SECURITY AWARENESS TRAINING: CAN IT CHANGE BEHAVIOR?

KEY ISSUE:

Advances in cognitive science point to more effective training methods.

CISOs should be concerned that security awareness training will not affect end user behavior, and that the training will not improve the security posture of the enterprise— but it doesn't have to be that way. Tremendous advances in understanding how the mind learns provide new insight into improving instructional techniques. Rather than dismissing security awareness training as a low value proposition, consider modernizing your instruction techniques to improve retention of your key takeaways.

In 2004, a select group of cadets at West Point were the subject of an experiment called the Carronade Exercise. The cadets attended four one-hour sessions on computer security awareness; shortly thereafter they were sent an email that was a test phishing attack. Almost 80 percent of the cadets failed by clicking on the hyperlink in this email signed by a fictitious colonel. The tip off? The final line in the signature: "Washington Hall, 7th Floor, Room 7206." The cadets frequently used the building the fictitious officer's room is in; they would have known that that building doesn't have a seventh floor.

Since 2004, this story has been used to justify the conclusion that "money spent on security awareness is money wasted." Others argue that companies should not conduct security awareness training at all. A third perspective says that poor training is worse than no training at all, listing only the shortcomings in existing training, not what would make for more effective training. In 2014, 43 percent of those surveyed report that their organization does not have a training and awareness program.[1] These viewpoints miss the mark.

Two-thirds of incidents of cyber-espionage involve phishing.[2] Organizations of over 10,000 employees spend $3.7 million a year on phishing-related cost alone.[3] According to a Ponemon report, organizations that implement training achieve up to 99 percent improvement in email click rates. Educating your workforce can save you organization from a security incident while reducing cost.

CHALLENGES AND OPPORTUNITIES:

Average Attention Span: 10 Minutes

Research shows that your audience's recall is based on what they think about during the lecture. However, what they think about is not necessarily what is said. The human mind is inclined to wander. A key challenge in any training activity is maintaining your audience's attention.

Take the opportunity to lead the audience's thinking in such a way that participants remain focused on your message.

A second challenge is that technical subjects, such as security awareness, often present a gap between the audience's knowledge and the level required to understand the lecturer's material. Careful consideration of audience creates the opportunity for awareness training with "no end user left behind."

Other challenges exist in reinforcing security awareness training over time, and integrating that awareness into the audience's work day. While your primary training efforts may focus on a single, or even several, classroom based training sessions, there exists an opportunity to move some of the training into the end user's actual workday. This provides the highest likelihood of changing their ability to recognize risks and react appropriately.

THE PATH FORWARD:

Start with the end in mind.

To increase the impact of your effort, decide first what you want the audience to take away from your training. You are more likely to affect their behavior by teaching them about secure behaviors rather than teaching them about security threats. Consider whether your end users need to know that smishing is an attack that comes through their mobile device, as opposed to a phishing attack that comes through their PC. Focus their thinking instead on how to recognize each of those attacks and safe ways to deal with them.

Manage your audiences' focus. What your audience thinks about during training is what they will remember; help them focus on their own behavior by explaining how their actions can either be risky or maintain security. Often, an exercise that requires hands-on activity at the keyboard will distract some of your audience as they deal with their computer, turning their thinking from your point to their system, or even their email.

Students learn new ideas by relating them to things they already know. Ensure your audience has the necessary background knowledge to understand your points. Using jargon the audience is unfamiliar with will lose their attention. Training that is delivered in the context of the end user's work will be more effective at increasing their awareness, improving the retention of the ideas and changing behavior.

Attention spans are short. When your topic expands to more material than can be covered in ten minutes, break your subject into sections. Covering shorter, ten minute segments will help maintain your audience's attention. Transitions can come in the form of a change of topic, a question that leads into new material, or an anecdote that illustrates the topic just covered, or introduces the next.

People enjoy a challenge. Posing moderate problems increases engagement. If the challenge isn't hard enough, it will be dismissed as boring. If the challenge is beyond the knowledge-base of your audience, they will dismiss the problem as too hard. For example, a question about how the audience might identify signs that an email is not legitimate will move their thinking to the details of an email. Their thinking will be engaged as your lecture covers how to recognize and deal with problem email.

Repetition reinforces learning. Find ways to present your concepts after the formal training has ended. The mind needs time to assimilate new knowledge and to be reminded of the material frequently. Relating where your current topic fits into the overall agenda is a good way to reiterate important points. It also helps reorient anyone who might be confused as to how all of your points fit together, or those who are struggling to see the big picture.

Learning in context improves retention. Reinforce training with messaging in the context of the learning. Send messages about email scams or put security reminders on the startup screen of your web conference interface. Remember, the point isn't to have a "gotcha" moment that makes everyone feel as though they failed. Rather, create teachable moments that keep security top of mind without punishing staff.

CALL TO ACTION:

Leverage the latest thinking in cognitive science to improve training.

In the past twenty-five years, more has been discovered about how the mind learns than in the previous 2,500 years. This is a great time to rethink your approach to security awareness training to empower end users to recognize incidents that pose risks in their use of IT. By showing users how to best react to those risks, you can help protect them personally and prevent harm to the enterprise.

1. Ponemon Institute. "Is Your Company Ready for a Big Data Breach? – The Second Annual Study on Data Breach Preparedness" – Retrieved from: http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf
2. Verizon. "2015 Data Breach Investigations Report". Retrieved from: http://www.verizonenterprise.com/DBIR/2015/
3. Ponemon Institute. "The Cost of Phishing and Value of Employee Training". August 2015. Retrieved from: http://info.wombatsecurity.com/hubfs/Ponemon_Institute_Cost_of_Phishing.pdf

1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

12.15 | F1