Why Changing Behavior, Not Sharing Information, Is The Key To Successful Cybersecurity Training

After working on the digital forensic assessments of many cybersecurity breaches, I've learned that hackers are not hacking tech anymore: They're hacking people. This isn't a new concept to anyone familiar with the world of cybersecurity, and it's what led me on a journey to start purchasing cybersecurity awareness training for various teams I ran over the years (something my company offers).

A challenge that I faced years ago is that the cybersecurity awareness training I purchased didn't seem to actually work. What I mean is that, yes, the training was filled with incredible content from leaders in the industry. The employees were tested, and they were given certifications. But they'd still click on links they shouldn't over and over again, not to mention that they were still partaking in a wide range of other cyber no-nos — regardless of how much training I paid for them to take.

I overcame this challenge by understanding the difference between sharing information and changing behavior. When you need to share information — regardless of what information you're sharing — you need to be familiar with your content to do it properly. As an example, if I want to let someone know about an upcoming meeting, the only way I can do that properly is by knowing where the meeting will be located, the date of the meeting, the time, who is going to be there and what the topic of the meeting will be. Only when I understand the content can I share that information properly. And then after I've shared it, I can ask the person I shared the information with to take a test to make sure I did a good job sharing the information and to make sure they understood it. I can ask them to answer questions about the location, the date, the time, and the topic of the meeting, and if the person in question passes my test, I can even go so far as to give them a certification proving that they know whatever information I passed on to them.

For the most part, sharing information in this manner works very well. However, what if in that same example I just gave, the person in question is notorious for not showing up to meetings — and when they do show up, they show up late and unprepared? In that situation, it doesn't matter how well I know my content as the sharer of information. It doesn't even matter if the person in question passes my test and gets a certification saying they know the information I presented. The certification only proves the person in question knew enough of the information to pass the given test at the time, but it doesn't mean anything if it doesn't change their behavior. Whether we're talking about cybersecurity awareness training or anything that requires a move from sharing information to changing behavior, we need to understand that our lesson can't just be focused on the content and the certification. It also needs to focus on individualized content and the psychology of the student.

When it comes to the psychology of the student, I have had great success using a simple formula: why + what + how = a change in behavior.

Whether you are working with an in-class, instructor-led lesson; on-demand online classes or video training modules, the first part of your lesson needs to start with the “why.” Specifically, you should start with why your audience will be interested in the content you’re covering. And that “why” needs to be specific to your audience. Know who your audience is, and make it about their needs, not your needs. As an example, when you’re doing a session on cybersecurity awareness training, don’t tell the employees how important these lessons are to the company; talk to your audience about how learning cybersecurity awareness will better protect them and their families. Start your lesson with stories and case studies on how real this problem is and make it specific to them. Once you’ve established a good base with the “why,” you can continue to bake that message throughout your entire lesson.

The next part of the formula is the easy part. For the “what” and the “how,” you can tell your audience exactly what you need them to do and how you need them to do it. For example, within a cybersecurity awareness lesson, instead of focusing the bulk of the lesson on the history of all things malware, focus on *what* sensitive information is and *how* to protect it. Cover *which* attacks are most common and *how* to spot and avoid them. Discuss *which* environments are the most vulnerable and *how* to better prepare them for attacks. A detailed “what” and “how” combined with a powerful “why” will help you make a great step toward a change in behavior.

When it comes to cybersecurity awareness training, the biggest complaint I hear is “Danny, I bought really expensive training for my employees. The training gave my team access to a wealth of information. They took tests, and they got certified, but no one’s behavior has actually changed. Everyone still clicks on things they shouldn’t!”

If you’re in this boat, the training that you bought for your team was focused on sharing information. In some cases, yes, it provided a wealth of information with really cool-looking certifications — but the training was not at all about the psychology of changing behavior.

There are many places in business where sharing information is exactly what you need. But when it comes to cybersecurity awareness training, if you are not changing behavior, then what’s the point?