TechTarget | Custom Media

Shoring Up the Weak Link in Phishing Defenses: Your People

By David Strom

When it comes to defending your network, many enterprise IT managers tend to forget that it is the people behind the keyboards who can make or break their security posture, and sometimes the people matter more than the machines. Phishing is happening all the time, to every organization. The trick is understanding this dynamic. "I don't know where the next attack is going to come from," says Rick Vanover, director of product strategy for Veeam. "I have to become better prepared."

One way to do this is by having effective security awareness training and overall user education, to help users recognize phishing attacks.

Certainly, the marketplace has recognized the need for better security and anti-phishing training. Companies such as Wombat Security, PhishMe, Phishline, Securecast and Popcorn Training all have either been acquired by major security vendors or received significant investments in the past several months. And, given that phishing attacks continue to plague businesses, having this training in place can make a difference, but only if it done properly.

VEEAM

All the security efforts at keeping the bad guys at bay can be quickly neutralized with a single click of the mouse to activate a piece of malware.

Security experts aren't above shaming those users who click on a phished attachment or can't distinguish between an email from a real CEO and an attacker posing as one. The TV series Mr. Robot has frequent plot points that make an issue out of a user mistake as the cybercriminals worm their way through another episode. It is frustrating: All the security efforts at keeping the bad guys at bay can be quickly neutralized with a single click of the mouse to activate a piece of malware. And there are plenty of security studies which have shown that phishing works and is at the heart of a large share of attacks these days.

The reason why shaming doesn't stop phishing is because it **doesn't motivate people to do a better job**, nor does it help increase their vigilance when it comes to recognizing the difference between a phished and a genuine message. The attackers are getting cleverer with each day: They craft emails that use the same logos and type fonts that are exact copies of the real ones, steal or purchase SSL certificates to make their messages encrypted and pass muster with browser HTTPS checking mechanisms, and employ typosquatting or homographic domain constructions so that the casual observer will mistake them for the real domain names. They spoof the executive email addresses and use tantalizing subject lines that make the message more compelling and realistic, and count on busy office workers to just scan the message and not examine everything carefully, the better to convince the target user to click on them.

Former FBI agent Jeff Lanza calls this appealing to our emotions, and says he has seen this frequently in the phishing attacks that he has analyzed. "Common sense will tell us when we see a scammer's message," he says. "But a victim may not be using common sense at that

moment because they are under stress or are operating at an emotional level reacting to the message content. It is at this point in time when they can be more easily tricked into making bad decisions."

Security awareness training has to be delivered in bite-sized pieces, in regular installments, and reinforced with a variety of learning methods

Even the most skilled security expert only has to be wrong with processing one email, and then the phishing attack has succeeded. Many studies in the past cite that it often is the IT staff that is more prone to click on phishing messages, because they are either overconfident or because they think they are immune. In reality, it is almost impossible to spot one of these malicious emails. So, it's hardly surprising people make mistakes.

It is time for a better solution. We have to get over the shame game and move into a different mode. But that is just a start, and once you move beyond user shaming you need to ensure that you run the best possible security awareness program at your company. Here are a few suggestions:

First, **make it collaborative, not punitive**. A new report based on interviews with several Australian CISOs found that instead of focusing on the number of people who click on malicious links, there's greater value in encouraging people to report suspicious emails and track those who report these incidents. And even if some employees still fall for a few phishing emails, others will have spotted them and alerted the security team that there's something wrong. This way, you have multiple eyes on the target, and users working together to collaborate on recognizing phishing emails and badly formed messages.

Second, **make your training digestible**. Security awareness training has to be delivered in bite-sized pieces, in regular installments, and reinforced with a variety of learning methods and follow-up tests to ensure that the messages were communicated clearly. Don't schedule an all-day class once a year: Spread your training throughout the year and in smaller sessions that won't bury someone in too much information. As attention spans drop, we need frequent reminders and shorter lessons to keep us focused and sharp.

Next, **make it inclusive**. This means designing training for everyone from the very top to the bottom of the corporate ladder. Security awareness has to be designed to engage all levels of employees, including the board of directors. As Lanza has said, "If your board doesn't recognize what is Spectre or Apache Struts, they aren't doing their job and need to learn about these attacks. You have to have board-level focus on cybercrime, otherwise you aren't doing enough to prevent it from happening at your company."

"The diligence required in the ransomware era is going to be part of doing business from here onwards"

"We work with a lot of boards and senior management in setting up security awareness programs. And we go back and see if there's a change in behavior," said Siobhan MacDermott, principal in the cybersecurity practice at Ernst & Young and quoted in this CSO Online blog post. The consultants talk about whether this behavior is modeled by the most senior executives, all the way down. "It can't be just implemented from HR," she said. Security consultant David Froud often has written about how to get your board's attention, and explaining that a CISO needs to explain about security concepts before something goes wrong. A Microsoft report interviewing several Australian CISOs found that "Many company directors aren't adequately informed and place too much faith in the security measures implemented by their organization."

Finally, **pick the right kinds of people to run your training program**. What many enterprises are finding out with their cybersecurity training, communications and awareness programs is to not have them run by technical experts, but by business and marketing specialists, people who can communicate well and can present the technical information clearly. Having these types of backgrounds means that the programs will be designed to get your points across about identifying and preventing phishing, rather than on the bits and bytes about the various exploits.

"The diligence required in the ransomware era is going to be part of doing business from here onwards," says Veeam's Vanover. "You need to stay sharp and continuously train all of your employees to watch out for potential threats."