Association for Information Systems

AIS Electronic Library (AISeL)

ICIS 2020 TREOs

TREO Papers

12-14-2020

Exploring the Role of Feedback in Improving Anti-Phishing Performance

Shihe Pan
The University of Wisconsin-Madison, span44@wisc.edu

Dong-Heon Kwak
Kent State University, dkwak@kent.edu

Follow this and additional works at: https://aisel.aisnet.org/treos_icis2020

Exploring the Role of Feedback in Improving Anti-Phishing Performance
Taking a Perspective of Self-Regulated Learning

Shihe Pan span44@wisc.edu; Dong-Heon (Austin) Kwak dkwak@kent.edu

Phishing is a fraudulent attempt in which an attacker tries to lure individuals into providing sensitive information by sending deceptive emails, text messages or telephone calls. It is one of the most pervasive cybercrime issues encountered in individuals, organizations, and society. According to the Federal Bureau of Investigation, phishing is the most frequently reported type of cybercrime complaints in 2019. Besides technical solutions, human beings are recognized as a critical part in the process of fending off phishing attacks. In order to help individuals combat phishing attacks, nowadays organizations take various anti-phishing approaches such as online training programs and simulated phishing tests. Within each approach, feedback is often provided either during some phishing detection exercises after training or following a simulated phishing test. It provides information about individuals' previous anti-phishing performance (i.e., how well an individual can detect phishing messages) and offers suggestions for further improvement. Based on the feedback, Individuals assess their anti-phishing performance, modify their knowledge and perceptions about phishing, and finally adjust their behaviors to prevent phishing attacks in the future. In this way, individuals can improve their anti-phishing performance through a process of self-regulated learning (Butler & Winne 1995). Previous phishing studies have given valuable insights into our understanding about anti-phishing performance. Researchers have investigated anti-phishing performance from either an email receiver's or an attacker's perspective. From a receiver's perspective, prior studies have focused on individuals' coping strategies, attention, personalities, knowledge, habits and also demographic factors to explain their anti-phishing performance (Moody et al. 2017; Vishwanath et al. 2011; Vishwanath 2015; Wang et al. 2017; Wright & Marett 2010). Diverse anti-phishing training programs have also been investigated in order to show the importance of anti-phishing education (Jensen et al. 2017; Kumaraguru et al. 2007a, b; Sheng et al. 2010). Studies from an attacker's perspective have compared the power of phishers' strategies to successfully trick individuals (Goel et al. 2017; Wright et al. 2014). However, little is known about how self-regulated learning process occurs in a phishing context. Moreover, it is important to identify the factors that may filter the effect of feedback on improving anti-phishing performance. Drawing on the literature on self-regulated learning (Butler & Winne 1995; Carver & Scheier 1990; Nelson & Narens 1990), this study identifies various important factors in the self-regulated learning process: individuals' prior phishing detection self-efficacy, affect, perceptions about the task (i.e., identifying phishing messages), expectation about task achievement, actual task achievement, attention allocation and cognitive effort on feedback and task achievement after reading feedback. The study will conduct an online experiment consisting of phishing detection exercises both before and after feedback is provided. A web-based eye-tracking platform combined with an online survey will be used to collect both subjective and objective data in the learning process. The data collected as a whole will give a more comprehensive view about the self-regulated learning process in the context of phishing.

Presentation at TREO Talks in conjunction with the 41st International Conference on Information Systems, ICIS 2020
TREO Talks are not peer-reviewed and not a formal part of the ICIS 2020 Proceedings
All TREO Talks are available in the TREO Talks section of the AIS e-Library