KSU Proceedings on Cybersecurity Education, Research and Practice

2016 KSU Conference on Cybersecurity Education, Research and Practice

Developing and Using Evidence-based E-learning Videos for Cybersecurity Education

Wu He
Old Dominion University, whe@odu.edu

Xin Tian
Old Dominion University, xtian@odu.edu

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

Abstract

To help people improve their knowledge and security self-efficacy in dealing with malware attacks that are relevant and meaningful to their organizations, we recently developed over 30 e-learning videos based on the major types of malware attacks we captured using the state-of-the-art anti-malware solution. The preliminary evaluation results of the videos are quite positive and indicate that these evidence-based e-learning videos have great potential to increase users' security self-efficacy.

Disciplines

Curriculum and Instruction | Information Security

INTRODUCTION

Human beings are often the weakest link in information security (Warkentin&Willison, 2009). Hackers and cyber criminals often use social engineering attacks, such as phishing and scams which involve the use of deceptive or manipulative tactics, to gain unauthorized access to people's computers and sensitive information. Implementing the latest security technologies may not help much if the users are not properly 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. As the result, more and more businesses are concerned with cybersecurity. Many organizations have implemented security training and awareness programs with the aim to influence their employees' attitude and behavior and make them become more security-conscious and responsible(Thomson&vonSolms, 1998). Many of these security training and awareness programs have provided employees with security requirements, guidelines and policies concerning how to ensure information security. Although providing employees with security requirements, guidelines and policies is essential, they are often general in nature and not specific enough. 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). Our recent survey study revealed four unique predictors of self-reported cybersecurity behavior: Computer Skill, Perceived Benefits, Perceived Barriers, and Security Self-efficacy and we recommend organizations to assess these four variables and identify employees who are at risk of cyber attacks and could be the target of interventions (He et al., 2016). In particular, security self-efficacy has a strongimpact on end users' intentions to adopt recommended security practices against malware (Johnston &Warkentin, 2010). For employees with low security self-efficacy, organizations are recommended to devise mechanisms to improve their employees' security self-efficacy in preventing and detecting malware (He, Yuan, &Tian, 2014).

METHOD

To help people improve their knowledgeand security self-efficacy in dealing with malware attacks that are relevant and meaningful to their organizations, we recently developed over 30 e-learning videos and materials based on the major types of malware attacks we captured using the state-of-the-art anti-malware

Figure 1. A screenshot from the ransomware video

solution. Camtasia Studio 8 was used to create these e-learning videos. 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. Both anti-malware tools detected and captured a variety of malware during the research period. As the result, we identified the popular malware that affectour employees' computers and then created some e-learning videos along with relevant materials for the selected malware such as Trojan.Generic, Trojan.Zbot, malicious URL, SQL injection attack, ransomware and Win Adware Agent.

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.The e-learning resources we developed can be found at http://securitybehavior.com. Figure 1 shows a screenshot from the ransomware video we developed. These evidence-based e-learning malware videos can be very good teaching or learning resources for cybersecurity education.

PRELIMINARY EVALUATION RESULTS

To evaluate the effectiveness of these e-learning videos, we showed some of the videos to students in our undergraduate courses and conducted short surveys. For example, we asked 20 students in an introductory IT class to watch the e-learning video regarding Trojan. Generic and then complete a questionnaire about this video. We collected 16 effective questionnaires and removed 4 questionnaires that had missing data.4 of them are female students. The preliminary results are quite positive. Most students reported that this video was easy to understand and was helpful to understand how the Trojan. Generic works. After watching the e-learning video, most of them (81.3%) felt confident that they have the skills to implement security measures to prevent the Trojan. Generic from damaging their computers. 62.3% of the students expressed their confidence in terms of getting rid of the Trojan.Genericfrom their computers if their computers were infected.

Recently we showed two malware videos about ransomware and malicious URL to middle school and high school students who attended the GenCyber cyber security summer camps at Old Dominion University. 37 students in Week#1 of the camps watched the ransomware video and completed an assessment questionnaire (See Appendix). 44 students in Week#2 of the camps watched the malicious URL video and completed the same assessment questionnaire. Below is a summary of the evaluation results. We used SPSS to do the data analysis.

The first two questions in the questionnaire assess the computer skills and Internet skills of the participating students. We use 5-point Likert scale for the first two questions where 1-is poor and 5-is excellent. Then, the following 5 evaluation questions use 7-point Likert scale (from 1-strongly disagree to 7-strongly agree)to measure the quality of E-learning video, student perception and learning, and their confidencein terms of preventing and removing the malware.

Variables	Mean	SD	Q1	Q2	Q3	Q4	Q5	Q6	Q7
Q1	3.514	.9609	1						
Q2	3.649	.9780	.759**	1					
Q3	5.459	1.0434	.312	.190	1				
Q4	5.297	1.0766	.278	.234	.419**	1			
Q5	5.108	1.1968	.458**	.437**	.248	.061	1		
Q6	5.243	1.0383	.400*	.387*	.279	-.017	.559**	1	
Q7	5.595	1.1657	.241	.237	.500**	.487**	.331*	.313	1

*Correlation is significant at the .05 level (two-tailed).

**Correlation is significant at the .01 level (two-tailed).

Table 1. Mean, Standard Deviation, and Correlation of Question 1 to Question 7 (Week 1)

Table 1 shows the correlation table of the questionnaire. The respondentsare 37 middle school and high school students who attended the cybersecurity summer camp in the first week and watched the ransomware video. 55% of them are boys and 45% are girls. The first two questions are highly correlated and have a significant positive relationship between computer skills and Internet skills. We found that students who have good computer skills are more confident to implement security measures introduced in the E-learning malware video to prevent or stop the malware from damaging their computers.These students also feel more confident in getting rid of the malware from their computer after watching the E-learning malware video.

In the second week, another group of 44 middle and high school students attended the cyber security summer camp. 67% of them are boys and 33% are girls. Table 2 shows the results of questionnaire after they watchedthe malicious URL video. We found that their Internet skill is significantlypositive related to their motivation of learning malware attacks as well as their skills to implement security measures. Students who have stronger motivation to learn knowledge about malware attacks and online risks also foundthat this video was very useful to help them understand those security concepts introduced in the videos.

Variables	Mean	SD	Q1	Q2	Q3	Q4	Q5	Q6	Q7
Q1	3.432	1.0207	1						
Q2	3.614	.8685	$.639^{**}$	1					
Q3	4.614	1.3332	.262	$.471^{**}$	1				
Q4	4.977	1.6209	.034	$.324^{*}$	$.362^{**}$	1			
Q5	4.659	1.5840	.280	$.477^{**}$	$.399^{**}$	$.341^{*}$	1		
Q6	4.932	1.1891	.159	$.402^{*}$	$.306^{*}$	.265	$.802^{**}$	1	
Q7	5.535	1.2974	.053	$.315^{*}$	$.355^{*}$	$.540^{**}$	$.613^{*}$	$.433^{**}$	1

*Correlation is significant at the .05 level (two-tailed).

**Correlation is significant at the .01 level (two-tailed).

Table 2. Mean, Standard Deviation, and Correlation of Question 1 to Question 7 (Week 2)

According to the survey results, both group of students agreed that the malware videoswere useful to help them understand the online risks. In addition, we gathered some qualitative feedback and suggestions from these students on our developed malware videos (See Table 3).

What do you like best about the malware videos?	Do you have any suggestions or feedback to the malware videos?
-The 3D animation, the virus character designs. -They were very interesting and I was really focused on it. -The information was easy to retain. -They keep me informed about malware. -The malware videos are interesting. Cool and funny. -How amazing the animations were. -Animation is good. Videos provide beneficial information. -Visuals were appealing and contained good and simple information.	-Add more information about what NOT to do to prevent viruses. -Include all possible risks - lowest and highest - for worst - possible situation thoughts. -Explain other ways to remove malware. -I suggest they show all the negatives and dangers of the malware. -They should have given us more examples. -Show the malware in action that may be running on a VM. -They should be more informative.

-It gave me information about Cyber Security. -Very simple format in a clear way and straight forward way. They were in depth and clear to understand.	

Table 3. Selected Comments from Two Groups of Students

In summary, the evaluation results indicate that students enjoyed watching ourdevelopede-learning malware videos and such videos have great potential to increase students’ motivation, learning and security self-efficacy. We plan to show these videos to organizational employees in the near future and survey employees with low security-efficacy to assess the impact of these evidence-based e-learning malware videos on improving their security self-efficacy.

ACKNOWLEDGMENT

This work is partially supported by the National Science Foundation (NSF) under the award SES-1318470 and SES-1318501 and the National Security Agency (NSA) under the award H98230-16-1-0245. 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 NSF and NSA.

REFERENCES

[1]He, W., Anwar, M., Ash, I., Yuan, X., Li, L., & 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.

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

[3]Johnston, A. C., &Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS quarterly*, 34(3), 549-566.

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

[5]Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What Everyone Needs to Know*. Oxford University Press.

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

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

APPENDIX

Malware Video Survey Questions

1. How would you evaluate your computer skills in general?
   1) Poor
   2) Fair
   3) Good
   4) Very good
   5) Excellent

2. How would you evaluate your Internet skills in general?
   1) Poor
   2) Fair
   3) Good
   4) Very good
   5) Excellent

3. I enjoyed watching the malware videos
   1) Strongly disagree
   2) Disagree
   3) Somewhat disagree
   4) Neutral
   5) Somewhat agree
   6) Agree
   7) Strongly agree

4. I am motivated to learn about malware attacks.
   1) Strongly disagree
   2) Disagree
   3) Somewhat disagree
   4) Neutral
   5) Somewhat agree
   6) Agree
   7) Strongly agree

5. I have the skills to implement security measures to stop the malware from damaging my computer after watching the E-learning video.
   1) Strongly disagree
   2) Disagree
   3) Somewhat disagree
   4) Neutral
   5) Somewhat agree
   6) Agree
   7) Strongly agree

6. I feel confident in getting rid of the malware from my computer after watching the E-learning video.
   1) Strongly disagree
   2) Disagree
   3) Somewhat disagree
   4) Neutral
   5) Somewhat agree
   6) Agree
   7) Strongly agree

7. The malware videos were useful to help me understand online/cyber risks.
   1) Strongly disagree
   2) Disagree
   3) Somewhat disagree
   4) Neutral
   5) Somewhat agree
   6) Agree
   7) Strongly agree

8. What do you like best about the malware videos?

9. Do you have any suggestions or feedback to the malware videos?