MASTERCARD MAKES EMPLOYEES FEEL THE IMPACT OF PHISHING SCAMS

Mastercard drew on insights from GP Strategies to transform its annual compliance training from a check-the-box activity into a powerful, engaging e-learning program. In this self-service model, employees experienced the shock of falling prey to phishing scams and learn what they can do to protect themselves, customers and the company.

THE CHALLENGE

Phishing scams cost companies billions every year. Teaching employees how to avoid phishing attacks is key to an effective cybersecurity program.

Long gone are the days of poorly written emails from fictional foreign dignitaries asking recipients for personal information. Today’s phishing scams are much more sophisticated and difficult to recognize, often appearing to come from an employee’s colleagues – and they can happen anywhere at any time with devastating consequences.

In 2015, Ubiquiti Networks, a network technology company, lost $46.7 million to a personalized phishing scam in which the scammer impersonating the company’s finance department convinced employees to transfer money to an account in Hong Kong. In 2016, the Internal Revenue Service issued an alert to its payroll and HR staff warning of a phishing scheme purportedly from executives requesting employees’ personal information.

If just one person is fooled by these scams it can be financially devastating for a company and destroy customers’ faith in the brand. Yet they have become the most common security challenge and the financial services industry is most targeted by these scams.

To combat this growing threat, companies invest millions in cybersecurity but the risk remains that some new piece of malware will land in an employee’s inbox. That’s why the most effective cybersecurity programs include employee training as a last line of defense.

Mastercard recognized that training is a critical component of its cybersecurity strategy and that the content couldn’t be just a run-of-the-mill course. They needed something compelling that would capture employees’ attention and make them realize the risk these phishing scams represent.

One of the key obstacles in teaching about cybersecurity is employees often don’t take it seriously or fail to understand the impact their actions can have. A 2015 survey conducted by an enterprise security firm showed the majority of employees admit that downloading email attachments from an unknown sender was a threat, but that knowledge did not curb their behavior.

To combat this disconnect, the Mastercard Global Talent Development L&D team worked with GP Strategies, a global performance improvement provider of sales and technical training, to develop a course employees wouldn’t soon forget.

THE SOLUTION

Show employees the impact of clicking on phishing scams, then teach them the right approach.

Mastercard set the aggressive goal of reducing the number of employees who opened phishing emails to 15 percent or less – substantially lower than the industry standard of 24 percent. To do that, the company developed an enterprise-wide spear phishing exercise to thwart bad behavior, build cyber acumen and teach employees how to be vigilant about identifying and reporting malicious phishing attacks.

To initiate the learning program (Figure 1), employees received authentic-looking emails but instead of getting a general awareness page when clicking on a suspicious link,
GP Strategies created a program that mimics a hacker removing data from the employee’s computer. “Even though the phishing experience was simulated, to the employee, it appeared to be a real-life event,” said Jim Patton, business development manager, GP Strategies.

The program leaders developed two phishing emails that were sent three times over three months to a randomly selected group of employees making up 25 percent of the general workforce. Each email was constructed with progressive intensity to entice learners to click the phishing link.

The emails were tracked and employee responses were ranked as either:
- Bad: they opened email and clicked on the link.
- Unaware: completely ignored the email.
- Good: did not open or forward the email and reported it as Junk in Outlook.

Immediately following each simulated phishing attack, employees who responded correctly received a congratulatory email from Mastercard’s chief security officer while others received a notice that they had failed to follow security protocol.

“Getting a personal email from the chief security officer really drove home the seriousness of meeting the learning objectives,” said Jawanda Staber, Mastercard vice president, global talent development.

Employees who failed to follow security protocol received a direct link to an e-learning course with an introduction by the chief security officer. The course covered the impact of phishing to the business, how to recognize and avoid phishing scams, and the company’s formal reporting and email isolation procedures.

In addition to online content, the course offered a printable quick reference guide on what to do in the event a phishing email is opened or a phishing link is selected.

**THE RESULTS**

*Mastercard met its target to exceed industry standards and employees report loving the program.*

By focusing on qualitative design, implementation and measurable results, GP Strategies helped Mastercard exceed its ambitious goal through a dramatic increase in employee engagement in the training program (Figure 2).

But the numbers alone don’t tell the whole story. Over the last few years, the company’s L&D team has set out to create new and engaging compliance training that employees really respond to. By that measure, the spear phishing program developed with GP Strategies was considered a huge success.

“Feedback from employees showed they found the course to be innovative, provocative, entertaining and informative,” said Maureen Doran-Houlihan, Mastercard vice president, global talent development and learning and development. In fact, one participant commented: “This is how training should be. I almost wanted it to last longer.”

Cybersecurity is vital in today’s world. Ensuring employees are educated about phishing scams and understand the importance of following steps to mitigate their impact is a key risk management strategy that will help keep the company more secure from attack.