Effects of Evidence-Based Malware Cybersecurity Training on Employees

Completed Research

Wu He
Old Dominion University
whe@odu.edu

Mohd Anwar
North Carolina A&T State University
manwar@ncat.edu

Ivan Ash
Old Dominion University
iash@odu.edu

Ling Li
Old Dominion University
lli@odu.edu

Xiaohong Yuan
North Carolina A&T State University
xhyuan@ncat.edu

Li Xu
Old Dominion University
lxu@odu.edu

Xin Tian
Kennesaw State University
xtian2@kennesaw.edu

Abstract

This paper presents a research study conducted to investigate the effect of different evidence-based cybersecurity training methods on employees' cybersecurity risk perception and self-reported behavior. Our study participants were randomly assigned into four groups (i.e., malware report, malware videos, both malware report and malware videos, no interventions) to assess the effects of cybersecurity training on their perceptions of vulnerability, severity, self-efficacy, security intention as well as their self-reported cybersecurity behaviors. The results show that evidence-based malware report is a relatively better training method in affecting employees' intentions of engaging in recommended cybersecurity behaviors comparing with the other training methods used in this study.

Keywords

Malware, cybersecurity, training, employees.

Introduction

Social engineering attack vectors such as phishing are widely used for cyberattacks. Phishing involves the use of deceptive or manipulative tactics, to gain unauthorized access to people's computers and sensitive information. Implementing the latest security technologies to prevent phishing may not help much if the users are not adequately trained (Singer & Friedman, 2014). As security incidents continue to rise in cost and frequency, it becomes increasingly important to educate the users to practice safe online behavior and security countermeasures.

The past few years have witnessed numerous successful cyberattacks against businesses. Companies such as Sony, Home Depot and Target have suffered major breaches. Most recently, Marriot's data breach has affected up to 500 million guests. As a result, more and more businesses are concerned with cybersecurity.

Cybersecurity is a critically important issue for businesses today. It is widely accepted that people are the weakest link in a cybersecurity chain (Li et al., 2019).

Many organizations have implemented security training and awareness programs with the aim to influence their employees' attitude and behavior and make them more security-conscious and responsible (Thomson & von Solms, 1998). Many of these security training and awareness programs have provided employees with security requirements, guidelines, and policies concerning how to ensure information security. Cybersecurity awareness training is beneficial for helping employees understand various security threats and risks. For example, individuals with training are less likely to misuse information systems resources (D'Arcy, Hovav, & Galletta, 2009). However, an understanding of threats and risks alone seems insufficient to motivate users to change their existing behavior (Rhee, Ryu, & Kim, 2005). The chief information security officers want to know how to make cybersecurity training more effective.

Rhee, Ryu, & Kim (2005) suggest what really motivates one to take a precautionary and/or preventive action is the awareness of the personal risk of being involved in a negative security event. There is a difference between knowing a threat and acting on the threat because people often underestimate the risks (Schwarzer, 1994). Thus, we feel that an effective cybersecurity training program needs to target people's risk perception to motivate employees to take preventive and precautionary action. In this paper, we present a research study conducted to investigate the effect of different evidence-based cybersecurity training methods on employees' cybersecurity risk perception and behavior. Our study is driven by the research question: *what are the effects of different evidence-based cybersecurity training methods on employees' cybersecurity risk perception and self-reported cybersecurity behavior?*

The remainder of this paper is organized as follows. The following section describes the theoretical background of the study and develops the research hypotheses. The subsequent section describes the research methods. The research findings are then presented. The final section discusses the overall research findings and concludes with the theoretical and practical implications.

Research Study

Cybersecurity Training Methods

Malware report

To find the most pervasive malware types on the network, we deployed leading anti-malware tools provided by FireEye and the Wedge Networks to detect a variety of malware that was attacking the network of two university campuses for two years. We tracked the type and frequency of malware and identified the most common malware attacks in our networks. Then we did online search to find further information about these malwares. As the result, we developed informative reports about the most common malware attacks.

Training videos

To help employees improve their cybersecurity-related knowledge and self-efficacy in dealing with malware attacks that are relevant to their organizations, we developed over 30 E-learning malware videos and reports based on the essential types of malware attacks we captured. 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 Adware 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. For each attack, the e-learning video introduces what the malware is, how it affects the computer or the network, how it is transmitted, what is the consequence, how to remove the malware, and how to prevent it. Figure 1 shows a screenshot from the SQL Injection video we developed, and the video can be retrieved at https://youtu.be/rzVRpZIkc6U. These evidence-based e-learning malware videos can be valuable teaching or learning resources for cybersecurity education.

Research Questions

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?

Procedure

Supported by a grant from the National Science Foundation (NSF), we recruited 119 employees for a randomized control trial related to cybersecurity training. We randomly assigned these employees into four groups. 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.

To answer our research question, each participant filled out a pre-test survey at the beginning of the experimental study. The collected data were used as the baseline of their perceptions of susceptibility, severity, self-efficacy, security intention and self-reported security behaviors. We have four groups: video group, report group, video and report group, and control group. The video group watched four short videos from our developed educated cyber security videos. The four videos are Trojan Zbot, Malicious URL, SQL injection and Ransomware. The participants watched the videos. In contrast, the report group was assigned to the four corresponding reports to learn the materials without watching the videos. The video and report group were assigned to read the report and watch the videos. However, the control group did not receive any intervention during the study and just completed the post-survey without intervention.

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 are presented in the results section.

Figure 1. Screenshot of SQL Injection Learning Video

One-hundred-nineteen employees from two state universities completed the entire study (5 participants were removed due to incomplete data). Table 1 shows the descriptive data of four study groups.

Malware Report	**E-learning Video**	
	No	**Yes**
No	Control Group (n = 24)	Video Group (n = 29)
Yes	Report Group (n = 29)	Video + Report Group (n = 37)

Table 1. Distribution of study population

Figure 2 illustrates the research procedure. We created two surveys (pre-test and post-test) to measure self-reported security behavior through eight indicators: perceived vulnerability, perceived severity, perceived benefits, perceived barriers, response efficacy, response cost, security self-efficacy, and behavioral intention. Questions in the surveys were based on a 7-Likert point scale (1: Strongly Disagree and 7: Strongly Agree). For each of the indicators, we used 3 or 4 questions (adapted from the literature) to measure it. We provided one sample question for each of the indicator below.

- Perceived Vulnerability - I feel that my chance of receiving an email attachment with malware is high.
- Perceived Severity - It is very harmful to me if malware causes my computer to run more slowly.
- Perceived Benefits - I believe that compliance with my organization's information security policy will reduce the risk of losing valuable work.
- Perceived Barriers - It is inconvenient to check the security of an email with attachments.
- Response Efficacy - If I comply with information security policies, the chance of information security breaches occurring in my organizations will be reduced.
- Response Cost - Implementing security measures is time consuming.
- Security Self-efficacy - I feel confident in handling virus-infected files.
- Behavioral Intention - I will change my passwords more often

We collected the survey results from four groups. We also conducted a face-to-face exit interview with the participants and asked them to provide feedback for some questions. After one month, we sent an email to participants and asked them to complete a required follow-up survey, which was designed to assess whether there were any changes of their perceptions of vulnerability, severity, self-efficacy, security intention as well as their self-reported cybersecurity behaviors.

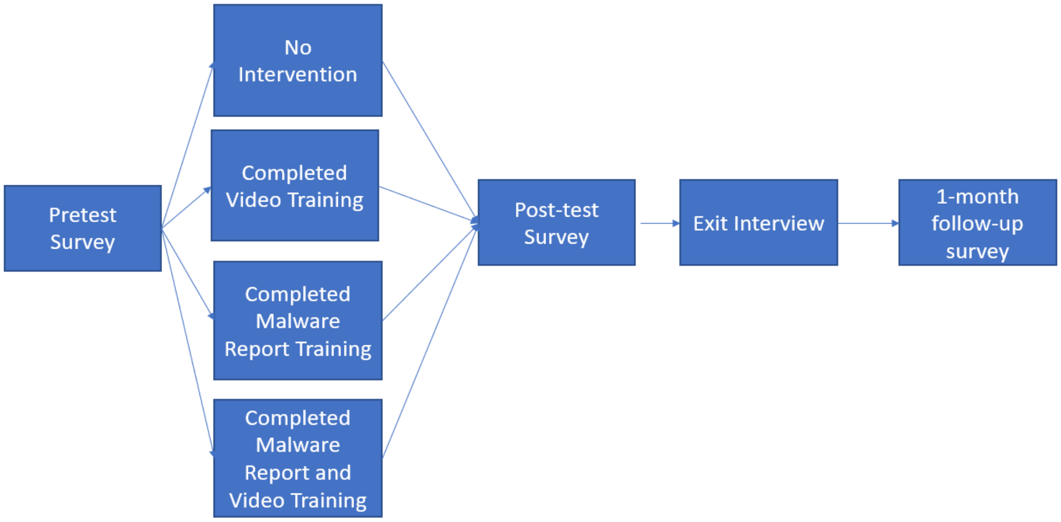

Figure 2. Study Procedure

Results

In order to investigate the effects of the Malware Report and Videos intervention on employee's cyber-security beliefs, we conducted a 2 (video condition) X 2 (malware report condition) analysis of covariance (ANCOVA) on each of the scales from our cyber-security questionnaire with the pre-test scores for each scale entered as a covariate. An alpha level of .05 was used to assess the main effects and interactions of each dependent variable. Corrected means and standard errors for each of the dependent variables are shown in Table 2.

Results revealed no significant main effects or interactions of the interventions on perceived vulnerability, perceived severity, perceived benefits, response efficacy, or response costs. Table 2 shows that the mean ratings for perceived severity (*M* = 6.03, *S.E.* = 0.91), perceived benefits (*M* = 5.95, *S.E.* = 0.18), and response efficacy (*M* = 6.02, *S.E.* = 0.12) were near the ceiling on the 7-point scale for all conditions. Response costs were rated low for all conditions (*M* = 3.41, *S.E.* = 0.23). This suggests that employees already have strong and accurate beliefs on these dimensions, and therefore it is understandable that the interventions did not affect these beliefs. Perceived vulnerability ratings were slightly higher malware report conditions (M = 5.39, S.E. = 0.14) than in the no malware report conditions (*M* = 5.04, *S.E.* = 0.12). However, this main effect was small and did not reach our criteria for statistical significance, *F*(1, 113) = 3.37, *p* = 0.07, η^2 = .03.

The analyses revealed a main effects of the malware report condition on ratings for perceived barriers, *F*(1, 113) = 13.97, *p* < .001, η^2 = .11. Those in the malware report conditions rated the barriers to good cybersecurity to be lower (*M* = 3.25, *S.E.* = 0.12) than those who did not receive the malware report (*M* = 3.94, *S.E.* = 0.13). The main effect of video, and the video by report interaction were not significant for perceived barriers (Fs < 1).

The analyses of cyber-security self-efficacy ratings revealed a main effect of malware report, *F*(1, 113) = 11.72, *p* < .001, η^2 = .09. Those in the malware report condition had higher self-efficacy ratings (*M* = 4.72, *S.E.* = 0.13) than those who did not receive the malware report (M = 4.07, S.E. = 0.14). There was also a main effect of video intervention, *F*(1, 113) = 6.22, *p* < 0.05, η^2 = .05. Those who received the video training reported higher self-efficacy (*M* = 4.16, *S.E.* = 0.13) than those who did not receive the video training (*M* = 4.16, *S.E.* = 0.14). The group means shown in Table 2 suggest that these two main effects were driven by higher self-efficacy ratings in all the intervention groups when compared to the no-intervention control group, however the interaction was small and did not reach our criteria for statistical significance, *F*(1, 113) = 2.90, *p* = 0.09, η^2 = .03.

The analyses of the behavioral intentions variable revealed a main effect of malware report, *F*(1, 113) = 11.04, *p* < .001, η^2 = .09. Those in the report conditions rated their intentions of future protective cybersecurity behaviors as higher (*M* = 5.98, *S.E.* = 0.09) than those in the conditions that did not receive the malware reports (*M* = 5.54, *S.E.* = 0.10). The analysis did not show any evidence of an effect of the video condition or an interaction of the video and report conditions on behavioral intentions (*F*s < 1).

These results suggest that the malware report was an effective intervention for changing employee's beliefs on these dimensions of cyber-security. However, these result show little to no evidence that the e-learning video training condition had an effect on these beliefs. Based on the results, evidence-based malware report training method can be viewed as better training method in terms of affecting employees' intentions of engaging in recommended cybersecurity behaviors.

	Control	Report	Video	Report & Video
	M (SE)	M (SE)	M (SE)	M (SE)
Vulnerability	5.04 (0.20)	5.42 (0.18)	5.05 (0.19)	5.35 (0.15)
Severity	6.26 (0.10)	6.35 (0.09)	6.33 (0.09)	6.29 (0.08)
Benefits	5.72 (0.13)	6.06 (0.12)	5.97 (0.12)	6.04 (0.11)
Response Efficacy	5.84 (0.13)	6.04 (0.12)	6.01 (0.12)	6.17 (0.17)
Response Costs	3.31 (0.26)	3.44 (0.23)	3.43 (0.24)	3.45 (0.21)
Barriers	3.99 (0.20)	3.14 (0.18)	3.90 (0.19)	3.66 (0.16)
Self-Efficacy	3.67 (0.21)	4.65 (0.19)	4.47 (0.19)	4.79 (0.17)
Behavioral Intentions	5.52 (0.15)	6.03 (0.13)	5.57 (0.13)	5.94 (0.12)

Table 2. Estimated means and standard errors for cyber-security belief scales as a function of cyber-security intervention condition

Discussion

The survey results show that the training methods do not have strong impact on employees' perceived severity, perceived benefits and response efficacy. Results suggest that employees are not new to cybersecurity issues and have recognized some aspects of the importance of cybersecurity. We found training methods have some impacts on employees' perceived vulnerability, barriers， response costs, self-efficacy as well as behavioral intentions. Thus, organizations should continue their cybersecurity training to employees. As online threats continue to evolve in complexity, organizations must do 'people patching' (Rayome, 2017). In other words, similar to updating hardware or operating systems, organizations need to consistently update employees with the latest security vulnerabilities and train them on how to recognize and avoid them.

Furthermore, the study found evidence-based malware report is a relatively better training method in affecting employees' intentions of engaging in recommended cybersecurity behaviors comparing with the other two training methods. Malware report works better than video and can be explained as follows: 1) people pay more attention to information that is self-relevant; 2) people have better memory for self-relevant information. Video tutorials did not affect employee's opinions or intended behavior because it lacks self-relevance information. Furthermore, the study found that using multiple modes of presentation for training is not necessary or more beneficial. Since many organizations have limited financial and human resources for their cybersecurity training programs, we recommend them to consider evidence-based malware reports that contain self-relevant information as a training method and incorporate evidence-based malware reports into their cybersecurity education and training programs (Murphy & Murphy,2013).

Conclusion

Many organizations provide training to employees once a year on best practices for cybersecurity. However, that is not enough and oftentimes not effective. Although providing employees with security requirements, guidelines and policies is essential, they are often general in nature. Individual employees may have general knowledge about information security but many of them lack experience in dealing with various malware attacks as malware continues to increase in frequency and complexity. Individual employees also have a different perception of the security vulnerability, severity or extent of the damage (Ng, Kankanhalli, & Xu, 2009). Thus, there is a need to explore and develop more effective evidence-based cybersecurity training approaches and materials.

Our empirical study revealed that evidence-based malware report training method is a relatively better training method in terms of affecting employees' intentions of engaging in recommended cybersecurity behaviors. It will help employees improve the level of their perceived vulnerability, barriers, costs, self-efficacy as well as behavioral intentions. Organizations are recommended to create and use malware reports for future cybersecurity training of their employees (He, Yuan & Tian, 2014).

Another finding of the study is that training programs and educational materials need to relate cyber awareness to employees' personal life, family and home in order to be more engaging and to change employees' cybersecurity behavior. Implementing strong cybersecurity in organizations needs to get people to care and understand why they need to do things in certain ways. Otherwise, it is hard to change their existing insecure behavior. Our study confirms previous literature that employees pay more attention and are more engaging when the information they receive is directly relevant to them in their home lives and their families and will help them to stay safe at home (Stilgherrian, 2018).

Acknowledgements

This work is partially supported by the National Science Foundation (NSF) under the award 1318470 and 1318501. This material is based upon work supported by (while serving at) the National Science Foundation. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., and Xu, L. 2017. "Gender Difference and Employees' Cybersecurity Behaviors," *Computers in Human Behavior*, 69, (pp. 437–443).

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Information Systems Research*, 20(1), 79-98.

He, W., Anwar, M., Ash, I., Yuan, X., Li, L., and Xu, L. 2016. "A Study of Employees' Self-Reported Cybersecurity Behaviors," *Proceedings of the 22nd Americas Conference on Information Systems* (AMCIS 2016), San Diego, USA, August 11-13, 2016.

He, W., Yuan, X., and Tian, X. 2014. "The self-efficacy variable in behavioral information security research," In *Enterprise Systems Conference* (ES), 2014 (pp. 28-32). IEEE.

Li, L. X., He, W., Xu, L. D., Ash, I. K., Anwar, M., and Yuan, X. 2019. "Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior," *International Journal of Information Management*, 45, pp. 13-24.

Murphy, D. R., and Murphy, R. H. 2013. "Teaching cybersecurity: Protecting the business environment," In *Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference* (p. 88). ACM.

Ng, B. Y., Kankanhalli, A., and Xu, Y. C. 2009. "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems*, 46(4), 815-825.

Rayome, A. 2017. "*How to make your employees care about cybersecurity: 10 tips,"* Retrieved on Sep 15, 2018 at https://www.techrepublic.com/article/how-to-make-your-employees-care-about-cybersecurity-10-tips/

Rhee, H., Ryu, Y. and Kim, C. 2005. "I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security," *ICIS 2005 Proceedings*. 32. http://aisel.aisnet.org/icis2005/32

Singer, P. W., and Friedman, A. 2014. *Cybersecurity: What Everyone Needs to Know*. Oxford University Press.

Stilgherrian 2018. "Security training is useless unless it changes behaviours," Retrieved on Oct. 15, 2018 at https://www.zdnet.com/article/security-training-is-useless-unless-it-changes-behaviours/

Thomson, M. E., and von Solms, R. 1998. "Information security awareness: educating your users effectively," *Information management & computer security*, 6(4), 167-173.

Warkentin, M., and Willison, R. 2009. "Behavioral and policy issues in information systems security: the insider threat," *European Journal of Information Systems*, 18(2), 101-105.