Editors: Matt Bishop, bishop@cs.ucdavis.edu
Cynthia Irvine, irvine@nps.edu

Teaching for Conceptual Change in Security Awareness

YUEN-YAN CHAN
The University of Hong Kong

VICTOR K. WEI
The Chinese University of Hong Kong

The ultimate goal of security awareness training is to make trainees adhere to safe computing practices. To meet this goal, training providers put much effort into designing the curriculum for security awareness programs—for example, they tailor highly customized training courses to participants to make them more useful. Gadgets can also help make classes less boring and more interactive, with the goal being that trainees pay more attention to course contents and eventually bring learned practices into their daily work lives.

However, we all know that people behave according to what they understand or perceive. If trainees haven't fundamentally understood the concept of information security, they might practice the security rules being taught but could soon feel the discrepancy between their preexisting knowledge and the newly learned behavior and return back to their original practices. This is what psychologists call *cognitive dissonance*—the discomfort caused by holding two contradictory ideas simultaneously.[1] Therefore, if the goal of security awareness training involves long-term behavioral changes in trainees, training providers should consider pedagogy that addresses the trainees' epistemological beliefs (ideas about the nature of the knowledge and its acquisition).

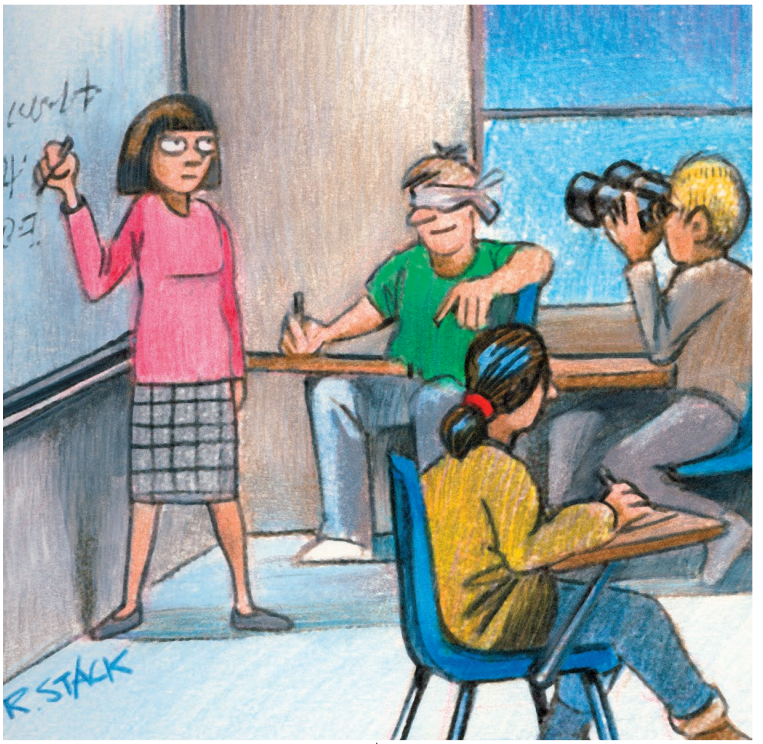
Why Conventional Teaching Doesn't Work

Conventional teaching is unidirectional—teachers teach, and students learn. It assumes teachers can deliver knowledge directly to their students. If students have trouble grasping new concepts, teachers usually apply instructional interventions, such as repeating basic instructions or illustrating concepts with more examples. However, when new knowledge is too advanced or deviates too much from students' existing conceptions, they tend to mend any inconsistencies superficially.[2] Educational psychologists give an example: most children between the ages of four and six believe that the Earth is a flat physical object located in the center of the universe (an example of naïve physics[3]). They develop this idea according to daily observations; when children learn that the Earth is a sphere without any further explanation, they end up with various synthetic models, such as a "disc Earth"[4] (one that's round but also flat at the same time). Without a rigorous approach to addressing the children's existing beliefs, the new information is simply added on top of existing knowledge superficially and does nothing to further comprehension.

This situation shares certain similarities with security awareness training. Most trainees in these classes have nontechnical backgrounds and don't receive formal education in computer networks and information systems. They might have developed an apparent understanding of computers and the Web from daily computer usage, but security training often involves advanced terms and concepts, such as the Secure Sockets Layer (SSL) and data encryption. When trainees receive such content directly without a serious approach to their existing security knowledge and perceptions, the trainee might end up with only a partial understanding of information security or an apparent (sometimes unwilling) adoption of newly learned rules and policies. Again, cognitive dissonance often arises here—trainees might soon feel the discrepancy between their original understanding and these new practices and could eventually return back to their original behaviors.

Conceptual Change

In educational psychology, conceptual change is a process that revises the student's understanding of a topic in response to new information.[5] Instructors have widely applied the conceptual change approach in science educa-



tion since the 1970s. Conceptual change belongs to constructivist pedagogies and has proven to be effective, especially in teaching and learning relatively advanced and complex scientific concepts.

Conceptual change occurs in students when they become dissatisfied with their prior comprehension and find the new information initially plausible, intelligible, and fruitful for future exploration. In general, the conceptual change pedagogical model involves the following steps:[6]

1. Reveal student preconceptions.
2. Discuss and evaluate preconceptions.
3. Create conceptual conflict with those preconceptions.
4. Encourage and guide conceptual restructuring.

The third step is particularly important because it's the turning point between old and new comprehension—that is, a change in understanding occurs at this step. Once this change happens in students, they can generalize the new ideas gleaned from other situations and retain them over time. Going back to security awareness training, if we can find a way to let our participants become dissatisfied with what they use every day and persuade them that the security practices being taught are plausible, intelligible, and meaningful, they'll then undergo a conceptual change and will generalize and apply what they've learned to their everyday lives. This sounds wonderful, but how do we make it happen?

Fostering Conceptual Change with Anomalous Data

The following personal experience might sound familiar. You used to have a certain thought or idea in mind, but one day you learn that the truth is (very) different from what you originally thought. Since then, you look at the same issue from a new angle and extend this new view to other things as well. In psychology, facts or data that deviate from what was expected are called *anomalies*—it's the major cause of dissatisfaction in existing comprehension. Therefore, conceptual change is often fostered by anomalous data.[2]

General computer users usually build their own ideas about computer security according to their daily usage and observations. Eventually, they accumulate a lot of misconceptions as well as their own assumptions. Therefore, instructors can use computer and network security demonstrations as anomalous data for training course participants—these demonstrations can reveal the actual behaviors of computers and networks, which often differ widely from what participants expect. To prove this, we performed a survey of 102 participants attending a security awareness training program at the Chinese University of Hong Kong. These participants come from a variety of nonengineering disciplines, such as medicine, business administration, law, social science, and education. Some questions tested their ideas about information security, and we noticed that a significant portion of the participants had misconceptions about the field.

Misconception One: Confidentiality of Network Traffic

General computer users usually interact with computer networks via user interfaces such as Web browsers and instant messengers. They rarely care about the technical details behind the scenes. One question in our survey asked participants if it were possible for someone to read the data sent between a user's computer and a Web server. The correct answer is "yes": network packet sniffers let eavesdroppers read network traffic quite easily. However, only 56 out of 102 gave the correct answer, whereas 32 and 14 responded "no" and "don't know," respectively. The portion of participants with misconceptions about the confi-

dentiality of network traffic (by responding "no" to the question) is significant.

Misconception Two: Privacy in Email Systems

Email applications are familiar to general computer users. Even though they know nothing about SMTP protocols or the email system's server-side operation, most people know how to compose, send, and receive email messages. In one of our questions, we asked participants if it were possible for someone besides the sender and receiver to read an email's contents. The correct answer is "yes"—SMTP doesn't provide encryption by default, and anyone with system administrator power over the email system can access an email message's contents. However, our results found that only 50 participants answered correctly ("yes"), whereas 31 and 21 responded "no" and "don't know," respectively. Again, the portion of participants with misconceptions about privacy in email systems is significant.

Our results show two examples of general misconceptions about security in daily computer use. The existence of misconceptions indicates the opportunity to apply conceptual change pedagogy in security awareness training. In a subsequent article, we'll present a case study that implements this pedagogy in higher education. □

References

1. D.J. Bem, "Self-Perception: An Alternative Interpretation of Cognitive Dissonance Phenomena," *Psychological Rev.*, vol. 31, no. 3, 1967, pp. 183–200.
2. C. Chinn and W.F. Brewer, "The Role of Anomalous Data in Knowledge Acquisition: A Theoretical Framework and Implications for Science Instruction," *Rev. Educational Research*, vol. 63, no.1, 1993, pp. 1–49.
3. S. Vosniadou, "On the Nature of Naïve Physics," *Reconsidering the Processes of Conceptual Change*, Kluwer Academic, 2002, pp. 61–76.
4. S. Vosniadou and W.F. Brewer, "Mental Models of the Earth: A Study of Conceptual Change in Childhood," *Cognitive Psychology*, vol. 24, 1992, pp. 535–585.
5. J.E. Ormrod, *Educational Psychology: Developing Learners*, Pearson Education, 2006.
6. G.J. Posner et al., "Accommodation of a Scientific Conception: Toward a Theory of Conceptual Change," *Science Education*, vol. 66, 1982, pp. 211–227.

Yuen-Yan Chan *is a postdoctoral fellow in the Faculty of Education at the University of Hong Kong and an adjunct assistant professor in the Department of Information Engineering at the Chinese University of Hong Kong. Her research interests include learning sciences, engineering education, cryptography, and security education. Chan has a PhD from the Chinese University of Hong Kong, with a doctoral dissertation focused on cryptography. She's the founding chair of the IEEE Education Society, Hong Kong Chapter, and is a US National Academy of Engineering Center for the Advancement of Engineering Education new faculty fellow. Contact her at yychan@ie.cuhk.edu.hk.*

Victor K. Wei *is a professor in the Department of Information Engineering at the Chinese University of Hong Kong. His research interests include cryptography, provable security, and coding theory. Wei is an IEEE fellow. Contact him at kwwei@ie.cuhk.edu.hk.*

Interested in writing for this department? Please contact editors Matt Bishop (bishop@cs.ucdavis.edu) and Cynthia Irvine (irvine@nps.edu).