Simplicity is Bliss: Controlling Extraneous Cognitive Load in Online Security Training to Promote Secure Behavior

Jeffrey L. Jenkins, Marriott School of Management, Brigham Young University, Provo, UT, USA
Alexandra Durcikova, Price College of Business, The University of Oklahoma, Norman, OK, USA
Mary B. Burns, Jake Jabs College of Business & Entrepreneurship, Montana State University, Bozeman, MT, USA

ABSTRACT

User-initiated security breaches are common and can be very costly to organizations. Information security training can be used as an effective tool to improve users’ secure behavior and thus alleviate security breaches. Via the lens of learning, working memory, and cognitive load theories, this research examines how to improve the effectiveness of security training through decreasing extraneous stimuli in the presentation of online security training. The authors conducted a realistic laboratory experiment to examine the influence of training with different levels of extraneous stimuli on secure behavior. They found that training presented with low levels of extraneous stimuli improved secure behavior more than training presented with high levels. The results question the effectiveness of elaborate training programs, and rather suggest that simple, direct training modules are most effective.

Keywords: Cognitive Load Theory, Extraneous Stimuli, Information Systems Security, Learning Theory, Security Training, Theory of Working Memory

INTRODUCTION

Life is really simple, but we insist on making it complicated. – Confucius

The news is full of headlines of information security breaches (Google, 2011), and most security compromises and exploits are a result of employees’ insecure behavior (Adams & Sasse, 1999; Davies & Price, 1989; Straub & Welke, 1998). Indeed, the human is often referred to as the weakest link of security (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009), and human-caused security breaches can be very costly to organizations (Goel & Shawky, 2009). Thus, an important area of research is to explain how to improve users’ secure behavior, defined as users’ compliance with their organization’s security policy (Jenkins, Durcikova, Ross, & Nunamaker Jr., 2010).

Information systems security training (hereafter referred to as security training) has been shown to improve secure behavior (e.g.,...
Jenkins et al., 2010; Puhakainen & Siponen, 2010). Research has just begun, however, to discover how to design training programs to maximize their influence on secure behavior (e.g., Puhakainen & Siponen, 2010). With various options available of how much resources, such as time and money, to expand in developing security training, an important research question is how elaborate security training differs from simple training in improving secure behavior. In this study, we begin to answer this question by examining how the presentation strategy of security training influences secure behavior.

For example, simple online security training can be used that only relays the security information with very little additional stimuli (e.g., a narrated slideshow); or elaborate security training can be produced that accompanies the security information with various other stimuli (e.g., actors, graphics, sounds, etc.). However, very little is known about how these different presentation strategies influence employees’ secure behavior. In summary, we address the following research question in this paper:

How does elaborate vs. simple presentation of online security training influence secure behavior?

THEORY DEVELOPMENT

Security training is an intervention that helps users learn to behave more securely in an information systems security context (Puhakainen & Siponen, 2010). As such, theory of learning can be extended to help develop principles of effective security training programs. In this paper, we draw on cognitivism learning theory (Piaget, 1970, 1985) to explain that online security training should influence secure behavior. Then, building on theory of working memory and cognitive load (Sweller, 1988), we explain how the effectiveness of online training will be influenced by the level of extraneous stimuli in the training presentation.

First, we explain why training should influence secure behavior. Users who receive security training should demonstrate higher secure behavior than users who do not receive training (Jenkins et al., 2010; Puhakainen & Siponen, 2010). Several theoretical perspectives, collectively known as learning theory, have been adopted to explain why training influences secure behavior (Illeris, 2000). Generally, these perspectives can be summarized into three schools of thought—behaviorism, cognitivism and constructivism learning (Ertmer & Newby, 1993). Behaviorism treats the mind as a “black box” and posits that learning is manifested by changes in behavior caused by providing positive or negative reinforcement (Skinner, 1953). In organizations, this type of learning typically takes the form of training by the means of actual rewards or punishments for employees’ positive or negative secure behavior. Constructivism learning (DeVries & Zan, 2003), on the other hand, refers to an active learning process in which employees construct knowledge for themselves. For example, this type of learning is often accomplished by self-driven training—e.g., IT security managers who find solutions to security challenges in an organization, and in doing so, increase their own knowledge about security.

Although employees’ secure behavior is impacted through behaviorism and constructivism training when available, the majority of employees in an organization receive training that targets the cognitivism approach to learning—e.g., online security training. Cognitivism (Piaget, 1970, 1985) explains mental-process learning in which employees are presented with and taught information. Cognitivism posits that the brain is an active organized processor of information. Training influences secure behavior by being received through the senses, processed by working memory, and then stored in short-term and ideally long-term memory (Miller, 1960). Importantly, information must capture users’ attention and be organized into...
Electronic Mail in the University
[www.igi-global.com/article/electronic-mail-university/55676?camid=4v1a](www.igi-global.com/article/electronic-mail-university/55676?camid=4v1a)

Via: Using GOMS to Improve Authorware for a Virtual Internship Environment
[www.igi-global.com/chapter/via/183020?camid=4v1a](www.igi-global.com/chapter/via/183020?camid=4v1a)