

CASE STUDY

An Education Non-Profit and KnowBe4 – Training the Human Firewall

For more than two decades, a non-profit educational institution has offered a comprehensive, accredited education at the national level. With tens of thousands of alumni, and, through both a physical campus and online instruction, students can earn diplomas and degrees in a host of technical careers.

As an organization that delivers much of its value online, this educational institution understands the online threat landscape and has invested over the years in building out its internal cybersecurity practice. Its IT team has more than doubled over the past five years and the organization has put a dedicated cybersecurity team in place to protect itself and its students.

The Challenge

The educational institution has experienced explosive growth over the past five years. Its IT security analyst remembers that the organization put a formal security team in place three years ago. "We did not have a security awareness training (SAT) program in place. WannaCry had hit globally and we knew that phishing and ransomware attacks were going to continue to grow rapidly. The timing was right to formalize a team and get serious about training our users."

When the team started looking at security awareness offerings, they understood that it was a matter of if, not when, their organization was breached. There had been

"[SAT] was new to our executive leadership and they were concerened that our users would be restrained. We were going to have to show that the need and value of a SAT partner far outweighed the concern about being restricted."

instances of staff members clicking on bad links, but they had been lucky not to have a successful breach.

Now ready to get serious about security awareness, the team had an internal challenge. "This was new to our executive leadership and they were concerned that our users would be restrained. We were going to have to show that the need and value of a SAT partner far outweighed the concern about being restricted."

The educational institution looked at a few different vendors including KnowBe4, which was recommended by the director of IT at the time who had used the platform at a different company. The team was able to secure buy-in from executive leadership by showing them sample phishing and bad password tests.

Changing Mindsets and Behavior

Once approved, it took only about a week for the organization to roll out KnowBe4 to thousands of users. "KnowBe4 integrates with Active Directory, so we literally uploaded everyone and all of their attributes were carried over. We could section it by department and we could tag users and departments where we might want to give extra training. It was extremely simple."

"KnowBe4 integrates with Active Directory, so we literally uploaded everyone and all their attributes were carried over... it was extremely simple."

The IT security analyst ran a baseline phishing test to see how vulnerable the workforce really was. "I know that people are going to make mistakes, but we were all surprised that 34 percent of our users fell for the initial phish."

With a Phish-Prone™ Percentage (PPP) of more than a third of their users, the institution's security team understood that training users was going to be a behavioral shift, so they created a plan to execute against. All new hires receive the Kevin Mitnick Security Awareness Training as part of new hire training. All users are trained once a year and any users who fail phishing tests are retrained right away. The goal is to ensure all users receive training twice a year.

Since the start, it's been important that the trainings are as entertaining as they are educational. "I noticed that KnowBe4 had a phishing template for free pizza in the break room. I thought it was brilliant and it got me hooked on how to engage people. I'm so excited because we are just about to roll out KnowBe4's "The Inside Man" video training, which is so good! It's episodic and engaging, and trains people while pulling them into a storyline."

To reinforce training, the security team issues regular KnowBe4 phishing tests to gauge how well their users can identify false emails.

A Healthy Outcome

Since deploying KnowBe4 three years ago, the educational institution has seen significant improvements to its security posture and has succeeded in shifting the behavior of its users. "In terms of how likely our users are to be phished, our users have learned a lot and know how to protect our organization and themselves." Whereas more than a third of users failed their first phishing test, post-training and testing saw a progressive drop down to single digits.

The organization also noticed its users reporting suspicious emails via the Phish Alert button from within the KnowBe4 platform. "Before, nobody wanted to connect with the security team because it meant they were in trouble or had done something wrong. Now, our users are the most engaged with us they have ever been. With KnowBe4, we have educated our human firewall so that we don't have to use our insurance policy."

The security team achieved its initial goal, which was to train users and reduce risk. But they still hoped to turn around their leadership team which was concerned a

SAT offering would be too restrictive. "Leadership has committed to security and it's been a complete 180 on security awareness training. They get weekly reports and make it a point to ask us how users are performing. Security is no longer a scary topic in our organization."

"Leadership has committed to security and it's been a complete 180 on security awareness training."

Over the past three years, this educational institution has seen KnowBe4 go above and beyond. "KnowBe4 had the complete package for us. The phish testing gives us the data we need to know, the trainings are entertaining and educational, and the platform itself is easy to use and has an all-in-one dashboard." As an unexpected bonus, the security team has been struck by the relationship they have created with KnowBe4. "The rapport that we have with KnowBe4 is something we try to replicate with other vendors. They are responsive and receptive and feel like a part of our team."