Validation of the Online Security Behaviors and Beliefs Questionnaire with College Students in the United States

Daniel R. Schaffer, MS¹ and Scott M. Debb, EdD^{1,2}

Abstract

The Online Security Behaviors and Beliefs Questionnaire is a 75-item self-report inventory assessing awareness, attitudes, behaviors, and beliefs toward various aspects of cybersecurity best practices. The questionnaire was originally constructed and validated for use with adult employees in corporate settings, with the measure assessing 13 latent constructs. The goal of this study was to adapt the questionnaire to implement it with a college sample and examine if the identified factor structure for use with this population. Data were collected from 735 students at two public universities in the Southeastern region of Virginia, 676 of whom were retained for analyses. Confirmatory factor analysis using the means and variances adjusted weighted least squares method was conducted using Mplus 8.1 to assess goodness of model fit. The 13-factor model failed to meet criteria for exact or approximate model fit: χ^2 (2701)=44569.85, $p<0.001$; root mean square error of approximation=0.07, 95 percent confidence interval [0.06–0.07]; confirmatory fit index=0.86; Tucker Lewis index=0.85. The results suggest significant differences between cybersecurity awareness, attitudes, and beliefs between the corporate workplace and college student populations that ultimately influenced the reliability and validity of the questionnaire when adapted for use with college students in the United States. It is also possible that the theoretical underpinnings of this questionnaire may not apply, or they may apply differently, in this sample of predominantly African American and Caucasian students.

Keywords: Online Security Behaviors and Beliefs Questionnaire, cybersecurity, confirmatory factor analysis

Introduction

ATTITUDES AND KNOWLEDGE play a critical role in the adherence to cybersecurity best-practices and, more generally, how people view privacy and security expectations. Researchers have found that an individual's perception of information security and self-awareness of their tendencies significantly impact decision-making and behaviors.¹ Furthermore, knowledge of information security policy and procedures tends to predict attitudes toward these policies.² Accordingly, there is a need to better understand the views that diverse groups of people espouse regarding their attitudes and beliefs.

People are both products of their environment, and the environments are products of the people.³ Collectively, the culturally based narrative that people are immersed in on both the group and systemic levels of society shapes their perspectives and, subsequently, their social interactions. Information security awareness encompasses the attitudes, behaviors, and knowledge one has toward the use—or misuse—of electronic information (i.e., passwords or account information), with specific regards to the protection of that

information⁴; however, it is unclear as to how group-based differences might differ based on the cultural context with which a person is associated.

Generational factors may impact how this responsibility is perceived, with adherence to best practices being inconsistent across age groups. For example, while older adults' knowledge and behaviors related to information security may outrank those of younger adults, they may at the same time be less familiar with how information is disseminated across cyberspaces. This creates an increased possibility for having data misused due to gaps in knowledge or direct experience. Kim⁵ examined the status of information security awareness in college students, with results suggesting that this population understands the need and importance of security awareness, but individually, they do not necessarily engage in optimal behaviors.

A study by Farooq et al.⁶ used a general population of university students and demonstrated that information security awareness was based on a combination of factors related to knowledge, behavior, and the impact of individual factors. Furthermore, it appeared that students learned

¹Virginia Consortium Program in Clinical Psychology, Norfolk, Virginia.

²Department of Psychology, Norfolk State University, Norfolk, Virginia.

security concepts gradually and from various sources—such as content from various news media, instructions indicated on specific websites for specific purposes, or in response to a fix needed when a program needs to be patched—rather than in a more direct, linear, manualized approach.

Additional research demonstrated that millennials tend to be more vigilant than older adults in avoiding cyberattacks, but they are also more likely to engage in online behaviors that make them more susceptible to cyberattacks.⁷ Other studies have shown that while younger adults recognize the need for increased cybersecurity training and that the individual is the weakest link in cybersecurity processes, younger adults still continue to engage in online behaviors that compromise cybersecurity at higher prevalence than older adults.⁸ This may be due to current online security practices not being congruent with their current needs or abilities.⁹

Online Security Behaviors and Beliefs Questionnaire

The Online Security Behaviors and Beliefs Questionnaire (OSBBQ) is an empirically validated, 75-item self-report questionnaire that assesses adult attitudes, beliefs, and behaviors toward various aspects of cybersecurity and related practices within a corporate or workplace setting.¹⁰ Recent research has indicated that, more specifically, this questionnaire assesses 13 different factors/constructs within cybersecurity attitudes, beliefs, and behaviors (Table 1). This questionnaire was conceptualized based on the Health Belief Model, which examines preventative health behaviors undertaken to detect

and prevent future disease,^{11,12} and Protection Motivation Theory, which outlines three components of fear appeal that drive cognitive appraisal and behavioral change: magnitude of an event, the probability of the event's occurrence, and the efficacy of a protective action.^{11,13} Using these two conceptual frameworks, the OSBBQ provides a comprehensive assessment of attitudes, beliefs, and behaviors surrounding both proactive and retroactive cybersecurity best practices.

Purpose of study

To evaluate and subsequently compare attitudes and behaviors between diverse groups of people, a valid and reliable instrument is needed that reflects the population being examined. For this study, the OSBBQ, which was originally validated for use with a general population of office workers¹⁰ was adapted for use with a sample of college students. Before using the instrument to offer any insights into the attitudes and behaviors of college students in general, the psychometric properties of the measure need to be examined within this population to determine if the constructs that the questionnaire purports to measure are equivalent.

Methods

Participants

A convenience sample of participants were recruited from two public universities in the Southeastern region of Virginia. Both are public universities—one that is more

TABLE 1. LATENT FACTOR STRUCTURE OF THE ONLINE SECURITY BEHAVIORS AND BELIEFS QUESTIONNAIRE¹¹

<i>Construct/factor</i>	<i>Brief summary</i>
Computer skills	One's self-reported comfort and ability levels when using computers and installing computer software.
Internet skills	One's self-reported comfort and ability levels when using the Internet and various Internet-based functions (e.g., social media, Internet-based transactions, information-finding, and so on).
Information-seeking skills	One's self-reported comfort and ability levels when using the Internet and various Internet-based search engines to find specific or targeted information.
Prior experience with computer security practices	One's self-reported prior experience or training in security best practices and application security best practices.
Perceived vulnerability	One's perceived level of vulnerability to cyber-attacks (e.g., viruses, malware, security breach, and so on), and one's perceived level of vulnerability within the educational institution.
Perceived severity	One's perceptions surrounding consequence severity of cybersecurity breaches or violations of security best practices.
Perceived benefits	One's perceptions surrounding the benefit of different protections against cyber-attacks (e.g., file backup, secure file storage, use of strong passwords, attending cybersecurity trainings, and so on).
Perceived barriers	One's perceptions surrounding possible barriers to implementing adequate cybersecurity (e.g., time commitments, general sense of inconvenience, and so on) or engaging in protective tasks (e.g., file backup, changing security settings, attending cybersecurity trainings, and so on).
Response efficacy	One's attitudes toward the effectiveness of their own actions in preventing possible cyber-attacks or cybersecurity breaches.
Cues to action	One's perception of their educational institution and its encouragement of cybersecurity best practices.
Security self-efficacy	One's sense of self-efficacy and self-agency in their abilities to prevent against cyber-attacks or cybersecurity breaches, and one's sense of self-confidence in being able to rectify certain cyber-attacks or cybersecurity breaches after they happen.
Peer behavior	One's perceptions of the behaviors of their peers regarding cybersecurity.
Self-reported cybersecurity behavior	One's self-reported current engagement in cybersecurity best practices.

research-oriented and the other (a historically Black university) being more teaching oriented. College students were surveyed from April 2017 to February 2018.

Measures

Demographic information. A demographics questionnaire created for this study asked participants to self-report their age, gender, race, and ethnicity.

Information security behaviors. The current study utilizes the OSBBQ, a self-report, Likert-scaled questionnaire consisting of 75 items assessing multiple domains of information security and associated behaviors.^{10,11,14} Participants completed the questionnaire by responding to all 75 items, and the researchers score the questionnaire, with each question being scored within its individual construct to create subscale scores for each of the 13 distinct constructs (Table 1). Initially developed for use in a corporate or workplace setting, minor changes in wording were implemented (i.e., changing “organization” to “university”) to facilitate relevance to typical college students who are unlikely to have experience in corporate or workplace environments. For example: “It is likely that an information security breach is occurring at my workplace” was changed to “It is likely that an information security breach is occurring at my university.” Items ask respondents to rate their degree of comfort with specific tasks and to evaluate their computer and Internet abilities, for example: “How would you rate your computer knowledge in general?”, “How comfortable are you using social media...?”, “I am confident in using the Internet to find the information I need,” “I use different passwords for different accounts,” and “I feel that my chance of receiving an email attachment with a virus is high.”

The OSBBQ is based on two theoretical frameworks: (a) the Health Belief Model and (b) the Protection Motivation Theory.¹¹ According to the previous research, the OSBBQ can be separated into multiple factors, each of which assess different manifest constructs within the latent constructs of online security behaviors and online security beliefs.^{10,11,14} As a result, the OSBBQ is able to provide more information than other assessments, and allows its users to assess various aspects, of online security beliefs and behaviors.

Procedure

Before collecting data, the study was approved by the Institutional Review Boards at both institutions. Participants were recruited through a series of email announcements to students and through faculty. All participants were given access to a hyperlink to a survey administered through a secure online surveying platform. After providing informed consent, participants were asked for basic demographic information and to complete a survey examining attitudes and behavior related to their online activity.

Results

A sample of 735 college students accessed the surveys. After removing 59 cases who did not provide complete responses to all items for the OSBBQ, a total of 676 cases remained. This included 552 from the larger research school and 119 from the smaller liberal arts school (5 respondents

did not report university affiliation). Only 1 item in the measure (item 5) required reverse scoring, and 1 additional item (item 19) was removed from the measure before its implementation into this study per the recommendations of the measure’s authors (I. Ash, personal communications, April 24, 2017). The average age of this sample was 23.18 years-old ($SD=6.94$; min.=18.00, max.=56.00). All other descriptive and demographic information of the survey respondents included in this study can be found in Table 2.

The OSBBQ was found to have strong internal consistency (Cronbach’s $\alpha=0.93$). For each item, the α if-item-deleted remained within ± 0.003 of the initial, indicating a strong pool of items. Split-half reliability was also assessed by randomizing survey items into two equal halves (n of items per half=37). Split-half reliability was found to be strong (reliability of half 1=0.88; reliability of half 2=0.90), with a correlation between the split halves of 0.59, Spearman Brown correlation of 0.75, and Guttman split-half coefficient of 0.74.

All data were assessed for normality of response distribution, and all items fell within an acceptable range for skewness and kurtosis.¹⁵ Goodness of model fit was assessed via confirmatory factor analysis (CFA) in Mplus 8.1 using the means and variances adjusted weighted least squares method. The chi-square test of exact model fit was significant, with $\chi^2(2701)=44569.85$, $p<0.001$, indicating significant differences between the patterns observed in these data and the model specified. As a result, exact model fit could not be declared. Metrics for approximate model fit were also examined: root mean square error of approximation = 0.07, 95 percent confidence interval [0.06–0.07]; confirmatory fit index = 0.86 and Tucker Lewis index = 0.85. Using criteria outlined by Asparouhov and Muthén,¹⁶ all statistics exceeded the limits for demonstrating approximate model fit, meaning approximate model fit could not be supported with this sample.

TABLE 2. SAMPLE DEMOGRAPHICS AND DESCRIPTIVE STATISTICS

	n	Percent
Gender		
Male	146	21.60
Female	528	78.10
Other	2	0.30
Race		
African American	292	43.20
Alaskan Native	1	0.10
American Indian/Native American	3	0.40
Asian/Asian American	28	4.10
Caucasian/white	259	38.30
Latino/a	45	6.70
Hawaiian Native/Pacific Islander	6	0.90
Multiracial	42	6.20
Ethnicity		
Hispanic	63	9.30
Non-Hispanic	592	87.60
Current academic status		
Freshman	138	20.40
Sophomore	116	17.20
Junior	152	22.50
Senior	244	36.10
Graduate student	25	3.70

Given the good internal consistency and previously established empirical validity of this questionnaire, a follow-up principle components analysis was performed in SPSS using varimax rotation. However, the results of this principal components analysis could not be interpreted due to high multicollinearity. While the Bartlett's Test of Sphericity was significant, with $\chi^2(2775) = 23410.40$, $p < 0.001$, and the Kaiser-Meyer-Olkin Measure of Sampling Adequacy was sufficient (0.91), the determinant value did not meet the acceptable threshold (< 0.00001), indicating a high number of interitem correlations and potential multicollinearity within the data. This was corroborated by a large number of significant interitem correlations in the correlation matrix and item cross-loadings within the factor structure. While the average interitem correlation between all items was 0.16, individual interitem correlations were observed up to 0.88. Using criteria by Robinson, Shaver, and Wrightsman,¹⁷ interitem correlations above 0.50 may indicate significant redundancy between items and constructs within a measure, thus corroborating the high multicollinearity observed within this measure for the current sample.

Discussion

The purpose of this research study was to assess the reliability of the OSBBQ for use in a sample of college students. Prior research demonstrated that younger adults appear to demonstrate different attitudes and awareness levels toward cybersecurity best practices compared to older age cohorts. The OSBBQ is a theoretically informed measure that has been studied and validated within an adult corporate employee population.^{10,11,14} This study modified the questionnaire slightly to make the wording of these questions applicable college students to examine the factor structure's fit.

While the questionnaire maintains strong internal consistency, the CFA results from this study suggest that the previously established 13-factor structure¹¹ does not maintain either exact or approximate model fit. Upon further analysis of the data, this questionnaire appeared to produce significant interitem correlations and multicollinearity within the data. As a result, the OSBBQ may not be an adequate measure, at this time, when adapted and applied to a college student sample. In addition, it is possible that the conceptual differences in cyber security attitudes and beliefs differ significantly beyond what, at face value, appears to be common best practices. As such, the instrument may not be adequately measuring the same latent constructs as initially determined in the original validation study.

Further research is needed to investigate and modify the OSBBQ for use with college students to address the issues of item multicollinearity and improve the questionnaire's overall validity within this population. Before this questionnaire sees continued use with college-aged students, these researchers recommend the use of focus groups containing college-aged individuals (aged 18–22) to better understand the OSBBQ questions, which were originally created to appeal to adult corporate employees, in their application with this different population. More insight is needed to better understand if the terminology of these items and their content is being fully understood, or if the specific online security practices being assessed are even relevant to this fundamentally different population. After data are col-

lected from these focus group sessions, the information may be applied to further modify the questionnaire to better reflect the varying values and expectations toward cybersecurity within the college-aged population.

Limitations

The data from which these conclusions were derived were collected from two public universities in Southeastern Virginia. Therefore, drawing overarching conclusions regarding the reliability and validity of the measure across all college student populations should be done with caution. The sample was also composed of predominantly African American and Caucasian undergraduate students, and drawing inferences across all ethnic and racial groups among college student populations is not advised. Furthermore, while changes to the questionnaire were minimalistic—slight changes in wording (i.e., changing “organization” to “university”) to adapt the items to a student sample—it is possible that even minor wording changes could impact the psychometric properties of the questions and subscales. As a result, different or alternate changes may allow the questionnaire to maintain its original factor structure in different populations.

Conclusions

This study's results suggest that the OSBBQ may not be able to maintain the same level of reliability or validity when adapted and administered to a college student sample. One possible explanation is that there are significant differences in cybersecurity awareness, attitudes, beliefs, and behaviors between college students and adult corporate employees, and these differences likely contributed to the validity of the measure when applied to these specific populations. Another explanation for the lack of model fit across samples may be found in the theoretical underpinnings of the questionnaire itself, as the OSBBQ incorporates two different conceptual frameworks: the Health Belief Model and the Protection Motivation Theory. Both of these theories provide a conceptual framework for how fear appeal aids in attitude change and behavior modification. Previous studies have shown that fear appeal produces different results across different age groups.^{18,19} As a result, the theoretical and conceptual frameworks that created this questionnaire may not apply, or may apply in a different manner, in a younger population.

Author Disclosure Statement

No competing financial interests exist.

Funding Information

The work in this study was supported in part by the Department of Defense (award # FA8750-15-2-0120) and the Norfolk State University Cybersecurity Research Complex.

References

1. Huang DL, Rau PLP, Salvendy G, et al. Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies* 2011; 69:870–883.
2. Parsons K, McCormac A, Butavicius M, et al. Determining employee awareness using the human aspects of informa-

- tion security questionnaire (HAIS-Q). *Computers and Security* 2014; 42:165–176.
3. Bandura A. Human agency in social cognitive theory. *American Psychologist* 1986; 44:1175–1184.
 4. Siponnen MT. A conceptual foundation for organizational information security awareness. *Information Management and Computer Security* 2000; 8:31–41.
 5. Kim EB. Recommendations for information security awareness training for college students. *Information Management and Computer Security* 2014; 22:115–126.
 6. Farooq A, Isoaho J, Virtanen S, et al. (2015). Information security awareness in Educational Institution: an analysis of students' individual factors. In: *Trustcom/BigDataSE/ISPA, 2015 IEEE*. IEEE, Vol. 1, pp. 352–359.
 7. Rainie L, Kiesler S, Kang R, et al. Anonymity, privacy, and security. *Pew Research Center: Internet & Technology*. 5 September, 2013. <https://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online> (accessed Nov. 14, 2019).
 8. Zang X. What do consumers really know about spyware? *Communications of the ACM* 2005; 48:44–48.
 9. Howe AE, Ray I, Roberts M, et al. The psychology of security for the home computer user. *Journal of Consumer Affairs* 2013; 43:449–473.
 10. Li L, He W, Ash I, et al. Does explicit information security policy affect employees' cyber security behavior? A pilot study. *Second International Conference on Enterprise Systems 2014*, Shanghai, China. DOI: 10.1109/ES.2014.66.
 11. Anwar M, He W, Ash I, et al. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior* 2017; 69:437–443.
 12. Rosenstock IM. (1974). Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In: Cacioppo J, Petty R, eds. *Social psychophysiology*. New York, NY: Guilford Press.
 13. Rogers RW. A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology: Interdisciplinary and Applied* 1975; 91:93–114.
 14. Li L, He W, Xu L, et al. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management* 2019; 45:13–19.
 15. Finney SJ, DiStefano C. (2006). Non-normal and categorical data in structural equation modeling. In: Hancock GR, Mueller RO, eds. *Structural Equation Modeling: A Second Course*. Greenwich, CN: Information Age Publishing, pp. 269–314.
 16. Asparouhov T, Muthén B. (2018). SRMR in Mplus. www.statmodel.com/download/SRMR2.pdf (accessed Nov. 14, 2019).
 17. Robinson JP, Shaver PR, Wrightsman LS. (1991). Criteria for scale selection and evaluation. In: Robinson JP, Shaver PR, Wrightsman LS, eds. *Measures of Personality and Social Psychological Attitudes*. San Diego, CA: Academic, pp. 1–15.
 18. Jones SC. Using fear appeals to promote cancer screening—are we scaring the wrong people? *International Journal of Nonprofit and Voluntary Sector Marketing* 2006; 11:93–103.
 19. Tannenbaum MB, Helper J, Zimmerman RS, et al. Appealing to fear: a meta-analysis of fear appeal effectiveness and theories. *Psychological Bulletin* 2015; 141:1178–1204.

Address correspondence to:
 Dr. Scott M. Debb
 Department of Psychology
 Norfolk State University
 Brown Memorial Hall: 216
 Norfolk, VA 23504
 E-mail: smdebb@nsu.edu