CASE **STUDY**

Topic: Preventing email phishing attacks in financial sector through security training

TERRANOVA

INSURANCE LENDER PREVENTS PHISHING AND RANSOMWARE ATTACKS THROUGH SECURITY TRAINING

The prevalence of cyberattacks and other security risks are quickly accumulating, threatening both the critical infrastructure and overall performance of many organizations. This is becoming especially concerning in the financial industry, where large amounts of personal and payment information are shared every day.

According to International Banker, cyber criminal target firms in the financial market 300 percent more often than they do any other sector, with email phishing schemes among some of the most commonly used tactics. This is a major issue because, in addition to the reputational damage and litigation fees that can occur, research has also found that consumers are less likely to do business with a firm that has been a victim of a security breach.

Acknowledging the urgent need to safeguard both its internal and external assets, a private mortgage insurance company wanted adapt in accordance to the evolving sophistication of cyberthreats.

Summary

Sector

Financial

Challenge

Provide its employees with security education, awareness and training to minimize risks and reduce rate of employees falling for phishing emails.

Solution

- Phishing simulations
- Customized security awareness campaign

Results

- 100% of users captured
- Increased reporting of phishing attempts

THE CHALLENGE

Although the client already performed audit assessments to ensure its security controls meet the necessary requirements to maintain compliance, it knew it needed to take a more proactive approach to protect its most valuable and sensitive information.

The client had experienced a number of issues with employees falling for phishing emails in the past. Therefore, the company decided that to truly minimize risks, it was crucial to provide its employees with security education, awareness and training.

The goal was to improve user education and to do so in a way that would enable the company to personalize the training materials and course content, thereby making them relevant to the business and easy for the staff to understand.

The company also sought a solution that would be succinct and brief for employees because it would not be effective to make them sit through hour long training. Rather, it preferred the ability to deliver short videos and high impact modules, followed by a quick test on the content. Furthermore, the firm wanted to utilize three to four modules per quarter.

«With attackers, the biggest threat is them gaining access to private data or extracting information through privileged accounts,» *the firm's security compliance specialist explained.* ***«Usually this happens through targeted phishing campaigns or ransomware.»***

THE SOLUTION

After evaluating the credentials and offerings of multiple vendors, the security compliance specialist decided on Terranova Corporation. Its security awareness program, he said, offered a handful of courses that were ideal for the specific needs of the organization. In addition to meeting its budget, the client appreciated the versatility of Terranova's courseware, the different modules that were available for each course and the timing of the videos. But the feature that provided the most value was the ability to edit and customize the training as needed.

To measure the effectiveness of the security awareness solution, the client collected metrics based on the completion rates, how long it look and what the scores were after the training.

Using Terranova's phishing simulation and measurement services, the company sent fake phishing emails out to employees as a pre-assessment tool. This allowed the financial firm to identify the baseline security knowledge of its users. Then, it was able to create a customized awareness campaign that was tailored to address the specific needs of its employees.

«Terranova's product wasn't out of the box or canned,» *the security compliance specialist said.* ***«We were able to make a lot of changes and ensure the courseware was specific to our organization. This was important because we wanted our employees to be familiar with it.»***

THE RESULTS

Because Terranova offered over 25 modules, the client was able to pick the ones that most pertained to its business and that would have the most impact. The easy usability of the video product made for seamless execution, and the editing features allowed the client to tailor the training materials to policies that were specific to the organization.

Only a couple stages into rolling out the phishing program, the company has already been able to track users who didn't score well in the training and target them first in future phases. Through the interactive module content, employees can click on a link and access a PDF to learn more about a specific policy without having to leave the training session.

The company uses the Terranova security awareness training system to target a set percentage of employees each quarter and, in doing so, has been able to capture all of its users this year. Next year, the client plans to proceed with the next stage of the program and continue to use Terranova's education suite of awareness courses and reinforcement tools to further fuel the security initiatives of its organization.