Case Study: Phishing At Henry M. Jackson Foundation

Go Phish Yourself: Non-Profit Tests Employees, Improves Security

How does an enterprise ensure its employees aren't being scammed or duped into cyber threats and understand the difference between malicious and non-malicious content? By phishing their employees and finding where the gaps are, of course.

When Rizwan Jan took on the role of Chief Information Security Officer at the Henry M. Jackson Foundation for military medicine research in May 2016, he quickly realized the organization needed a stronger security posture from the ground up. One of the best ways to do that, Jan said, was to actively bring awareness to the workforce at the foundation, and chose to kick-off a multi-message phishing campaign.

Using a solution provider that specializes in the practice and offers thousands of campaigns and templates to choose from, Jan's security team has been deploying phishing emails year-round, some of which are framed as internal messages while others look to be coming from outside parties.

"The process is a slow drip," Jan said. "The campaign is sent out to employees during the course of two weeks; the entire staff isn't hit at once. When someone clicks on the email, they're immediately alerted that it's a phishing scam and given information on how to avoid it next time."

In the latest exercise, which ran during the month of May, Henry M. Jackson Foundation employees received an email from uber@uber.com with a subject line that stated "Uber: Update Your Account (Link)" that was sent to 1,237 recipients. The campaign saw just 32 clicks, or a 3% click rate, captured in a dashboard from solution provider KnowBe4.

"That was a really, really good rate," Jan said about the campaign. "We've dropped drastically from the initial test, when we were hovering around 27% click rate."

Pictured: A screenshot of the alert message that pops up when employees fall victim to a phishing email.

Image courtesy of Henry M. Jackson Foundation.

That high water mark phishing campaign took place in October of 2016, when Jan's team deployed an email that appeared to come from within the organization, with a subject line of "HJF Email Server Migration Failure, which saw 169 clicks come from 692 recipients, or 26.4%.

An employee who falls for the scam is immediately given a pop-up alerting them about the phishing exercise and explains ways to avoid future attempts. A second-time offender will receive a 10-question cyber security quiz focusing on "IT hygiene," Jan said, and asking them questions about how to best guard their email and data.

"If someone falls for it three times, we'll just call them and have a discussion," Jan said.

The security department will then take the metrics they see on the backend and give the info to the Foundation's executive board for review. There'll be a week-long break, then a new campaign begins.

The practice isn't meant to harm anyone and there are no employment ramifications for anyone who does fall victim to the exercise. Rather, it's about creating awareness and keeping the staff prepared for anything that may come its way.

"It's about continuing the education and making sure everyone knows what's out there and how it can impact them and our organization," Jan said.