Predicting Students' Security Behavior Using Information-Motivation-Behavioral Skills Model

Ali Farooq, Debora Jeske, Jouni Isoaho

Predicting Students' Security Behavior Using Information-Motivation-Behavioral Skills Model

Ali Farooq[1], Debora Jeske[2] and Jouni Isoaho[1]

[1] University of Turku, Turku, Finland
[2] University College Cork, Ireland
[1]{alifar, jouni.isoaho}@utu.fi
[2]adminapsych@ucc.ie

Abstract. The Information-Motivation-Behavioral Skills (IMB) Model has shown reliability in predicting behaviors related to health and voting. In this study, we examine whether the IMB Model could predict security behavior among university students. Using a cross-sectional design and proxy IMB variables, data was collected from 159 Finnish students on their security threats' awareness (representing IMB's information variable), attitude toward information security and social motivation (replacing IMB's motivation variable), self-efficacy and familiarity with security measures (variables related to IMB's behavioral skills), and self-reported security behavior (IMB outcome variable). An analysis conducted with PLS-SEM v3.2 confirmed that the IMB Model was an appropriate model to explain and predict security behavior of the university students. Path analysis showed that behavioral skills measures predict security behavior directly, while students' information and motivation variables predicted security behavior through behavioral skills (self-efficacy and familiarity with security measures). The findings suggest that the security behavior of students can be improved by improving threat knowledge, their motivation and behavioral skills – supporting the use of the IMB Model in this context and combination with existing predictors.

Keywords: Information Security, Threat Knowledge, Security Behavior, IMB Model

1 Introduction

While the Internet has brought a variety of benefits to us, we are also exposed to the dark side of the Internet due to the different information security threats [1]. To mitigate these security threats, organizations implement not only technical measures [2] but also, non-technical or educational measures, such as information security policies and security education, training and awareness programs (also known as SETA programs; [3–6]). In this paper, the term security is used synonymously with information security.

Educational institutions have also been concerned about information security since the arrival of the Internet [7–9]. Educational institutions, especially higher education

institutions (HEIs), serve large populations of students, but also maintain the technological infrastructures to support learning and research activities. HEIs often manage large computer centres which collect work-related and private information of students and staff as well as crucial research information [10]. If compromised, these resources can be misused by the malicious entities. For example, leveraging denial of service attacks, phishing attacks and identity theft of staff and students (e.g. Cobalt Dickens attacks in 2018), and selling products information for financial gains.

Unlike other organisations, HEIs have two distinct groups of personnel to support, employees and students, both of which are subject to security policies [11]. Users are regarded as the weakest link in the security [12] and many young adults transitioning from school to HEIs lack awareness of how their behavior impacts network security. It is therefore important that measures are taken to improve the security behavior of both staff and students in HEIs. In this regard, it is imperative to understand users' (both staff and student) security knowledge and behaviors in the HEI context to devise appropriate strategies. Fortunately, a number of theory-driven approaches have been used in the security research to explore which factors influence behavior to identify ways in which the security behaviors of the users may be improved ([13, 14]). Among these approaches, the Protection Motivation Theory (PMT) [19–21] and Theory of Planned Behavior (TPB) ([22, 23]) has been used predominantly.

Information-Motivation-Behavioral Skills (IMB) Model was proposed in 1992 to predict health behavior [16]. The IMB Model posits that information and motivation are the key prerequisites towards a given behavior. These prerequisites connect to behavior through the behavioral skills of the person. Since then, the model has been effectively used for understanding users' behaviors as well as for designing interventions to improve users' behaviors in different domains (for example, health [19–21], voting [18] and recycling behaviors [22]). Considering Model's potential to effectively predict and change users' behavior, a few of security researchers have proposed the use of IMB model in the context of security and privacy as well (see [17, 23–25]). However, it has not yet been tested empirically in this context as yet.

The purpose of this paper is to empirically test the applicability of the IMB model to predict users' security behaviors. In doing so, we seek to contribute to the existing research in two ways. First, we wish to add to the theory-driven research in security by considering the IMB Model in the context of managing users' security behavior in HEIs. Second, we would like to improve the information security efforts of HEIs by examining the applicability of the IMB Model [16] as a suitable model to predict the security behavior of university students. The IMB Model has been used effectively as a tool for developing behavioral change programs in contexts other than education [18].

This paper summarises our effort to test the predicting powers of IMB Model in the context of security behaviors with a set of Finnish University students in 2017. The article is structured as follows. Section 2 provides a description of IMB Model and the research model constructed from this model and other theory components. Section 3 outlines the methodology and data analysis. Section 4 describes the results, followed by the discussion in Section 5.

2 Theoretical Background: The IMB Model

The IMB Model consists of two predictors (information and motivation), one proposed mediator variable (behavioral skills) and one outcome variable (behavior) (Figure 1).

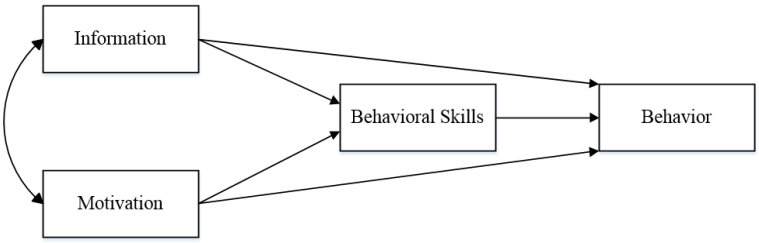

Fig. 1. The Information-motivation-behavioral skills model and its constituent variables

The first predictor in the IMB Model is ***information***. Information is a prerequisite to a correct and consistent enactment of given behavior [16, 21, 26]. An individual can hold accurate information (that will help in the performance of desired behavior) and inaccurate information (that may impede the desired behavior). Information in the context of information security and privacy may, for example, refer to awareness of the risks related to their use of various devices such as mobile phones [17]. Threat perception plays an important role in the selection of appropriate security measures ([11, 32, 33]). The assumption, therefore, is that if a person is aware of information security (risks and threats), he or she will have a more positive attitude and intention to comply to security policies [3] and behave securely [29]. Crossler and Belanger [17] suggest that the IMB Model provides an important link between information (awareness of threats/risk) and the development of skills to behave securely. We propose that threat awareness of users about security threats constitutes a measure of information users have to inform their behavior.

The second predictor of behavior in the IMB Model is ***motivation*** which is considered a critical component for engaging in and maintaining required behaviors ([20, 23, 30]). Fisher and Fisher [16, 21] posited that motivation includes both personal and social motivation. They operationalized personal motivation in terms of a user's personal attitude and socially derived motivation (which arises as a function of the perceived social support for performing a behavior). In terms of the attitude component, users are expected to engage in the desired behavior if they are highly motivated and have a positive attitude towards the desired behavior. In terms of the social motivation component, the assumption is that this may increase or decrease based on an individual's perceptions of the support one is getting from its surroundings to engage in a specific behavior. Such perceptions of support may be subject to both subjective norms [[30] (e.g., a user's perception of what kind of security behaviors other peers advocate) and descriptive norms (rules which significant leaders or managers follow, advocate and endorse publicly). Therefore, in the context of security, personal moti-

vation to engage in secure behavior is captured by the security attitude of individuals (as these would be strongly correlated), while social motivation may be a function of what users perceive to be the social support (which arise as a function of both subjective and descriptive norms) regarding security behaviors.

Behavioral skills is proposed as a mediator variable between the two predictors and security behavior in the IMB Model. An individual needs to possess the necessary skills to engage in certain behaviors, in both the health and security domain (see also [20, 23, 30]). However, there are mixed views on how behavioral skills can be measured, which led some authors to use self-efficacy measures to assess perceived capabilities to deal with challenges ([18, 31–33]). An example here is the use of self-efficacy as a proxy measure for behavioral skills in terms of patients' health-related behavior (see work by Fisher and Fisher [16, 21]). An alternative approach to using self-efficacy alone is to include some form of knowledge assessment in addition to self-efficacy ([17, 22]). Familiarity and actual knowledge have already been studied in the context of information security (for example [43] and [44]).Considering security measures familiarity here in addition to self-efficacy is important as users in a security scenario may find it difficult to select the appropriate behaviors when they are not familiar with the counter measures to combat a threat. In the context of HEIs, many users may need to not just feel capable to act in order to support security, but they also have to recognize specific threats as well as security measures that they should employ. As a result of these concerns and the existing research as well as the exploratory nature of the study, behavioral skills among HEI users may be dependent on a combination of self-efficacy (perceived capability) and subjective familiarity with security measures to counteract a threat - as both are needed for individuals to build and then engage the appropriate behavioral skills in response to potential threats.

Security behavior is proposed to be the dependent variable of the model. This includes specific behavior to counteract threats by employing specific measures such as using software against viruses, ransomware and identity theft.

In line with the discussion above, the following modified research model is proposed (Figure 2) to examine the applicability of IMB Model in the context of information security.

3 Method

3.1 Survey Design and Procedure

Quantiative methodology was adopted for the study for which data was collected using a two-part online survey which was developed using a tool called Webropol. The constructs of information, motivation and behavioral skills and demographic were part of first part, whereas, security behavior construct was measured in the second part. Participants were recruited from a large, public university in the Southwest of Finland. Prospective participants were enrolled in a four week long blended learning course on cybersecurity at the time of the study (fall 2017).

First part was administered before the start of the course, whereas, second part was shared among the students two weeks after the completion of the course. To clarify the difference between the awareness (information) and familiarity (behavioral skills), both concepts were introduced to the participants in the survey before they answered items related to threat awareness and familiarity with security measures. Threat awareness was introduced as a fleeting degree of threat knowledge, where a person has heard of a threat but may not have experienced it personally, whereas, Familiarity with security measures was referred to as a degree of knowledge where person has known a security measure through personal experience or association implying a deeper understanding (for further clarification, refer to [34]). The questionnaire took 15-20 altogether. The participants were asked to create a unique ID to connect responses from the two-part survey. While no financial or academic benefits were provided, participants were entered into a prize draw for movie tickets.

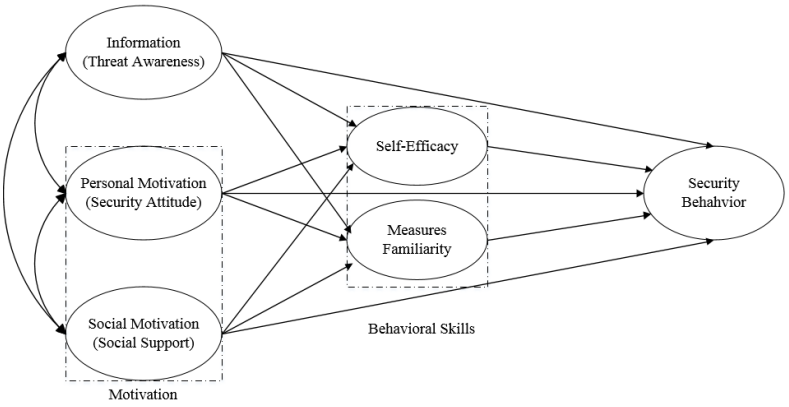

Fig. 2. Modified IMB model in the context of security behavior

3.2 Participants

All 376 enrolled students of the aforementioned course were invited to participate in the study. Out of which 169 students took the two-part survey (response rate = 45%). However, after removing incomplete responses, 159 responses were retained.

About 65% of the participants were male. The average age of the participants was 24 years (ranging from 18 to 63 years with SD = 6.94). The majority of the respondents were Bachelor level students (77%), while the rest were from a Master degree or above. Among the Bachelor level students, 45% were the 1st year, 15% were 2nd year, 6% were 3rd year, and 11% were 4th year students. About 69% of the participants were from computer science and information technology discipline, followed by 23% from the natural sciences, whereas, the rest belonged to other disciplines. The participants had an average internet experience of 14 years (SD = 4.10).

3.3 Measures

Several existing measures were utilized to assess the constructs chosen for information, motivation, behavioral skills and security behavior. Table 1 shows the operational definition of each construct (The detail of items and their sources is given in part-1 of supplement available here: https://goo.gl/AQs1XE.

Table 1. Constructs and operational definitions

Model Constructs	Operationalized Constructs	Operational definition
Information	Threat Awareness	The extent to which a participant is aware of security threats.
Motivation	Security Attitude	The personal attitude a participant has towards security (personal motivation)
	Social Support	The extent to which participant feels that others motivate for engaging in a secure behavior (social motivation)
Behavioral Skills	Self-efficacy	The extent to which participant believe he/she is equipped to deal with security threats and exhibit secure behavior.
	Measures Familiarity	The extent to which participant thinks s/he is familiar with security measures to counteract familiar threats.
Behavior	Security Behavior	The extent to which participant follow prescribed security advice.

Information. Threat awareness was chosen to provide a measure of threat information our participants were aware of. It was measured in terms of user awareness with 20 security threats (taken from [11, 34]). The list consisted of the following threats: Trojan, botnet, identity theft, cookies, virtual stalking, internet surveillance, theft/loss of devices, malware, shoulder-surfing, rogueware, theft/loss of cards and wallets, spyware, information leakage in social network, social engineering, data harvesting (applications), keylogger, virus, phishing, zero-day attack and email harvesting. In each case, participants were asked how aware they were with each threat. Answering options ranged from 1 = very poor to 5 = excellent.

Motivation. Motivation was measured in terms of two measures: attitude towards security (reflecting personal motivation) and social support (reflecting social motivation) [16]. Attitude was measured using four items, adapted from [36]. Social support was self-developed using work of [37, 38] and measured with the help of 3 items. Both constructs were measured on a 7-point scale (1 = strongly disagree to 7 = strongly agree).

Behavioral Skills. As suggested by [17], behavioral skills was measured in term of two proxies that influence skills use: the perceived self-efficacy to deal with a security challenge as well as familiarity with security measures to counteract specific threats. Self-efficacy was measured using six items (adapted from [39, 40]). The scale was similar to the one used for measuring personal motivation. The familiarity of security measures (measures familiarity) was assessed by familiarity of participants with top 20 security measures prescribed by the security experts [41]. The participants had

5-point scale (1 = not at all familiar to 5 = extremely familiar) to rate their familiarity with each measure.

Security Behavior. Self-reported security behavior of participants was measured with the help of self-developed scale consisting of 12 items. We measured the frequency of the engaging in behavior (1 = never, 2 = rarely, 3 = sometimes, 4 = often, 5 = always) related to updating operating system, anti-virus software, downloading software from trust sources, locking computer when stepping away, creating strong passwords, using unique passwords, use of password manager, use of two factor authentication, checking for https while web-surfing, be mindful for the popping up dialogue boxes, and avoid opening unexpected email attachments. Each item represents a piece of advice given by most of the security expert [42]. Measuring frequency of engagement has been considered better as compared to measuring degree of agreement. Egelman and Peer [43] used the same approach for developing security behavior intention scale (SeBIS).

Demographics. The questionnaire captured the following demographics: gender, age, education, discipline, work and Internet experience.

3.4 Data Analysis

For model testing, we used partial least squares structural equation modelling (PLS-SEM, Smart PLS 3.2) as it is particularly appropriate for estimating complex models using small sample size and non-normally distributed data ([44–46]). The model is tested in two phases: (1) measurement model testing, and (2) structural model testing. For these phases, established guidelines were followed [45, 47, 48]. Reflective constructs consist of items that show a common cause where cause flows from constructs to items, whereas, formative constructs is a composite measure summarizing a common variation through a set of items. In case of the formative construct, the causal relationship flows from items to the construct (for further differences refer to [49]) According to Chin [49], in formative construct, removal of a single item can affect the construct negatively. Our model consists of both reflective and formative constructs. Reflective model variables were three measures related to the IMB proxies for motivation (attitude and social support) and behavioral skills (in this case, self-efficacy). Formative model variables included the measures related to IMB proxies for information (threat awareness), behavioral skills (familiarity with security measures) and security behavior. The main results are briefly summarized below. (The detailed results of these are available for additional review in part-2 of the supplement available here (https://goo.gl/AQs1XE).

The results of reliability and validity assessment for reflective variables showed that the Coefficient α and composite reliability (CR) for the three reflective constructs were higher than the recommended threshold of 0.70. However, the average variance explained (AVE) of self-efficacy was below the threshold (0.50) suggested by [45]. Five items, two items (SE2 and SE5) were associated with self-efficacy (behavioral skills), two (SA2 and SA3) with security attitude (personal motivation), and one (SS2) with social support (behavioral skills) had items loading less than 0.70. Removal of two low loading items, improved AVE of self-efficacy, however, removal of

low loading items related to attitude and social support did not improve AVE of the respective variables. Therefore, as per guidelines [45, 47, 48] , low loading items of attitude and social support were retained. In the final model, both security attitude (personal motivation) and self-efficacy (behavioral skills) were measured with the help of four, whereas, social support (social motivation) was measured using three items. The HTMT ratio was below 0.85 for all the constructs, giving evidence of discriminant validity.

The quality of formative constructs was measured by assessing collinearity diagnosis and significance of formative items. In this regards, guidelines of [45] were followed. VIF for measures familiarity (behavioral skills) and security behavior was between 0.20 and 3, which was within the required threshold (VIF should between 0.20 and 5.0). However, two items (TA3 and TA5) of threat awareness (information) had values higher than the 5 (6.41 and 7.20 respectively). Removing of INFO5 from the model brought VIF for TA3 to 3.38, which was acceptable as per guidelines. Therefore, TA5 was removed from further analysis. In addition, six items (TA 18, MF11, SB1, SB4, SB10 and SB12) from measures capturing threat awareness (information), measures familiarity (behavioral skills), and security behavior did not fulfill significance criteria. Therefore, following the formative construct quality assessment, seven items were dropped, two from the measure for threat awareness (information, leaving 18 items), and one from the measure for familiarity with security measures (behavioral skills, leaving 19 items) and four from security behavior (leaving eight items).

4 Results

4.1 Validation of IMB Model

The standardized path coefficients (β), the coefficient of determination (R2) and significance ($p < .05$) of the individual paths in the estimated path analysis are shown in Figure 3. We also checked the collinearity of the structural model with the help of predictor construct's tolerance (VIF) and found to be between 1.02 and 1.68. As per [45], VIF coefficient between 0.2 and 5 shows lack of collinearity significant levels and effects in the structural model.

As shown in Figure 3, there were significant direct paths to security behavior from security attitude (IMB's motivation measure; $\beta = 0.28$, $p = 0.024$), self-efficacy (IMB's behavioral skills proxy; $\beta = 0.21$, $p = 0.035$), and familiarity with measures (also IMB's behavioral skills; $\beta = 0.23$, $p < 0.055$). There were indirect effects of information and security attitude (IMB's motivation proxy) on security behavior through self-efficacy (behavioral skills; $\beta = 0.34$, $p < .001$; $\beta = 0.28$, $p < .001$) as well as measures familiarity (IMB's behavioral skills;$\beta = 0.39$, $p = .001$; $\beta = 0.38$, $p = .001$). Social support (IMB proxy for motivation) did not have any direct or indirect significant path to security behavior. Moreover, information significantly correlate with both the personal and social motivation constructs, that is, security attitude ($r = 0.23$, $p < .05$) and social support ($r = 0.09$, $p < .05$). For detail statistics on structural model and correlation consult Tables 2 and 3.

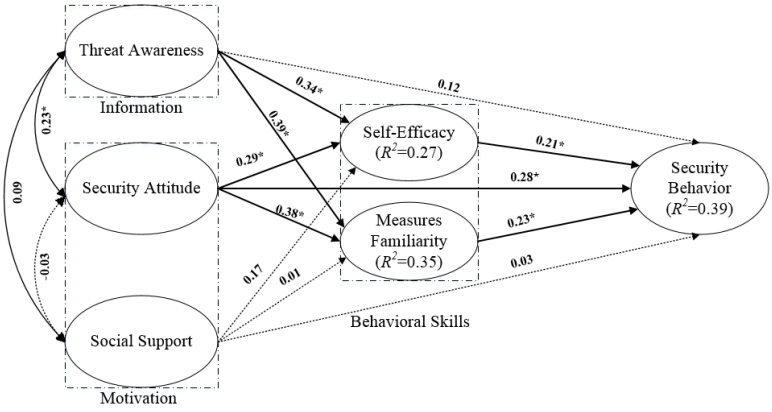

Fig. 3. IMB model constructs with path coefficients and determination coefficients. Dark arrows show a significant prediction, dotted arrows show insignificant prediction, and double edge arrows show correlations.

Table 2. Structural model statistics for IMB Model constructs. The path coefficient (β), adjusted coefficient of determination R^2, significance tested at p<0.05 with effect size f^2 . Non-significant relationships are highlighted in italic.

Path[1]	**VIF**	***β***	***t***	***R²****	***p***	**Sig.****	***f²***
TA→SE	1.07	0.34	3.06		0.002	Y	0.158
SA →SE	1.06	0.28	3.93		0.024	Y	*0.109*
SS → SE	*1.01*	*0.17*	*1.70*	0.27	*0.090*	*N*	*0.042*
TA→MF	1.07	0.39	3.46		0.001	Y	0.225
SA→MF	1.06	0.38	3.06		0.002	Y	0.216
SS → MF	*1.01*	*0.01*	*0.11*	0.35	*0.915*	*N*	*0.000*
TA →SB	*1.40*	*0.11*	*0.67*		*0.501*	*N*	*0.020*
SA→SB	1.35	0.28	2.26		0.024	Y	0.097
SS→SB	*1.05*	*0.03*	*0.29*		*0.769*	*N*	*0.001*
MF → SB	1.66	0.23	1.92		0.050	Y	0.057
SE → SB	1.47	0.21	2.11	0.39	0.035	Y	0.052

Note. [[1] TA= Threat awareness (Information), SA = Security Attitude (personal motivation), SS = Social Support (social motivation), SE = Self-efficacy (behavioral Skills), MF= Measures familiarity (behavioral Skills), SB = Security behavior. Effect size(f^2): 0.02 = low, 0.15=Medium, 0.35=large]

Table 3. Correlation matrix of measures (in relation to IMB constructs)

Constructs	**1**	**2**	**3**	**4**	**5**	**6**
Threat Awareness (Information)	1					
Security Attitude (Personal Motivation)	**0.23**	1				
Social Support (Social Motivation)	**0.09**	-0.03	1			
Self-efficacy (Behavioral Skills)	0.42	0.36	0.19	1		
Measures Familiarity (Behavioral Skills)	0.49	0.47	0.03	0.44	1	
Security Behavior	0.39	0.50	0.08	0.48	0.51	1

5 Discussion

This study examined the applicability of IMB Model in a slightly modified format in a HEI information security context. Our study shows behavioral skills (both self-efficacy and familiarity with security measures) and personal motivation (security attitude) directly predicted the security behavior of the students. Also, our proxy variables (all selected on the basis of information, motivation, and behavioral skills in the IMB Model) explained 39% of the variance in security behavior in our student sample. Furthermore, information (threat awareness) and personal motivation (security attitude) were positively associated with behavioral skills (self-efficacy as well as measures familiarity). We also found that information (threat awareness) and personal motivation (represented by security attitude) indirectly affected security behavior - through the behavioral skills variables (which operated as a mediator). Social motivation (captured in the form of social support) does not have a direct or indirect relationship with security behavior. Information and motivation variables (personal and social) also correlated with one another.

To evaluate our contribution to the study of information security in the educational context, two points need to be clarified beforehand. First, our results need to be interpreted in the context of existing theory and previous findings. Mayer et al. [15] found that self-efficacy has a reliable but weak to medium positive effect on behavioral intention in three different studies. However, in the case of attitude measures, these have been shown to a reliable medium effect on behavioral intention in security studies [15]. The results in our study confirmed the previous findings: self-efficacy had a small effect size on the security behavior ($f2$=0.05). However, in contrast to the medium effect reported for attitude [19], we found that attitude in our sample has a small effect size ($f2$=0.01) as well. As our results pertain to behavior rather than intention, it is difficult to compare these effects directly. However, given the often noted disconnect between behavioral intention and behavior (as intention may not always lead to behavior), higher effect sizes may be expected for intention rather than behavior - which may not always align with one's intention.

5.1 Recommendations

The previous two points lead us to the following recommendations for those responsible for managing information security training in HEIs. According to our results based on the IMB Model, constructs related to information (threat awareness) and motivation (based on security attitude and social norms) are crucial factors for students to acquire skills to engage in information security behaviors. However, practical knowledge is important in addition to information and motivation to employ security measures [17]. HEIs should focus on all IMB related constructs simultaneously to achieve improved security behavior. This means tackling threat awareness, personal motivation (in form of security attitudes) and behavioral skills (such as self-efficacy and familiarity with measures to counteract security threats) together, rather than just picking one of the three to improve security behavior.

Training and other interventions based on the IMB Model may improve students' security-related knowledge by: (a) increasing their access to information (e.g., through training about threats and measures), (b) raising their motivation (by increasing the perceived relevance and providing resources (social support) to perform secure behaviors), and (c) providing them with opportunities to gain and test their behavioral skills as this will increase their confidence and capability to do so when an actual threat emerges which requires immediate counteraction. All three may then hopefully improve the security behaviors of the students in HEIs, reducing institutional vulnerability to threats while also giving the students the skills to act securely when they transition into the workplace and use employer systems.

5.2 Limitations and Future Research

The study is not without limitations. For example, our cross-sectional sample was recruited from a pool of students who enrolled on a security-related course. This suggests they may have been more interested in information security compared to those who selected other courses instead. Moreover, the majority of the students were Bachelor level students belonging to computer science, information technology and engineering (STEM) disciplines. Therefore, our findings may not translate to students' behavior outside these STEM areas that may lack familiarity with threat and also behavioral skills. Furthermore, some methodological issues arise also. First, in this paper, behavioral skills (familiarity with security countermeasures) and security behavior were assessed using a self-report measures rather than objective indicators. And second, considering the nature and types of security measures, the aforementioned variables were measured as formative variables.

This leads us to four areas worthy of more investigation. One, further research is needed to establish the generalizability of our findings to other non-STEM samples. Two, moving from subjective to objective measures would hopefully be possible when assessing security skills and behaviors. As proposed in the recommendations section, it would be helpful to run security tests and countermeasure exercises (similar to health and safety trial runs) to ensure students know how to effectively respond to a threat not just in theory but also in practice. Such trials would also, if captured, generate more objective data about the behavioral skills and actual security behavior of students. If the study is replicated with the help of an IT support center, for example, actual security behavior may be captured by the IT system through the interaction of users with the system, circumventing the need for self-reported behavioral measures.

And three, it would be interesting to see the longitudinal effect of information, motivation and skills on security behavior. We had a brief interval (two weeks) between our assessment of motivation, information and behavioral skill on the one hand, and security behavior on the other. The relationship between the constructs may change over time, particularly if training is provided following the first round.

Four, security behavior may be measured in numerous ways. A thoroughly designed construct may improve the predictability of the IMB Model. In this study, security behavior was measured by asking participants to indicate which of the twelve security recommendations they follow (see also [42]). Considering that there are more

than twelve measures that a user requires for his/her information security, a concise list of important security behaviors may be identified, and security measure may be operationalized accordingly. We believe using formative structure for a holistic security behavior variable will be suitable.

6 Conclusion

The purpose of the study was to examine the predictability of a slightly modified IMB Model in the context of information security. We tested IMB model using SmartPLS SEM, and found that indeed proxies for information (threat awareness), motivation (security attitude and social support) and behavioral skills (self-efficacy and familiarity with threat measures) enabled us to predict the security behavior of 159 university students. The results showed that students with higher threat awareness, more positive security attitude, higher self-efficacy, and familiarity with security measures engaged in more secure behavior. This work proves empirically that IMB model can be used to study security behaviors of the students.

References

1. Kim, W., Jeong, O.-R., Kim, C., So, J.: The Dark Side of the Internet: Attacks, Costs and Responses. Inf. Syst. 36, 675–705 (2011).
2. Aurigemma, S., Panko, R.: A Composite Framework for Behavioral Compliance with Information Security Policies. In: 45th Hawaii International Conference on System Sciences. pp. 3248–3257. IEEE (2012).
3. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Q. 34, 523–548 (2010).
4. Pahnila, S., Siponen, M., Mahmood, A.: Employees' Behavior towards IS Security Policy Compliance. In: 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07). p. 156b–156b. IEEE (2007).
5. Abraham, S.: Information Security Behavior: Factors and Research Directions. In: AMCIS 2011 (2011).
6. D'Arcy, J., Hovav, A., Galletta, D.: User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterence Approach. Inf. Syst. Res. 20, 79–98 (2009).
7. Kerievsky, B., Bruce: Security and Confidentiality in a University Computer Network. ACM SIGUCCS Newsl. 6, 9–11 (1976).
8. Ingerman, B.L., Yang, C.: Top-Ten IT Issues, 2011. Educ. Rev. 46, 24 (2011).
9. Al-Janabi, S., Al-Shourbaji, I.: A Study of Cyber Security Awareness in Educational Environment in the Middle East. J. Inf. Knowl. Manag. 15, 1650007 (2016).
10. Katz, F.H.: The Effect of a University Information Security Survey on Instruction Methods in Information Security. In: Proceedings of the 2nd annual conference on Information security curriculum development - InfoSecCD '05. p. 43. ACM Press, New York, New York, USA (2005).
11. Farooq, A., Kakakhel, S.R.U., Virtanen, S., Isoaho, J.: A taxonomy of perceived information security and privacy threats among IT security students. In: 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015. pp. 280–286. IEEE (2016).

12. Savitz, E.: Humans: The Weakest Link In Information Security, https://www.forbes.com/sites/ciocentral/2011/11/03/humans-the-weakest-link-in-information-security/#77a4bb46de87.
13. Lebek, B., Uffen, J., Neumann, M., Hohler, B., Breitner, M.H.: Information security awareness and behavior: a theory-based literature review. Manag. Res. Rev. Inf. Manag. Comput. Secur. Iss Comput. Secur. Iss. 37, 1049–1092 (2014).
14. Howe, A.E., Ray, I., Roberts, M., Urbanska, M., Byrne, Z.: The Psychology of Security for the Home Computer User. In: 2012 IEEE Symposium on Security and Privacy. pp. 209–223. IEEE (2012).
15. Mayer, P., Kunz, A., Volkamer, M.: Reliable Behavioural Factors in the Information Security Context. In: Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES '17. pp. 1–10. ACM Press, New York, New York, USA (2017).
16. Fisher, J.D., Fisher, W.A.: Changing AIDS-risk behavior. Psychol. Bull. 111, 455–474 (1992).
17. Crossler, R.E., Bélanger, F.: The Mobile Privacy-Security Knowledge Gap Model: Understanding Behaviors. In: 50th Hawaii International Conference on System Sciences (2017).
18. Glasford, D.E.: Predicting Voting Behavior of Young Adults: The Importance of Information, Motivation, and Behavioral Skills. J. Appl. Soc. Psychol. 38, 2648–2672 (2008).
19. Robertson, A.A., Stein, J.A., Baird-Thomas, C.: Gender differences in the prediction of condom use among incarcerated juvenile offenders: testing the information-motivation-behavior skills (IMB) model. J. Adolesc. Heal. 38, 18–25 (2006).
20. Fisher, W.A., Williams, S.S., Fisher, J.D., Malloy, T.E.: Understanding AIDS Risk Behavior Among Sexually Active Urban Adolescents: An Empirical Test of the Information–Motivation–Behavioral Skills Model. AIDS Behav. 3, 13–23 (1999).
21. Fisher, J.D., Fisher, W.A., Harman, J.J.: An Information-Motivation-Behavioral Skills Model of Adherence to Antiretroviral Therapy. Heal. Psychol. 25, 462–473 (2006).
22. Seacat, J.D., Northrup, D.: An information–motivation–behavioral skills assessment of curbside recycling behavior. J. Environ. Psychol. 30, 393–401 (2010).
23. Khan, B., Alghathbar, K.S., Khan, M.K.: Information Security Awareness Campaign: An Alternate Approach. In: International Conference on Information Security and Assurance. pp. 1–10. Springer, Berlin, Heidelberg (2011).
24. Mariani, M.G., Zappalà, S.: PC Virus Attacks in Small Firms: Effects of Risk Perceptions and Information Technology Competence on Preventive Behaviors. TPM esting, Psychom. Methodol. Appl. Psychol. 21, 51–65 (2014).
25. Pattinson, M.R., Anderson, G., Analyses, A.: End-user Risk-taking Behaviour: an application of the IMB model. In: 6th Annual Security Conference (2007).
26. Fisher, J.D., Fisher, W.A., Misovich, S.J., Kimble, D.L., Malloy, T.E.: Changing AIDS risk behavior: Effects of an intervention emphasizing AIDS risk reduction information, motivation, and behavioral skills in a college student population. Heal. Psychol. 15, 114–123 (1996).
27. Huang, D.-L., Rau, P.-L.P., Salvendy, G.: Perception of information security. Behav. Inf. Technol. 29, 221–232 (2010).
28. Yeh, Q.-J., Chang, A.J.-T.: Threats and countermeasures for information system security: A cross-industry study. Inf. Manag. 44, 480–491 (2007).
29. Farooq, A., Isoaho, J.J., Virtanen, S., Isoaho, J.J.: Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors. In: Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015. pp. 352–359. IEEE (2015).
30. Ajzen, I.: The theory of planned behavior. Organ. Behav. Hum. Decis. Process. 50,

179–211 (1991).
31. Chang, T., Shan, Y., Liu, S., Xiao-yue, S., Li, Z., Du, L., Li, Y., Douqing, G., Gao, D.: A study on the Information-Motivation-Behavioral Skills Model among Chinese Adults with Peritoneal Dialysis. J. Clin. Nurs. 27, 1884–1890 (2018).
32. Compeau, D., Higgins, C.A., Huff, S.: Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study. MIS Q. 23, 145 (1999).
33. Compeau, D.R., Higgins, C.A.: Application of Social Cognitive Theory to Training for Computer Skills. Inf. Syst. Res. 6, 118–143 (1995).
34. Jeske, D., van Schaik, P.: Familiarity with Internet threats: Beyond awareness. Comput. Secur. 66, 129–141 (2017).
35. Kruger, H., Drevin, L., Steyn, T.: A vocabulary test to assess information security awareness. Inf. Manag. Comput. Secur. 18, 316–327 (2010).
36. Taylor, S., Todd, P.A.: Understanding Information Technology Usage: A Test of Competing Models. Inf. Syst. Res. 6, 144–176 (1995).
37. Zimet, G.D., Dahlem, N.W., Zimet, S.G., Farley, G.K.: The Multidimensional scale of perceived social support. Artic. J. Personal. Assess. 52, 30–41 (1988).
38. Hupcey, J.E.: Clarifying the social support theory-research linkage. J. Adv. Nurs. 27, 1231–1241 (1998).
39. Anderson, C.L., Agarwal, R.: Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. MIS Q. 34, 613–643 (2010).
40. Thompson, N., McGill, T.J., Wang, X.: "Security begins at home": Determinants of home computer and mobile device security behavior. Comput. Secur. 70, 376–391 (2017).
41. Reeder, R., Ion, I., Consolvo, S.: 152 Simple Steps to Stay Safe Online: Security Advice for Non-tech-savvy Users. IEEE Secur. Priv. (2017).
42. Ion, I., Reeder, R., Consolvo, S.: "...no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In: 2015 Symposium on Usable Privacy and Security. pp. 327–340 (2015).
43. Crossler, R., Belanger, F.: The Quest for Complete Security Protection: An Empirical Analysis of an Individual's 360 Degree Protection from File and Data Loss. AMCIS 2012 Proc. (2012).
44. Ringle, C.M., Smith, D., Reams, R.: Partial least squares structural equation modeling (PLS-SEM): A useful tool for family business researchers. J. Fam. Bus. Strateg. 5, 105–115 (2014).
45. Hair Jr, J.F., Hult, G.T., Ringle, C., Sarstedt, M.: A primer on partial least squares structural equation modeling (PLS-SEM). Sage Publishers (2016).
46. Lowry, P.B., Gaskin, J.: Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It. IEEE Trans. Prof. Commun. 57, 123–146 (2014).
47. Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E., Tatham, R.L.: Multivariate data analysis. Prentice Hall, Upper Saddle River, NJ (2010).
48. Henseler, J., Ringle, C.M., Sarstedt, M.: A new criterion for assessing discriminant validity in variance-based structural equation modeling. J. Acad. Mark. Sci. 43, 115–135 (2015).
49. Chin, W.W.: The partial least squares approach to structural equation modeling. In: George A. Marcoulides (ed.) Modern methods for business research. pp. 295–336 (1998).