Effects of Different Evidence-based Cybersecurity Training Methods on Employees

TREO Talk Paper

Wu He  
Old Dominion University, Norfolk, VA, USA  
whe@odu.edu

Mohd Anwar  
North Carolina A&T State University, Greensboro, NC, USA  
manwar@ncat.edu

Ling Li  
Old Dominion University, Norfolk, VA, USA  
lli@odu.edu

Xiaohong Yuan  
North Carolina A&T State University, Greensboro, NC, USA  
xhyuan@ncat.edu

Ivan Ash  
Old Dominion University, Norfolk, VA, USA  
iash@odu.edu

Li Xu  
Old Dominion University, Norfolk, VA, USA  
lxu@odu.edu

Abstract

In this talk, we present a research study conducted to investigate the effect of different evidence-based cybersecurity training methods on employees’ cybersecurity perception and behavior. To help employees improve their cybersecurity-related knowledge and self-efficacy in dealing with malware attacks that are relevant to their organizations, we recently developed over 30 e-learning malware videos and reports based on the major types of malware attacks we captured using the state-of-the-art anti-malware solutions. Specially, we deployed leading anti-malware tools provided by FireEye and the Wedge Networks to detect a variety of malware that were attacking the network of our campuses in the past two years. As a result, we identified popular malware that affects our employees’ computers and then created some e-learning videos along with relevant reports for the selected malware such as Trojan, malicious URL, SQL injection attack, ransomware and Win Ander Agent. For each attack, the malware videos and reports introduce what the malware is, how it affects the computer or the network, how it is transmitted, what the consequence is, how to remove the malware, and how to prevent it.

Supported by a grant from the National Science Foundation (NSF), we recruited 120 employees for an experimental study related to cybersecurity training. We randomly assigned these employees into 4 groups, each group having 30 employees. Employees in each group received their respective intervention (i.e., malware report, malware videos, both malware report and malware videos, no interventions) during the study. Our research question is: what are the effects of different evidence-based cybersecurity training methods (i.e., malware report, malware videos, both malware report and malware videos) on employees’ perceptions of susceptibility, severity, self-efficacy, security intention as well as on their self-reported cybersecurity behaviors?

To answer this research question, each participant filled out a pre-test survey at the beginning of the experimental study. The collected data was used as baseline of their perceptions of susceptibility, severity, self-efficacy, security intention and self-reported security behaviors. After receiving their respective intervention, each employee completed a post-test survey and an exit interview. One month later each employee also completed a follow-up survey. The group comparison results from statistical analysis of the pre-test, post-tests and follow-up tests will be presented in this TREO Talk.