wombat security technologies
Change Behavior. Reduce Risk.

# A Northeastern College Reduces Successful Phishing Attacks with Wombat's Security Education Solution

## INTRODUCTION

There is no question that cyber threats have become very real and ubiquitous as of late. No one—not even the company CTO or the fresh-faced college freshmen—is immune to scams.

That's because the number of Internet users who faced phishing attacks grew from 19.9 million in 2011-2012 to 37.3 million in 2012-2013, representing an increase of 87 percent, according to Kaspersky Lab's "The Evolution of Phishing Attacks: 2011-2013" report. Moreover, each day during the 2012-2013 timeframe, more than 100,000 Internet users around the world were subjected to such attacks; this is twice the number of intended victims over the previous period.

Phishing attacks come in all forms. Users can be tricked via email messages into clicking on illicit links—that they think will verify account information, for example—that are used to collect confidential data. Others, namely companies, can be targeted in malware-based attacks, in which malware is introduced as an email attachment or downloadable file from a website. And then there are those Web Trojans that pop up invisibly when users log in, and are designed to collect credentials locally and transmit them to the phisher.

Criminals do not discriminate, and individuals and companies become more and more vulnerable to these types of attacks when they lack the edification and understanding about such cyber threats.

## A SCHOOL COMMITTED TO TRAINING

Founded in the 1800's, a public college in the Northeast understood that without proper training and use cases, its faculty and staff would continually be susceptible to online attacks. The liberal arts and sciences school, boasting both graduate and master programs, has a population of about 7,500 students and 1,400 faculty and staff.

Traditionally, the college had not done a lot concerning security education. From time to time, the institution would send out emails warning its population about bogus links, scam emails and telltale signs of spam. But there was no online or in-person training specifically dedicated to raising awareness about phishing attacks.

To describe the former state of security awareness at the school, its 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 alarm grew as the years went by and security breaches became more dire.

"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 CHALLENGE**

In 2012, the need for such training became clear to school administrators when a cyber-criminal fabricated an email that appeared to originate from the new dean's email address. The message addressed new policies and staffing changes and asked school officials to update their personal information.

The phishing attack triggered an anxiety response from administration, according to the school's information security officer. "We recognized that a significant hole in our security was our people in that they were not very savvy with regards to these issues," he stated.

The college began its search for a cyber training program that would bring a new level of awareness to its faculty and staff. It consulted with a number of vendors and quickly learned that a great many companies think that effective training need only include slide decks, short videos and quizzes at the end of each session. But the school wanted more. It wanted a training product that was interactive and would give its users hands-on experience with simulated cyber-attacks. And its quest led it straight to Wombat Security Technologies.

**THE SOLUTION**

Wombat's security education solution immediately caught the attention of the college due to its leading-edge simulated phishing attack-prevention results. Wombat's Anti-Phishing Suite includes PhishGuru®, a software-as-a-service product, which assesses employees through the use of simulated phishing emails, and multiple interactive anti-phishing software training modules which educate employees. The product is built around two core components: assessment and training.

**"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."**

Security officers begin by sending employees a fake phishing message that lets them know how vulnerable they are to cyber-attacks. Next, the people who fall for the attack receive an automatic assignment comprised of 10-minute anti-phishing training modules that they can complete at their convenience. 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 re-enforced.

"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 school's information security officer.

The college began implementing the Wombat Security Anti-phishing Training Suite at the end of 2012 for 300 of its faculty and administrators. By the end of 2013, it had rolled out the product to another 300 staff members. Rollouts began with an announcement to personnel that they would be receiving an email about upcoming training modules that they would be asked to complete. Once training began, the school started to take advantage of PhishGuru simulated attack components. Every few weeks, the school sent out mock phishing attacks to see if the training modules had effectively prevented faculty and administrators from falling for the scams.

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

According to the school representative, there are a number of individuals and companies who think they are immune to these kinds of threats: They assume they would never be targeted or that they would know what is 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," the school information officer said.

**THE RESULTS**

Since deploying the Wombat Security program in 2012, "the effectiveness of the product has been fantastic," said the school representative. For starters, administrators have learned just how detrimental it can be to the school when sensitive information is compromised. Using the Wombat product has raised the levels of accountability for each staff member.

In addition, since using the product, the school has been able to enjoy the following benefits:

- Before teaming with Wombat, the college saw its users fall for five to six criminal phishing attacks a month. Since deploying Wombat Security's solution, so far in 2014, the school has seen the **number of successful phishing attacks decrease to three in the last 6 months**. This represents a 90% reduction in successful phishing attacks.
- The help desk has reported a **significant drop in spyware or actual viruses** on campus computers; the desk has also had to address considerably fewer support requests, which has freed up time for other school matters.

- There has been an **increase in the number of users reporting actual phishing emails** .The school has observed 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,” the school representative said. “Our users have been appreciative of what they’ve learned.”

Perhaps most importantly, the school succeeded in finding a product that not only benefitted its users but also held their interest. Administrators and faculty have valued the real use case examples that are a part of the training process.

**LOOKING FORWARD**

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,” said the rep. “We don’t want to make the simulations look like scams anymore. We want them to look like truly sophisticated attacks.”

The school will also look to continually reward those employees who successfully dodge and report the simulated attacks. The Wombat Security solution provides a variety of reporting capabilities so security professionals can analyze employee responses to various attack scenarios. For example, security professionals can take a look at Campaign Reports, which show opens and clicks for each campaign delivered; Device Type Reports, which show from which devices, operating systems and browsers the phishing email was accessed; and Repeat Offender Reports, which demonstrate which employees, respond the most often.

“The response to the training has been positive; our administration has been behind us 100 percent,” the rep said.

“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,” he added. “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.”