Journal of Information Systems Education

Volume 28
Issue 2
December 2017

Is Seeing Believing? Training Users on Information Security: Evidence from Java Applets

Ramakrishna Ayyagari and Norilyz Figueroa

Recommended Citation: Ayyagari, R. & Figueroa, N. (2017). Is Seeing Believing? Training Users on Information Security: Evidence from Java Applets. *Journal of Information Systems Education*, 28(2), pp. 115-122.

Article Link: http://jise.org/Volume28/n2/JISEv28n2p115.html

Initial Submission:	6 September 2016
Accepted:	14 September 2017
Abstract Posted Online:	7 November 2017
Published:	12 December 2017

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Is Seeing Believing? Training Users on Information Security: Evidence from Java Applets

Ramakrishna Ayyagari
Norilyz Figueroa
University of Massachusetts – Boston
College of Management
Boston, MA 02125, USA
r.ayyagari@umb.edu

ABSTRACT

Information Security issues are one of the top concerns of CEOs. Accordingly, information systems education and research have addressed security issues. One of the main areas of research is the behavioral issues in Information Security, primarily focusing on users' compliance to information security policies. We contribute to this literature by arguing that proper implementation of security policies requires effective training. Specifically, we argue that adherence to security policies could be improved by using training strategies where written policies are 'shown'. To test our assertion, we use a scenario that users often face when browsing – installation of java applets. Based on previous literature, we identified key antecedents of compliance and tested their effectiveness in an experimental setting. One group of users received guidance from a written policy, whereas the other group was 'shown' the meaning of the written policy in the form of a video. Our contribution is simple yet powerful – effective information security training can be accomplished when users are shown the reasons behind the written policies. In other words, in addition to written policies, it is beneficial to actually 'show' what the policies accomplish.

Keywords: Security, Security policies, Training, Compliance, Java applets

1. INTRODUCTION

In this digital age, information has become an important asset to any type of organization. From big corporations to small businesses, non-profit organizations, and governments, organizations need to safeguard and secure their information. To safeguard the critical information, organizations spend valuable resources on technology tools like intrusion detection systems, firewalls, anti-virus, and similar technologies (Lee and Larsen, 2009; Morgan, 2015b). However, a purely technological solution to security is not going to work (Mitnick, 2003).

Organizations are socio-technical systems, and a holistic approach to security needs to involve a socio-technical solution. Individuals are an integral part of organizations, and their interactions with technology can be a weak link. Researchers argue that employees are the weakest link in the security chain of an organization (Mitnick, 2003; Warkentin and Willison, 2009). In fact, it is reported that as much as 95% of all security incidents involve human error (IBM, 2014), and security awareness training is now a billion dollar industry (Morgan, 2015a). Employees can become an asset to information security, rather than a liability, if they choose pro-security behaviors. These behaviors are driven by organizational policies and their adherence towards these policies. Accordingly, research in information systems has studied why employees comply or do not comply with information security policies (Bulgurcu, Cavusoglu, and Benbasat, 2010; Guo, 2013; Safa, Von Solms, and Furnell, 2016; Siponen and Vance, 2010; Vroom and von Solms, 2004). Security compliance issues can be due to intentional (malicious) and unintentional behaviors. Our paper focuses on unintentional behaviors due to lack of awareness or inappropriate assessment of risk and argues that effective training strategies could reduce these risks.

Although previous research focuses on the reasons for not complying or how to improve compliance (Crossler et al., 2013; Herath and Rao, 2009; Johnston and Warkentin, 2010; Safa, von Solms, and Furnell, 2016), it is still unclear why issues of non-compliance to security policies arise in the first place. We argue that one of the reasons is ineffective training on policies, i.e., the gap between the message of the policies and users' understanding of these policies. Written policies are long and typically full of technical jargon. For an average user, it is difficult to understand the "why" behind the behaviors suggested by the policies. For example, the Department of Health and Human Services lists several Dos and Don'ts when using HHS Information resources (see https://www.hhs.gov/ocio/policy/hhs-rob.html), but does little to explain the reasons behind those policies. We suggest that rather than educating users only on what to do or what not to do (typical wording of security policies), *show them why*. Accordingly, in this paper, we study information security training strategies of users.

We test our assertion of training effectiveness by studying user reactions to a security decision involving the installation of java applets. Specifically, we test user awareness and compliance to java applet warnings for two groups – group A has to choose a behavior based on an applet warning (educating using written policy) while group B has to choose a behavior after seeing a video about the meaning of the applet warning (explaining the 'why' of the written policy).

The rest of the paper is organized as follows. First, we provide a brief literature review of related works in information security education and information security behaviors. Next, the research model and hypotheses are presented. Third, we discuss our study methodology and results. Finally, we discuss the contributions from our study.

2. LITERATURE REVIEW

The growing importance of information security is reflected in the inclusion of security topics in information systems curriculum. Accordingly, the past literature has focused on the approaches to developing information security curriculum (Harris and Patten, 2015; Kim and Surendran, 2002), the challenges of teaching security to business students (Hazari, 2002), and the advantages of incorporating hands-on, case, and service learning to information security (Ilvonen, 2013; Wu et al., 2014). More specifically, research has also looked at effective training strategies on individual information security behaviors. For example, Yoon, Hwang, and Kim (2012) argue that education in security awareness and understanding of the severity of security issues influence users' security behaviors. We contribute to this stream of research by arguing for an effective way to train users.

Users have to make security decisions as part of their interactions with computer systems. For example, whether to update software, to install a plugin or applet, or to click on links, etc., these are all decisions that are not directly part of work tasks. For typical users, these actions add to the mental overload and can lead to irrational decisions (West, 2008). It is an organization's responsibility to enable pro-security behaviors without overloading users' daily activities. Organizations provide guidance for expected behavior through security policies. However, compliance to such policies is difficult to achieve. How can better compliance be achieved with established policies? This has been a theme of information security studies (Crossler et al., 2013). Since our goal is to find ways to enhance user compliance to security policies, we draw on previous works to identify key variables that influence compliance behaviors.

What motivates users to practice pro-security behaviors? Anderson and Agarwal (2010) have addressed this question by using modified protection motivation theory. This theory "predicts individual response when faced with a threat" (p. 615). Based on a multimethod study, the research found that cognitive variables like self-efficacy are an important driver determining pro-security behaviors. Once the user encounters a security decision like a message from an applet, if the user is unsure about the consequences, the user will not be confident of his/her response to the security scenario. Previous research has shown that self-efficacy influences security behavior (Anderson and Agarwal, 2010; Lee and Larsen, 2009). Therefore, we include self-efficacy in our study as it is a key antecedent to pro-security behaviors.

Researchers have also used variants of the Theory of Planned Behavior to explain the behavioral intention to comply with security policies. Studies using this approach suggest that the attitude towards the behavior is a critical variable in explaining user behaviors (Anderson and Agarwal, 2010; Bulgurcu, Cavusoglu, and Benbasat, 2010). Therefore, we include attitude in our study.

One of the ways to counter security threats is to use protective technologies. Dinev and Hu (2007) examined the factors that influence user's intentions to use protective technologies. Protective technologies are "information technologies that protect data and systems from disturbances such as viruses, unauthorized access, disruptions, spyware, and others" (p. 386). Drawing from the theory of planned behavior, they found that the awareness of threats is a strong predictor of making a pro-security decision. Similarly, Bulgurcu, Cavusoglu, and Benbasat (2010) found support for awareness as a key driver for intent to comply with security policies. Therefore, we include awareness in our study.

Previous research suggests that users are willing to learn about safer security practices, but might be unsuccessful if not provided guidance (Flinn and Lumsden, 2005). For example, Furnell, Jusoh, and Katsabas (2006) show that users are not adept at setting security options, even on browsers, without guidance. They suggest that unless proper training is provided, users might not be able to make pro-security decisions when presented with security scenarios like java applet messages.

Users are often unaware of the impact of their security decision (Zurko et al., 2002). In a study of Lotus client users, Zurko et al. (2002) found that when presented with a security decision during users' work, users who are normally conscious of security issues allowed potentially insecure applications to run. However, if users understand the impact of their security decisions, they are prone to make pro-security decisions. In the literature this is reflected in the construct of vulnerability of resources (Bulgurcu, Cavusoglu, and Benbasat, 2010). This construct captures the users' belief that organizational resources are at risk if they do not follow security recommendations. Based on the above review, the key variables included in this paper are awareness, self-efficacy, attitude, and vulnerability of resources.

3. OUR STUDY

One of the activities that is far reaching is browsing the web. Typical policies that govern users' behaviors regarding browsing can be found in an "Internet use policy," an "acceptable user policy," or something similar. While browsing the Internet, many users encounter mobile codes (like applets, ActiveX controls, and plugins) that enhance the user experience, and at the same time pose a security risk.

Mobile codes are executable software that are transferred between systems. Common mobile codes are Java Applets, ActiveX controls, and Plugins. This study will focus specifically on how users behave towards Java Applets. Java Applets will run on a variety of platforms and browsers, unlike ActiveX controls that will only run on Microsoft applications and platforms (Finnegan, 2000). A Java Applet is a program written in the Java Programing Language which is transferred

to a system and then executed by a web browser (Oracle, 2015). The mobile code dialog boxes typically require users to make a security decision, and users might override security protections (for example, running an untrusted applet).

While browsing the Internet, users can encounter two different types of Java Applet warning messages. Users can encounter Applets with a verified digital signature or an unverified digital signature. A verified signature indicates that the Applet is coming from a trusted source, and if the Applet is executed it will have greater access over the users' computing resources (Oracle, 2015). It should be noted that a trusted source does not imply a safe source. If the computer crashes after installing an applet from a trusted source, then at least what caused the crash is known (because the source of the applet is known). On the other hand, if the signature cannot be verified then the Applet is originating from an untrusted source. Users can easily overlook this important distinction between these two types of Applets. Further, since users are so used to seeing mobile codes (like Applets and ActiveX controls), they might not think twice when installing mobile codes.

If users mistakenly allow a malicious Applet to run on their computer, the Applet can gain full control over the users' computing resources. A malicious Applet has the ability to capture keystrokes that can compromise the users' sensitive information, such as passwords. They are also capable of executing new programs on the users' computer. Given the potential capacity for damage, we study how users behave when presented with Applet warnings. To what degree do users follow the Applet warning recommendation? We argue that if the users are shown the meaning of these recommendations, it leads to users who are better prepared to handle security decisions. As discussed in the next section, we achieve this by comparing two groups. Group A received the standard Applet warning, whereas Group B received an explanation of the meaning of the Applet warning through a video.

When presented with a security decision like an Applet warning, users have different abilities to process the meaning of the message or understand the options it presents (Anderson and Agarwal, 2010). This concept is captured through self-efficacy, which reflects users' confidence in dealing with security scenarios (in this study, Java Applets). If the users are actually shown the impact of the Applet options, they will be better prepared. In addition, better understanding of the Applet options increases users' awareness of the security message and the consequences of their actions. In general, technology or information security awareness captures the raised consciousness or understanding (Bulgurcu, Cavusoglu, and Benbasat, 2010; Dinev and Hu, 2007). Armed with the knowledge and understanding of options provided in the Applet messages, users will be more responsible and understand the risk posed by their actions to organizational resources (Bulgurcu, Cavusoglu, and Benbasat, 2010; Zurko et al., 2002). Understanding the severity of their actions (e.g., clicking a button can lead to the complete ownership of a machine by an attacker) leads to changed attitudes towards Java Applets. Therefore, we hypothesize that:

H1: Users' perception of self-efficacy will be higher for the group trained on *Applet warning meaning* compared to the group receiving *Applet warning* only.

H2: Users' perception of awareness will be higher for the group trained on *Applet warning meaning* compared to the group receiving *Applet warning* only.

H3: Users' perception of vulnerability of resources will be higher for the group trained on *Applet warning meaning* compared to the group receiving *Applet warning* only.

H4: Users' perception of attitude will be higher for the group trained on *Applet warning meaning* compared to the group receiving *Applet warning* only.

4. METHODOLOGY AND RESULTS

We used surveys to collect data for this research and test the hypotheses. The survey population consisted of 141 undergraduate students from a large, public university in the northeast United States. The participants belonged to the College of Management and were enrolled in either introductory business or information technology courses. There was no incentive for students to complete the survey, and participation was strictly voluntary. No personally identifiable information about the respondents was collected, and respondents were assured of anonymity of their responses.

Surveys were administered by paper and contained questions measured on a 5-point Likert scale (see items in Appendix). The survey contained a captured image of a typical Java Applet warning "The application's digital signature… Do you want to run the application?" The scales used in the present study were adapted from previous research (Bulgurcu, Cavusoglu, and Benbasat, 2010). For example, the information security awareness scale was adapted to reflect Java Applet awareness. The variables used in this study are self-efficacy (Anderson and Agarwal, 2010), awareness, attitude, and vulnerability of resources (Bulgurcu, Cavusoglu, and Benbasat, 2010). The adapted scales were reliable as measured by Cronbach's alpha. Values ranged from 0.76 (for awareness) to 0.94 (for vulnerability of resources). These values are above the generally accepted value of 0.70.

Since the goal of the study is to see if different training strategies improve adherence to policies, we divided our sample into two groups. Group A consisted of 65 students, and Group B contained 76 students. Both groups responded to the same questionnaire. Group A respondents had to respond to the survey based on the standard 'applet warning' (akin to written policies in organizations). On the other hand, respondents in Group B were given an explanation of the meaning of the 'applet warning' using a video.

The three-minute video demonstrated the risks associated with downloading and installing unverified Java Applets. The video started by demonstrating a user being prompted to install a Java Applet during a web browsing session. Then, the user installs the Applet and continues the browsing session. However, unknown to the user, the act of installing the Applet provides attacker access to the users' computer. The video then shows how easy it is for the attacker to capture screenshots of the users' desktop, execute programs, capture keystrokes, etc. This video was intended to visualize and

explain the 'applet warning' message. The respondents in Group B then completed the survey.

The descriptive statistics for both groups are presented in Table 1. Since our goal is to see if the training by video message was effective over just the text message, the test for mean differences is deemed appropriate. Therefore, we used SPSS software to test for mean differences for two groups (video vs. no video) across the four variables of Awareness, Self-Efficacy, Attitude, and Vulnerability of Resources to test the hypotheses. The results of the t-tests for mean differences are presented in Table 2.

Variable	Group	Average	Standard Deviation
Applet Awareness	A: No Video	3.46	0.94
	B: Video	3.91	0.91
Self-Efficacy	A: No Video	3.23	0.97
	B: Video	3.66	0.92
Vulnerability of Resources	A: No Video	3.52	0.79
	B: Video	3.77	0.97
Attitude	A: No Video	3.39	1.17
	B: Video	3.66	1.07
Age	A: No Video	21.43	4.70
	B: Video	22.75	5.05
Gender	A: No Video	53% Male	
	B: Video	83% Male	

Table 1: Descriptive Statistics

Hypothesis 1 argued that users who view the video would be better prepared to handle Applet warnings. Our results indicate that users' self-efficacy in dealing with Applets is higher if they are trained with video messages ($t=2.69$, $p<0.05$), supporting H1. Similarly, Hypothesis 2 argued that users who view the video would have a better understanding of the options presented by Applets. Our results indicate that users' Applet awareness is higher if they are trained with video messages ($t=2.86$, $p<0.05$), supporting H2. Training with video clearly shows how a simple action can put computing resources at risk. This technique concretely presents a link between users' actions and risks their actions pose. Therefore, as argued in Hypothesis 3, the users' perception of vulnerability of resources will be higher for the video group. The results support this assertion ($t=1.78$, $p<0.05$). As argued in Hypothesis 4, after seeing the potential damage that can be done with the Applet, it is expected that users' attitude towards Applet warning will be different. Our results indicate that this hypothesis is weakly supported ($t=1.38$, $p<0.10$).

Variable	Mean Diff.	Std. Error Diff.	t-value	df	p-value
Applet Awareness	0.45	0.15	2.86	139	0.002
Self-Efficacy	0.43	0.16	2.69	139	0.004
Vulnerability of Resources	0.25	0.14	1.78	139	0.030
Attitude	0.26	0.19	1.38	139	0.080

Table 2: Test for Mean Differences

5. DISCUSSION

Before discussing our results, we highlight some limitations of the study. To operationalize the study, we chose mobile code as the study context. To generalize the findings from this study, other scenarios need to be studied. For example, users can be trained by showing the impact of responding to phishing emails. Since our sample was based on students in courses, we could not proactively ensure equivalency between the groups. Although no significant differences were found for mean age, gender proportions were significant between the two groups. Therefore, it is possible that gender could also have contributed to the differences found in this study. This raises an interesting question for future research about the role of gender in information security compliance. In addition, we only focused on four variables for testing the effectiveness of the different training approaches. Although previous research has shown the importance of these four variables (awareness, self-efficacy, vulnerability of resources and attitude) in compliance studies, additional variables could be studied to test the effectiveness of different training approaches.

Our study is motivated by a simple question – since users are identified as one of the weakest links in the information security chain, is there a way to train and strengthen this link? Previous research has approached this issue from the perspective of users' compliance to information security policies. We suggest that in addition to compliance, it is important to understand if the users know what to do to be compliant. In particular, we argue that the compliance message (policies) can be better presented. Drawing on previous research in information security, we argue for effective ways to educate users on security policies. Based on the information security literature, we identified awareness, self-efficacy, attitude, and vulnerability of resources as some of the key variables that lead to users' compliance with policies. Our research indicated that presenting the reason behind the policy messages leads to higher scores on these key variables. We contribute a simple yet powerful message to the behavioral information security literature. Educating users on the reasons behind security policies rather than just telling them what to do (typical policy language) is more effective. Our research provides evidence that the 'seeing is believing' strategy can be used to train users on information security. For example, we are still mainly dependent on passwords as an authentication mechanism. It is a well-known issue that users tend to choose easy passwords or write down their passwords. Almost all organizations have written password policies that suggest the opposite. If organizations show a training video on why users need to have strong passwords or how easy it is to crack an easy password (issues covered in written password

policies), then users might be inclined to follow the password policies.

We can also draw similar implications for instructors of information security courses. Especially for introductory information security courses that may not have hands-on lab components, students might not appreciate the importance of theoretical policies. Instructors might use their school's email policies and then show them the importance of the elements of the email policy by demonstrating cracking a password that doesn't follow the email policy. A similar approach can be taken for the need to patch the vulnerabilities in software. Here the instructors can demonstrate the ease with which vulnerable software can be exploited. This will be much more effective than just teaching the students to keep the software up-to-date.

6. CONCLUSION

The importance of the human element in Information Security is well established. To improve Information Security, users' compliance to information security policies is important. Previous research has proposed different approaches to achieve this compliance. We contribute to this literature by arguing that effective training is a critical aspect in implementing the security policies. Using the Java Applet scenario, we have shown that the approach used to present the policy message will have differing impacts on compliance variables. Our results argue for and provide evidence for effective delivery of security messages that are inherent in policies. We hope that the 'seeing is believing' message from our study strengthens the human element in information security.

7. REFERENCES

Anderson, C. L. & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, 34(3), 613-643.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 34(3), 523-A527.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future Directions for Behavioral Information Security Research. *Computers & Security*, 32, 90-101.

Dinev, T. & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems*, 8(7), 386-408.

Finnegan, S. (2000). Managing Mobile Code with Microsoft Technologies. Retrieved from https://msdn.microsoft.com/en-us/library/cc750862.aspx.

Flinn, S. & Lumsden, J. (2005). User Perceptions of Privacy and Security on the Web. http://www.lib.unb.ca/Texts/PST/2005/pdf/flinn.pdf.

Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The Challenges of Understanding and Using Security: A Survey of End-Users. *Computers & Security*, 25(1), 27-35.

Guo, K. H. (2013). Security-related Behavior in Using Information Systems in the Workplace: A Review and Synthesis. *Computers & Security*, 32, 242-251.

Harris, M. A. & Patten, K. P. (2015). Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity Topics into a Computing Curriculum. *Journal of Information Systems Education*, 26(3), 219-234.

Hazari, S. (2002). Reengineering an Information Security Course for Business Management Focus. *Journal of Information Systems Education*, 13(3), 197-204.

Herath, T. & Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems*, 18(2), 106-125.

IBM. (2014). IBM Security Services 2014 Cyber Security Intelligence Index. Retrieved from https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf.

Ilvonen, I. (2013). Information Security Assessment of SMES as Coursework - Learning Information Security Management by Doing. *Journal of Information Systems Education*, 24(1), 53-61.

Johnston, A. C. & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 34(3), 549-A544.

Kim, K. -Y. & Surendran, K. (2002). Information Security Management Curriculum Design: A Joint Industry and Academic Effort. *Journal of Information Systems Education*, 13(3), 227-236.

Lee, Y. & Larsen, K. R. (2009). Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software. *European Journal of Information Systems*, 18(2), 177-187.

Mitnick, K. D. (2003). Are you the Weak Link? *Harvard Business Review*, 81(4), 18-20.

Morgan, S. (2015a). CIOs Turn to Security Awareness Solutions to Change Poor Employee Behaviors. Retrieved from http://www.csoonline.com/article/2926173/security-awareness/cisos-turn-to-security-awareness-solutions-to-change-poor-employee-behaviors.html.

Morgan, S. (2015b). Cybersecurity Market Reaches $75 Billion in 2015 Expected to Reach $170 Billion by 2020. Retrieved from https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#6d4b0a310c33.

Oracle. (2015). What Applets can and cannot Do. The Java Tutorials. Retrieved from http://docs.oracle.com/javase/tutorial/deployment/applet/security.html.

Plant, R. (2014). The Top Issues CEOs Face these Days. Retrieved from http://www.wsj.com/articles/SB10001424052702304914904579439501124390682.

Safa, N. S., von Solms, R., & Furnell, S. (2016). Information Security Policy Compliance Model in Organizations. *Computers & Security*, 56(C), 70-82.

Siponen, M. & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, 34(3), 487-A412.

Vroom, C. & von Solms, R. (2004). Towards Information Security Behavioural Compliance. *Computers & Security*, 23(3), 191-198.

Warkentin, M. & Willison, R. (2009). Behavioral and Policy Issues in Information Systems Security: The Insider Ihreat. *European Journal of Information Systems*, 18(2), 101-105.

West, R. (2008). The Psychology of Security. *Communications of the ACM*, 51(4), 34-40.

Wu, H., Kshirsagar, A., Nwala, A., & Yaohang, L. (2014). Teaching Information Security with Workflow Technology -- A Case Study Approach. *Journal of Information Systems Education*, 25(3), 201-210.

Yoon, C., Hwang, J. -W., & Kim, R. (2012). Exploring Factors that Influence Students' Behaviors in Information Security. *Journal of Information Systems Education*, 23(4), 407-415.

Zurko, M. E., Kaufman, C., Spanbauer, K., & Bassett, C. (2002). Did You Ever have to Make up Your Mind? What Notes Users Do when Faced with a Security Decision. *Proceedings of the 18th Annual Computer Security Applications Conference*.

AUTHOR BIOGRAPHIES

Ramakrishna Ayyagari is an associate professor of Information Systems at UMass – Boston. His work has appeared in leading IS journals such as *MIS Quarterly*, *European Journal of Information Systems*, and *Journal of the AIS*.

Norilyz Figueroa is a recent graduate of UMass – Boston. Currently, she is working as a Storage Engineer at Wayfair.

APPENDIX

Measurement Items
Attitude To me, proceeding with the recommendations of the browser alert would be (5 point Likert scales with these anchors): • Unnecessary – necessary; • Unbeneficial – beneficial; • Unimportant – important; • Unclear – clear.
Awareness (5 point Likert scales with anchors: strongly disagree – strongly agree) Web Browsers will alert users to install Applets when visiting certain websites. • I understand the alert I receive when attempting to download Applets. • I am aware of my options when attempting to download Applets.
Self efficacy (5 point Likert scales with anchors: strongly disagree – strongly agree) Web Browsers will alert users to install Applets when visiting certain websites. • I feel comfortable making decisions with respect to installing Applets. • I am confident in my ability to determine if an Applet is useful or harmful. • I am confident I can prevent the installation of harmful Applets.
Vulnerability of Resources (5 point Likert scales with anchors: strongly disagree – strongly agree) If I don't comply with the recommendations of the Applet alert, my computing resources _____ • Will be at risk • Will be vulnerable • Can be exploited • Can be misused • Can be compromised

Information Systems & Computing
Academic Professionals

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 2574-3872