Employee Benefits Organization Reduces Phishing Susceptibility by More Than 89%

Wombat's assessments and education modules are core components of the organization's security awareness and training program

The Challenge

In early 2015, a retirement benefits organization for public employees in the western United States was researching options for security awareness training. As part of that process, the association wanted more insight into its level of phishing susceptibility.

"That is when we first engaged with Wombat Security," said the organization's IT systems manager. "They were able to perform a proof of concept [POC] for us, which came with our cyber liability policy."

But these assessments were 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 and training program.

The Solution

The POC executed by Wombat revealed a phishing click rate of just under 20%. Although this percentage was higher than the 13% average end-user click rate that was revealed in data gathered for Wombat's *2017 State of the Phish Report*, the assessment exercise reinforced the association's own expectations of its susceptibility.

"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 Wombat'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 association kicked off its program at an annual all-hands meeting, where a professional speaker discussed the importance of cybersecurity education. “We felt this was an effective way to introduce the concept to our employees,” said the IT systems manager.

The association’s program embraces the foundational principles of the Wombat Continuous Training Methodology and includes assessment, education, reinforcement, and reporting activities on an ongoing basis.

Regular Phishing and Knowledge Assessments

The association leveraged the POC findings to embark on quarterly simulated phishing attacks, which are sent and tracked via Wombat’s ThreatSim® phishing tool. The mock phishing emails include Teachable Moments, and these just-in-time teaching messages are displayed to any end user who clicks on a simulated attack.

The Teachable Moments provide context for the users — they explain the purpose of the simulated phishing exercises and offer brief, actionable tips that can help prevent future clicks — but they do not deliver in-depth training. Rather than surprising clickers with an immediate training session, the organization uses ThreatSim’s Auto-Enrollment feature to automatically send clickers an anti-phishing training assignment via email. The users can then complete the training as their schedules allow during the assignment period.

The organization also began using Wombat’s Predefined CyberStrength® assessments, which use a Q&A format that allows the IT team to evaluate their end users’ knowledge of a range of cybersecurity topics. The IT systems manager liked the administrative simplicity of Predefined CyberStrength options, which include a set selection of questions about a specific issue and provide the Auto-Enrollment feature. CyberStrength assessments are used in conjunction with simulated phishing attacks in order to obtain a clearer understanding of end-user knowledge and susceptibility. The goal is for all users in the organization to reach a 70% or higher score on CyberStrength assessments; employees who don’t reach that threshold receive additional instruction and guidance.

CyberStrength Knowledge Assessments are used in conjunction with simulated phishing attacks to give the organization a clearer understanding of end-user knowledge and susceptibility to cybersecurity threats.

Quarterly Training Assignments

The organization assigns at least two mandatory training modules to approximately 300 employees each quarter. End users are divided into three groups, and training is assigned appropriately:

1. **Application development and IT group** – Because these employees have more advanced technical knowledge (and are likely to be a prime target for attackers), members of this group are put on a fast track through the program and are assigned up to four modules per quarter.
2. **PII group** – These workers regularly handle PII of employees and benefit recipients, but they do not handle protected health information (PHI). They receive two training assignments per quarter.
3. **PHI group** – These end users handle both PHI and PII on a regular basis, so their training assignments include information about HIPAA and HITECH standards. Members of this group are assigned two modules per quarter.

The IT systems manager likes the straightforward nature of Wombat's SaaS-based Security Education Platform, which he uses to create, manage, and track assignments. The organization regularly utilizes the Training Jackets feature, which allows administrators to add custom content to the start and close of each module.

> "We're definitely building awareness. There's no doubt about that."
>
> *IT Systems Manager*

"It's easy to set up a training assignment and track completion, which is good. It takes some time to write the reminder notifications and the Training Jackets, but everything else moves pretty quickly," said the IT systems manager. "We appreciate the Training Jackets feature because we are able to easily and regularly remind our employees about our security policies. With the front jacket, we introduce the topic, and we use the back jacket to reinforce how the topic applies to our organization by including our policy."

Regular Reinforcement of Key Principles

Along with Wombat assessments and training, the association believes in regularly reinforcing key principles and keeping their end users informed of relevant news and emerging cybersecurity threats.

"We communicate monthly via our company newsletter, which always includes security awareness factoids," said the IT systems manager. "Plus, the first week of every month, we put up a new security awareness poster in common areas. And once or twice a week, we send out awareness emails that highlight key cybersecurity issues, like ransomware prevention, industry trends, and more."

In the near future, the association will also be rolling out PhishAlarm®, an email client add-in that is included with the organization's ThreatSim Phishing Simulations license. This reporting tool will allow

end users to forward suspicious emails (with headers intact) to the organization's specified inbox(es) with a single mouse click. PhishAlarm will not only reinforce positive behaviors, it will give insights into which employees are able to identify suspicious emails (both simulated and actual), and help the organization reduce the amount of time a malicious message is active within its network.

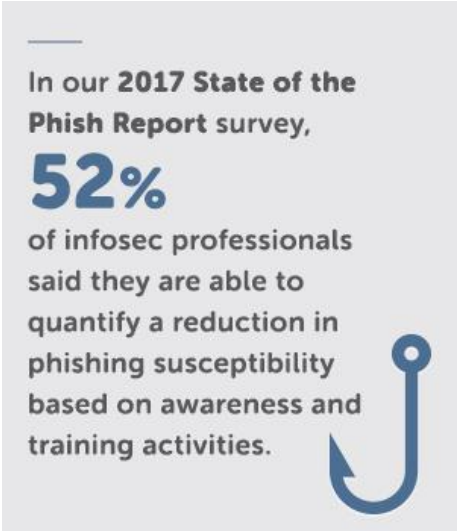
Consistent Tracking and Biannual Reporting

All Wombat assessment and training tools have tracking and reporting capabilities that allow administrators to follow and measure progress, as well as export data that can be shared with stakeholders. The association utilizes these reports and communicates Wombat results and other data points on a regular basis.

"We produce a report twice a year that the information technology director presents to the board, said the IT systems manager. "It includes all we've done since the prior report: our assessments, our training, our awareness and reinforcement activities, and the time we spend on the program."

Measurable Results, Organizational Benefits

Significantly Decreased Click Rates and Phishing Susceptibility



The association's baseline click rate, which was established via the POC, was 19.8%. A year later, the rate had fallen to 5.1%. Just shy of the 15-month mark, the organization registered its lowest click rate of the program: 2.1%. This 17.7% improvement translates to an 89.39% reduction in susceptibility.

The IT systems manager noted, "We're definitely building awareness. There's no doubt about that." But even though the drastically lower click rate shows that positive progress is being made, the organization expects susceptibility measurements to fluctuate over time.

"As we use new tools and run new campaigns, I'm sure we'll see click rates go up and down," said the IT systems manager. "And there's nothing wrong with that."

Overall, the association is focused on delivering 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 IT systems manager noted, is for the association to continue to get a better understanding of where its vulnerabilities lie, and work to limit end-user risk.

Increased Responsiveness to Training Assignments

Though the association's training is mandatory, that doesn't mean all employees are receptive to completing their assignments within the specified timeframes. But administrators do see its users becoming more responsive as the program progresses.

"We don't get a lot of complaints back, I believe because users recognize that it's a mandated initiative. That said, we do still have to chase some people down to complete the training," said the IT systems manager. "That's probably our biggest obstacle, managing user completion and getting up to full participation. At the outset, we had probably about 10% of our user population resistant to the training. But it is improving over time."

Simplified Board Reporting and Auditing Requirements

"Without Wombat, it would be very hard to do as comprehensive a program as we do."

IT Systems Manager

In addition to the numbers-oriented results that the association has experienced, there are administrative and organizational benefits the program managers have realized since kicking off their security awareness and training initiative. The advantages have been noticed by multiple members of the IT staff.

"The program has been a real help in reporting to the Board," said the association's IT project manager, "and it's also been valuable with regard to our annual external auditing. We do a security management practices certification every year. 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 also acknowledged that the program's benefits extended beyond risk reduction and improvements in end-user behaviors. "The program's helped with our liability insurance, and just meeting regulations in general. For all intents and purposes, security awareness and training initiatives are being required by all external entities that our organization deals with."

The IT project manager noted that because cybersecurity and data breaches have become a very public problem, the issues are starting to be widely discussed among organizations and individuals. He feels the association has benefitted by starting their program when they did; with regulations only likely to increase, there will be more focus on security awareness and training. He indicated that Wombat has been a good partner who has enabled the association's program to move forward more quickly.

The IT systems manager agreed that Wombat has been a good fit for the organization. "Without Wombat, 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 Wombat's resources as components of our overall security awareness program."