KnowBe4
Human error. Conquered.

CASE STUDY Education

Industry
A K-12 Education School District with operations serving 5 counties in Illinois

Customer Profile
- A Unit School District (District 129) in Aurora, Illinois
- Serves Aurora, North Aurora, Montgomery, Sugar Grove, and Batavia Counties
- District spans 15 schools, 12, 500 students and 1,500 staff

West Aurora School District 129

Requirements
- Must protect the district's sensitive data, including student and staff PII
- Educate and train its faculty and administration on the danger of phishing schemes
- Must ensure adherence to The Family Educational Rights and Privacy Act

Product Features Used
KnowBe4 Integrated Security Awareness Training and Simulated Phishing Platform

- Baseline Simulated Phishing Test
- Discovered Phish-prone percentage
- Monthly Phishing and Training Campaigns
- Customized Phishing Templates for Staff

The Customer
West Aurora Public School District 129 ("District 129") is a unit school district in southeastern Kane County, Illinois serving Aurora, North Aurora, Montgomery, Sugar Grove and Batavia. The district spans 12,500 students and 1,500 staff and thus holds an abundance of pristine student data on its servers. Because students often do not have credit records, student identity data is particularly valuable and attractive to hackers and cyberthieves. Being a sought-after target and to ensure adherence to The Family Educational Rights and Privacy Act, it was critical that District 129 put an emphasis on protecting its student data as well as all proprietary and staff data.

The Challenges
In the case of K-12 education, technology adoption is often a bit behind the curve as compared to the public sector. While there are professional consortiums raising awareness of technology and security, unfortunately educational tech departments are often not aggressively staffed nor have the appropriate budget and resources.

Don Ringelestein, CETL, Director of Technology at District 129, knew he needed to put more emphasis on security and phishing. This became even more of a priority in 2016 when District 129 fell victim to a DDoS attack that included weekly attacks and lasted nearly two months. With so much of the District relying on the internet, this was highly problematic for them to operate efficiently and showcased the dire need for improving its cybersecurity hygiene. At the same time, phishing attacks were increasingly plastered all over the news—including a nearby school district that fell victim to a phishing attack and divulged all social security numbers of its staff.

Ringelestein recognized that he needed to ramp up security and phishing, particularly in terms of end-user training. However, like many IT pros, he didn't know exactly where to start in terms of creating a customized security awareness program that would be effective for District 129.

CASE STUDY **Education**

The Answer

After learning about KnowBe4 at an industry conference, Ringelestein quickly engaged with KnowBe4 to get a better understanding of its offerings. The key goals were to create awareness around phishing and teach employees how to properly vet emails.

> ***You can spend a lot of money on firewalls and technology, but there's no device that's going to make you safe from phishing. The only way you can be as safe as possible, is to make sure employees and end-users know what they are doing."***
> *--Don Ringlestein*

District 129 first ran KnowBe4's baseline simulated phishing tests to uncover how susceptible the staff was and to determine a "Phish-prone percentage." Initial results showed that more than a quarter of teachers were phish prone.

Following baseline testing, Ringelestein started to train his staff via KnowBe4's library of educational content. Staff was particularly receptive to the three-minute videos covering a variety of topics such as safe practices using Wi-Fi and USBs. In conjunction with the trainings and overall awareness education, Ringelestein implemented monthly phishing campaigns.

Over the course of five months, District 129 leveraged KnowBe4's hundreds of phishing templates and customized them so they were more appropriately targeting staff.

The Results

As a result of working with KnowBe4, District 129 saw very dramatic and favorable results in only a short time. In a five-month period, monthly phishing rates dropped from 27% to .03 percent. "These results are stunning—we were thrilled to see how quickly the training yielded results," said Ringelestein.

Not only is the staff far more cautious, but teachers have responded very favorably and are open to the opportunity to educate themselves on phishing—tools that they can use even beyond the workplace.

Successful Outcomes

- Phish-prone percentage dropped from 27% to .03% in 5 months
- More security-aware culture among staff
- Positive teacher engagement with training content
- Phishing and training campaigns reinforced cautious vetting of emails

"My staff is excellent at teaching, but aren't as experienced with technology, and they don't have time in their busy days to gain a better understanding of technology and information security. The KnowBe4 Security Awareness Training model was a way to get their attention and their interest. 'You just got had with a phishing email' stands out and would grab anyone's attention!"

Don Ringlestein, CETL
Director of Technology, West Aurora School District 129

KnowBe4, Inc | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com