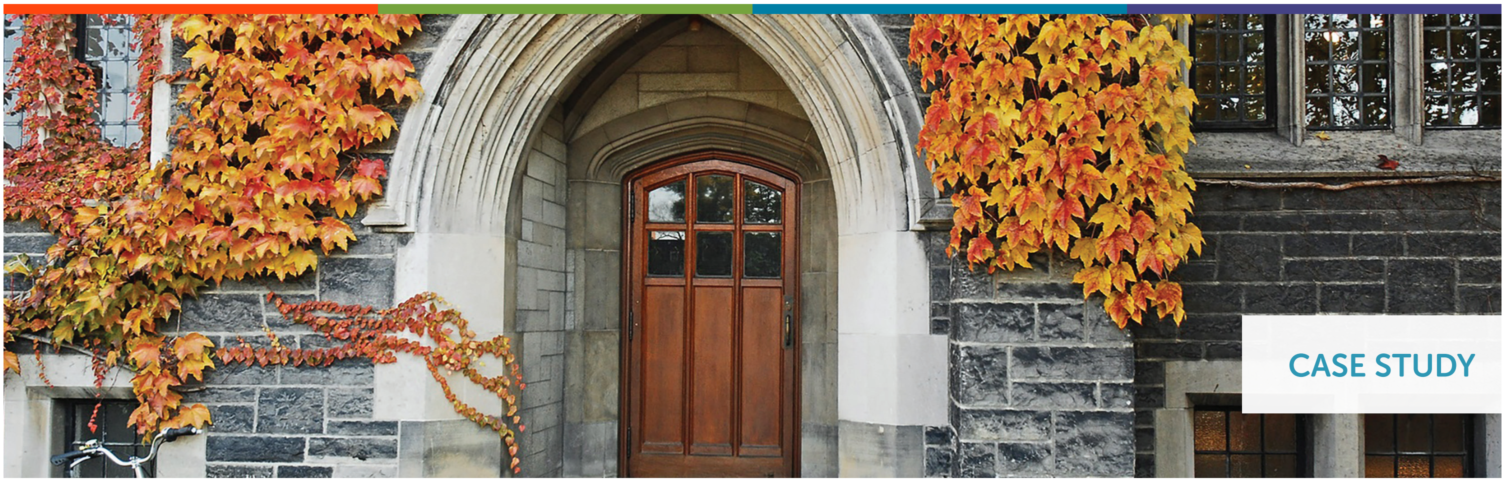


CASE STUDY

Successful Phishing Attacks at a Northeastern US College Drop by 90%

Wombat's Security Education Platform helps administrators reduce threats from phishing, spyware, and viruses

The Challenge

A public college in the Northeastern US found itself at a cybersecurity crossroads. Founded in the 1800s, the liberal arts and sciences school has a population of approximately 7,500 students and 1,400 faculty and staff. In the past, the school had not done a lot of security education. From time to time, emails would be sent to warn the population about bogus links, scam emails, or telltale signs of spam. But there was no online or in-person training specifically dedicated to raising awareness about phishing attacks. With security breaches becoming more dire, administrators recognized that the college's resources were increasingly vulnerable to attack.

In the early days of online threats, "we used to see situations in which someone would have a virus on his or her computer or unintentionally install spyware," said the college's information security officer. "We didn't have a lot of widespread issues." But that changed — and alarm grew — as the years went by and the scale and sophistication of phishing attacks increased. "Our administration realized we needed to do more than just buy another firewall or another appliance. We needed to actually focus on our people."

The situation came to a head when a cybercriminal fabricated an email that appeared to originate from the new dean's email address. The phishing message addressed new policies and staffing changes and asked school officials to update their personal information.

The attack triggered an anxiety response from the school's administration, according to the information security officer. "We recognized that a significant hole in our security was our people, in that they were not very savvy with regard to these issues," he said. "We use an email filter that works fairly well on spam, but it's not as effective at catching phishing messages. Though we manually filter by keywords, a good number of malicious messages still slip through."

The Solution

The college began searching for a security awareness training program that would help its faculty and staff recognize cybersecurity threats and respond appropriately. Administrators consulted with a number of vendors and quickly learned that many companies delivered their training via more basic tools, such as slide decks and short videos, followed by quizzes at the end of each session. But the college wanted more: It wanted a system that was more like the cooperative education its own students receive. The school was searching for a solution that would give users interactive training and hands-on experience with simulated phishing attacks.

Case Study Highlights

Problem

- 5-6 successful malicious phishing attacks every month
- Some staff members believed they would never fall for a phishing attack

Results

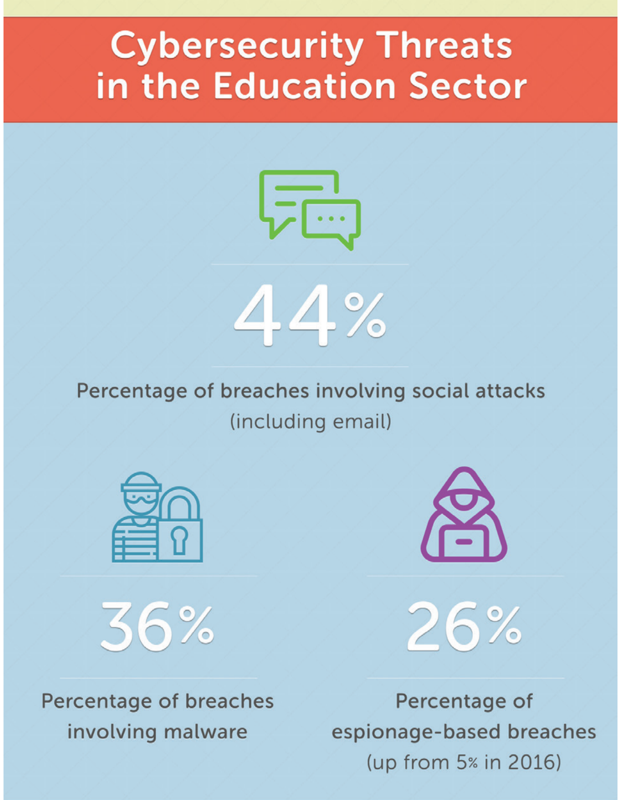
- 90% reduction in successful phishing attacks
- Less spyware, fewer infections
- Rise in proactive reporting and recognized accountability
- Recent sophisticated attack was not successful

wombat™ security
a division of proofpoint.

This quest for a better solution led the administrators to Wombat's Security Education Platform. Wombat's learning management system (LMS) resonated with the college because of its emphasis on both information and education. Because Wombat's methodology focuses on raising awareness and changing behaviors, it gives organizations the best opportunity for a long-term defense against cyberthreats.

Assess, Educate, Measure, Repeat

Wombat's Security Education Platform caught the college's attention due to its simulated phishing attack-prevention results. Wombat's leading-edge, SaaS-based Anti-Phishing Training Suite includes simulated phishing attacks (which allow organizations to assess employees through the use of mock phishing emails) as well as multiple interactive anti-phishing training modules.



Source: *Verizon's 2017 Data Breach Investigations Report*

Security officers began by sending employees a simulated phishing message; results and analysis of click-through rates on the mock attack let the officers gauge the organization's level of vulnerability. Administrators then automatically or manually assigned anti-phishing training modules that employees completed at their convenience.

In each module, users learned through engaging teaching methods, realistic examples, and interactive practice. Whether employees made a mistake or answered correctly, protective behaviors were reinforced. "The interactive nature of the Wombat training, as opposed to a simple quiz at the end, made everything else we looked at seem poor in comparison," explained the information security officer.

Another advantage with Wombat's platform is that organizations can measure results during and after every phase, enabling security officers to identify weaknesses and respond accordingly. The flexibility of the Wombat LMS allows assessment and training cycles to be repeated at targeted intervals, increasing the chances of long-term risk reduction.

Implementation

The college initially launched the Wombat Security Anti-Phishing Training Suite to 300 of its faculty and administrators. Within a year, it had rolled out the product to another 300 staff members. Rollouts began with an announcement to personnel, alerting them to a forthcoming email about training modules they would be asked to complete.

Once training began, the school initiated a series of simulated phishing attacks. Every few weeks, administrators would send out mock phishing emails to see if the training modules were helping faculty and administrators to avoid falling for the scams.

"The interactive nature of the Wombat training, as opposed to a simple quiz at the end, made everything else we looked at seem poor in comparison."

According to the college's information security officer, a number of individuals thought they were immune to phishing threats; they assumed they would never be targeted or that they would know what was happening and not fall for such an attack. "When we phish our users with this product and they fall for it, it breaks that part of their psyche that says, 'I am not going to fall for these things and I am not being targeted.' It makes them more receptive to training," he said.

The Results

According to the college's information security officer, the effectiveness of the Wombat Security Education Platform "has been fantastic." For starters, administrators have learned just how detrimental it can be to the school when sensitive information is compromised. Using Wombat's LMS has raised accountability levels for each staff member and delivered measurable benefits:

90% Reduction in Successful Attacks

Before teaming with Wombat, the college saw its users fall for five to six criminal phishing attacks per month. In a six-month span following training, the school saw the number of successful phishing attacks decrease to three. This represents a 90% reduction in successful phishing attacks from the wild.

"We had a moderately sophisticated phishing email slip through our filters recently," said the information security officer. "The message included a spoofed 'from' address, our logos, and the phone number, and what looked to be the web link of our Faculty/Staff Help Desk. The malicious URL linked to a site that was a clone of our email login page. We didn't have anyone fall for it, though, which is due in no small part to the training we've done."

The college has seen the number of successful phishing attacks decrease by 90%.

Less Spyware, Fewer Infections

The school's help desk has reported a significant drop in spyware and viruses on campus computers. In addition, help desk representatives have had to address considerably fewer support requests, freeing up time for other school matters.

Rise in Proactive Reporting

The school has seen an increase in the number of users reporting actual phishing emails as well as quicker response times and greater awareness of phishing issues. "Users are coming to me and saying they find the training helpful, even when it comes to their personal environments," said the information security officer. "Our users have been appreciative of what they've learned."

Looking Forward

Perhaps the most important result is that the school found a product that not only benefits its users but also holds their interest. Administrators and faculty have valued the real-use case examples that are a part of the training process.

With 600 users fully immersed in Wombat's anti-phishing training, the public college is looking to continue with the rollout of this cybersecurity education by upping the program another notch.

"We are going to get more sophisticated with our training and simulations," the information security officer said. "We don't want to make the simulations look like scams anymore. We want them to look like truly sophisticated attacks."

The college will also look to continually reward those employees who successfully dodge and report the mock attacks. The Wombat platform provides a variety of reporting capabilities that allow security professionals to analyze employee responses to various attack scenarios. For example, administrators can view (and export) different reports that show opens and clicks for each campaign delivered; devices, operating systems, and browsers used to access mock phishing messages; and a list of employees who were most susceptible to the attacks.

"The response to the training has been positive; our administration has been behind us 100 percent," said the information security officer. "In addition to our users being significantly less vulnerable to these scams, the Wombat Security solution is letting the IT staff sleep at night again. We take pride in the fact that our students', our alumni's, and our faculty's data is now more protected due to what we are doing with Wombat."