Security Awareness Training Effectiveness Report

Results of a Survey of KnowBe4 Customers and Non-Customers

An Osterman Research Survey Report

Published July 2013
EXECUTIVE SUMMARY

Anti-phishing solutions are critical in protecting an organization from the infiltration of phishing, spearphishing, whaling and other email- and Web-based attacks that can create financial loss, theft of intellectual property and other serious problems. However, no technology-based solution can overcome the problems caused by users who mistakenly or carelessly click on suspect links and thereby introduce malware into the corporate network. Consequently, users remain the first level of a layered defense system in protecting an organization from these attacks and so must receive appropriate Security Awareness Training in order to recognize phishing characteristics and what to do when confronted with them.

Our research demonstrated that KnowBe4’s Security Awareness Training system provides:

• A significant and positive impact in the confidence that security-focused IT professionals have about their employees’ ability to recognize and thwart a phishing attack.

• A much more positive view about improvements in the state of overall email security at the organizations that have implemented it.

OVERVIEW

In order to understand the efficacy of various types of Security Awareness Training, Osterman Research conducted two market research surveys: one survey (135 respondents) was conducted with the Osterman Research survey panel, while the other (113 respondents) was conducted with customers of KnowBe4’s Security Awareness Training solutions. The online surveys were conducted during July 2013. Only decision makers and/or influencers familiar with their organization’s security management and/or Security Awareness Training were permitted to complete the survey.

KEY FINDINGS FROM THE RESEARCH

FIVE APPROACHES TO SECURITY AWARENESS TRAINING

There are five basic types of Security Awareness Training that organizations can employ to educate their users about phishing and related types of attacks:

• The Do Nothing Approach
  The organization conducts no Security Awareness Training.

• The Break Room Approach
  Employees are gathered for a lunch or special meeting and told what to avoid when surfing the Web, in emails from unknown sources, etc.

• The Monthly Security Video Approach
  Employees view short security awareness training videos to learn how to keep the network and organization safe and secure.

• The Phishing Test Approach
  Certain employees are pre-selected, sent a simulated phishing attack, and then IT determines if they fall prey to the phishing attack.

• The Human Firewall Approach
  Everyone in the organization is tested, the percentage of employees who are prone to phishing attacks is determined, and then everyone is trained on major attack vectors. Simulated phishing attacks are sent to all employees on a regular basis.
Results of a Survey Comparing KnowBe4 Customers and Non-Customers

Not surprisingly, our research found that KnowBe4 customers are most likely to use the Human Firewall Approach given that this approach is the one promoted by the company. Non-customers, on the other hand are most likely to use the Break Room Approach or to do nothing, as shown in the following figure.

Security Awareness Approaches in Use

MALWARE INFILTRATION
Our research found that KnowBe4 customers have had a slightly higher level of malware infiltration over the past 12 months – a mean of 7.4 infiltrations versus 6.2. We believe this is the result of the fact that organization will be more likely to implement some sort of specialized Security Awareness Training for its employees if it has had a serious problem with malware infiltration, for example as a result of phishing attacks. Consequently, we believe that the higher level of malware infiltration is a key motivator for adoption of systems like KnowBe4’s, not a result of their use. The fact that 42% of KnowBe4’s customers in our survey are banks or credit unions (as opposed to 17% in the control group) is also probably contributing to this difference, since this is the industry with the highest percentage of phishing attacks.

BENEFITS OF THE HUMAN FIREWALL APPROACH
Our research found that there is a significant difference between KnowBe4 customers and non-customers with regard to confidence in employees’ ability to detect and thwart phishing attacks. When asked to rate their confidence that all employees are well trained to deal with phishing attacks on a scale of 1 (not confident at all) to 100 (very confident), KnowBe4 customers gave a confidence score 29% higher than non-customers. Similarly, when non-customers were asked to rate their employees on the same scale with regard to whether or not employees will refrain from clicking on phishing links, KnowBe4 customers’ confidence score was 40% higher than those of non-customers.
We wanted to determine if the fact that non-KnowBe4 customers have a much higher rate of doing nothing about Security Awareness Training contributed to the much lower confidence scores for non-customers. However, even when eliminating all of the “Do Nothing” responses from both the KnowBe4 customer data set and the non-customer data set, we found only a minor improvement in the confidence scores for each population, as shown in the following figure.

42% of KnowBe4’s customers in our survey are banks or credit unions...the industry with the highest percentage of phishing attacks.
FREQUENCY OF EMPLOYEE TRAINING
Our research also discovered that employees at KnowBe4 customers received substantially more exposure to Security Awareness Training than non-customers – an average of 40 days per year versus 12 days per year, as shown in the following figure. Of course, this does not imply that employees are investing 2.5 times more workhours in the training process, but merely that there are 2.5 times more days per year during which employees of KnowBe4 customers receive some sort of Security Awareness Training in the form of a simulated phishing attack in their inbox.

IT FOCUS ON SECURITY ISSUES
Our research found that the IT departments of both KnowBe4 customers and non-customers focus nearly the same level of effort on security-related issues. The IT staff of KnowBe4 customers spend 24.4% of their time focused on some sort of security-related issue compared to 22.9% for non-customers. This implies a couple of things:

• First, that the Security Awareness Training activities of both survey populations have roughly the same level of impact on the time demands of the respective IT departments. In other words, despite the fact that KnowBe4 customers’ employees receive more days of exposure to Security Awareness Training, this has minimal impact on the resource demands of the corporate IT department.

• Second, that both populations face roughly the same issues with regard to dealing with security-related issues.

IS THE PROBLEM GETTING BETTER?
Perhaps the most telling result from our research was the discovery that KnowBe4 customers are nearly three times more likely than non-customers to find that their phishing problem has gotten better over the past year, while roughly the same proportion believes it has gotten worse, as shown in the figure below. We interpret the significantly greater proportion of “getting better” responses to the efficacy of the Security Awareness Training model provided by KnowBe4.
SUMMARY

KnowBe4’s Security Awareness Training has provided a positive and measurable impact in the organizations that have implemented it. This can be measured in both the confidence level that security-focused IT professionals have in their employees’ ability not to fall prey to a phishing attack, as well as in the perception about improvements in the phishing problem that organizations have experienced.

“I am totally pleased with the training. We have just implemented the product and we have had great feedback from the employees. I can't imagine any SMB not wanting it!”

Information Security Officer at a US-based bank