Successful Phishing Attacks at a Northeastern U.S. 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 U.S. found itself at a cyber security crossroads. Founded in the 1800s, the liberal arts and sciences school — which offers graduate and master's programs — has a population of approximately 7,500 students and 1,400 faculty and staff. Traditionally, 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 describing the state of IT security in the early days of online threats, the college's information security officer said, "We used to see situations in which someone would have a virus on his or her computer or unintentionally install spyware. We didn't have a lot of widespread issues."

But that changed — and alarm grew — as the years went by. "The scale and sophistication of phishing attacks is increasing, and our school started realizing how much security as a whole was important," he added. "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 cyber-criminal 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 effective at catching phishing messages. Though we manually filter by keywords, a good number of malicious message still slip through."

The Solution

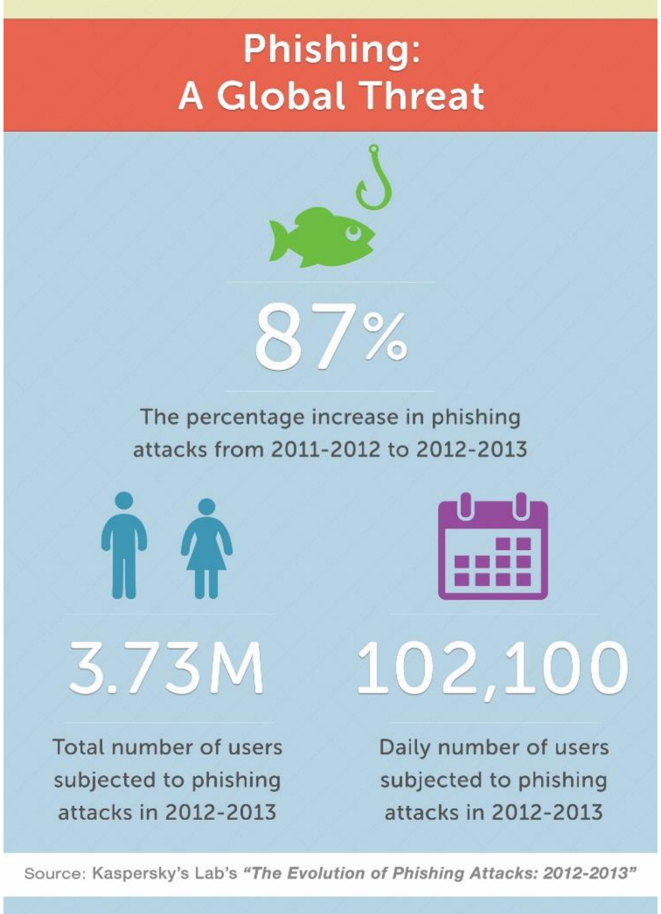
The college began its search for a security awareness training program that would help its faculty and staff recognize cyber security threats and respond appropriately. Administrators consulted with a number of vendors and quickly learned that a great many companies delivered their training via more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

This quest for a better product led the administrators to Wombat's Security Education Platform. Wombat's training methodology resonated with the college because of its emphasis on both information and education. Because Wombat's approach focuses on raising awareness and changing behaviors, it gives organizations the best opportunity for a long-term defense against cyber threats.

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 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 software training modules.

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


Phishing:
A Global Threat
87%
The percentage increase in phishing attacks from 2011-2012 to 2012-2013
3.73M
Total number of users subjected to phishing attacks in 2012-2013
102,100
Daily number of users subjected to phishing attacks in 2012-2013

Source: Kaspersky's Lab's ***"The Evolution of Phishing Attacks: 2012-2013"***

In each module, users learn through engaging teaching methods, realistic examples, and interactive practice. And whether employees make a mistake or answer correctly, protective behaviors are 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 the Wombat platform is that organizations can measure results during and after every phase, enabling security officers to evaluate where weaknesses are and respond accordingly. The flexibility of the Wombat Security Education Platform allows assessment and training cycles to be repeated at targeted intervals, increasing the chances of long-term risk reduction.

Implementation

The college launched the Wombat Security Anti-Phishing Training Suite for 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.

> *“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.”*

Once training began, the school initiated a series of simulated phishing attacks. Every few weeks, administrators sent out mock phishing emails to see if the training modules had effectively prevented faculty and administrators from falling for the scams.

According to the college’s information security officer, there were a number of individuals who thought they were immune to these kinds of 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 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 the Wombat platform has raised the levels of accountability 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 a 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.

"We had a moderately sophisticated phishing email slip through our filters recently. 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," said the information security officer.

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 actual viruses on campus computers. In addition, help desk representatives have had to address considerably fewer support requests, which has freed up time for other school matters.

Rise in Proactive Reporting

The school has also 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 has found a product that is not only benefitting its users but also holding 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 the Wombat Security Anti-Phishing program, the public college is looking to continue with the rollout of this cyber education by upping the training another notch.

“Now that we’ve had people go through training, 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 mocks 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 student’s, our alumni’s, and our faculty’s data is now more protected due to what we are doing with Wombat.”