proofpoint.

EMPLOYEE BENEFITS ORGANIZATION REDUCES PHISHING SUSCEPTIBILITY BY 89%

ASSESSMENTS AND INTERACTIVE MODULES SUPPORT ROLE-SPECIFIC TRAINING

THE CHALLENGE

- Test susceptibility to a variety of phishing threat vectors
- Create measurable, long-term improvements in security awareness
- Improve on security management practices

THE SOLUTION

- ThreatSim® Phishing Simulations
- CyberStrength® Knowledge Assessments
- Interactive Training Modules

THE RESULTS

- Lowered average click rates from 19.8% to 2.1% over 15 months
- Improved performance in audits of security management practices
- Increased ability to meet regulations and external requirements

THE ORGANIZATION

A retirement benefits organization for public employees in the western U.S. wanted more insight into its level of phishing susceptibility, so it began researching options for security awareness training.

Proofpoint executed a baseline assessment that revealed a phishing click rate of just under 20%—confirming the association's expectations. But this assessment was just the start of the association's focus on cybersecurity. Ultimately, the IT team was tasked with developing and delivering a comprehensive, organization-wide security awareness training program, built around Proofpoint's assessments and education modules.

THE CHALLENGE

Overall, the association needed a program that tests susceptibility to different phishing threat vectors—like malicious attachments, links, and data entry requests—and helps create measurable improvements over the long term. The important thing, the organization's IT systems manager noted, is to continue to get a better understanding of where vulnerabilities lie, and work to limit end-user risk.

"We recognized the need for security awareness training, and we had complete executive and board-level buy-in before we even started to define the scope of how we would deliver it," said the IT systems manager. "When we started to define the project, we did a project charter with an execution plan and a communications plan.

We defined a program that included [Proofpoint's] security awareness and training products as core components, but they are not the only pieces of our program. We are really comprehensive in our approach and execution."

THE SOLUTION

Phishing and Knowledge Assessments

The association sends quarterly phishing tests via Proofpoint's ThreatSim® simulated phishing tool. Any end user who clicks on a mock phishing email receives a Teachable Moment: "just-in-time" teaching messages that explain the purpose of the exercise and offer brief, actionable tips for avoiding future attacks. Next, ThreatSim's Auto-Enrollment feature automatically sends clickers an anti-phishing training assignment via email.

The organization also uses Proofpoint's Predefined CyberStrength® assessments, which evaluate end users' knowledge across a range of cybersecurity topics. Employees who score below 70% on the Q&A assessments receive additional instruction and guidance. Combining CyberStrength with simulated phishing provides a clearer understanding of end-user knowledge and susceptibility.

Role-Specific Training

The organization assigns mandatory training to approximately 300 employees each quarter. End users are divided into three role-based groups and given the most appropriate training:

1. **Application development and IT group** – Because these employees have more advanced technical knowledge (and are likely to be prime targets for attackers), they are put on a fast track through the program and assigned up to four modules per quarter.
2. **PII group** – These workers regularly handle the personally identifiable information (PII) of employees and benefit recipients, and receive two training assignments per quarter.
3. **PHI group** – These end users handle both PII and protected health information (PHI), so their training also covers HIPAA and HITECH standards. They are assigned two modules per quarter.

The IT systems manager likes the straightforward nature of Proofpoint's SaaS-based Security Education Platform, which he uses to create, manage and track assignments. Administrators can also add custom content to the start and close of each module, using the Training Jackets feature.

The assessment and training tools also have reporting capabilities that allow administrators to track progress and share data and results with stakeholders. The association utilizes these reports and communicates results on a regular basis.

THE RESULTS

The association's baseline click rate was 19.8%. Within 15 months, the rate fell to 2.1%. This 17.7% improvement translates to an 89.39% reduction in susceptibility. Though some initially resisted the mandatory training, users are becoming more responsive. "At the outset, we had probably about 10% of our user population resistant to the training," said the IT systems manager. "But it is improving over time."

The security awareness training initiative has also brought administrative and organizational benefits. The program has simplified reporting to the board and annual external auditing. "We do a security management practices certification every year," said the association's IT project manager. "In the past, before this program, we were getting dinged for not doing enough. But now we're doing really well in all those areas, so that's a big positive for us."

The IT systems manager noted that, without Proofpoint, "it would be very hard to do as comprehensive a program as we do. We absolutely feel there's a big benefit to partnering with an expert to quickly incorporate assessment and education tools," he said. "We've enjoyed using [Proofpoint's] resources as components of our overall security awareness program."

LEARN MORE

For more information, visit proofpoint.com/security-awareness