboxes, and takes them off the board.

"With a large number of users, I think PhishER is essential to provide feedback and automate responses"

Additionally, Moore and his incident response colleagues have used PhishER to set up automated email responses to users after they have reported an email using the PAB. Users love these messages, Moore says, which tell them whether an email they report was a real phishing attempt, spam or legitimate communication. Some users receive legitimate email from as many as 20 different sources, Moore says, so having PhishER provide backup and automated confirmation of a user's choice to report is vital.

"With a large number of users, I think PhishER is essential to provide feedback and automate responses," Moore says.

Just as with just-in-time phishing training and the PAB, PhishER is showing the benefit of taking a more personal approach that provides positive feedback. Positivity keeps people motivated, which in turn makes everyone want to be part of the same team protecting OU from cyber attacks.

"The motivational factor has to be there for people to actually change their behavior," Moore says.

© 2022 KnowBe4, Inc. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies. 01C08K01