Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

Understanding the role of the bring-your-own-device policy in mobile learning behavioral usage

Nida AL-Sous[a], Dmaithan Almajali[a*] and Zulkhairi Dahalin[b]

[a]*Applied Science Private University, Malaysia*
[b]*University Utara Malaysia, Malaysia*

C H R O N I C L E

Article history:
Received: May 3, 2022
Received in revised format: June 25, 2022
Accepted: July 3, 2022
Available online: July 3 2022

Keywords:
Attitude
Subjective norms
Information security awareness
BYOD

A B S T R A C T

The determinants of bring-your-own-device (BYOD) use protection intentions affecting BYOD usage protection behaviors were examined in this study. The determinants of employees' behavioral intention to use and their actual protection behavior in protecting their devices BYOD environment were identified. Jordanian residents aged 18 and above, with mobile learning behavioral usage awareness, made up the study population. A survey questionnaire was used to obtain the data, while the proposed research model was tested using structural equation modeling (SEM). The results show positive impact of BYOD usage protection intention on mobile learning behavioral usage, while attitude showed insignificant impact on BODY usage protection intention. Subjective norms significantly affected BYOD usage protection intention, while information security awareness showed insignificant impact on BYOD usage protection intention.

1. Introduction

The use of mobile devices in medical education and healthcare delivery is increasingly more common and crucial, especially following the progressions in information and communication technologies (ICTs). Personal mobile device usage in medical schools and healthcare facilities allows smooth communication and collaboration, as well as easy access to medical information (Al Ayubi et al., 2016; Chang et al., 2013). In addition, it allows flexible and timely self-paced learning (Ally, 2013; Hardyman et al., 2013). At the same time, certain issues have to be addressed pertaining to mobile device usage in this context, such as incorrect usage of mobile devices like the use of mobile devices that lack security features (Nguyen, 2019; Wani et al., 2020). Also, the lack of regulations to medical applications adds to the problem (Lewis & Wyatt, 2014). As the use of mobile devices is widespread today, there is also an issue relating to etiquette, as can be exemplified in the problems of distracted learning and doctoring (O'Connor et al., 2014; Tran et al., 2014), in addition to poor control measures of infection (O'Connor et al., 2014).

In medical education and healthcare environments, mobile devices for medical education and healthcare delivery are either provided by the institution or personally owned (Meneghetti, 2013; Williams, 2014). However, the use of personal mobile devices in medical education and healthcare delivery is increasingly favored and promoted, owing to several benefits, and the correct and safe usage of these devices are being fostered as well (Disterer & Kleiner, 2013; Weeger et al., 2016). This had led to the policy of bring-your-own-device (BYOD). BYOD policy is cost effective to the institution, as the cost is shifted from the institution to the user. Nonetheless, BYOD is not easy to implement owing to the varied conceptualizations and the

* Corresponding author.
E-mail address: zul@uum.edu.jo (D. Almajali)

doi: 10.5267/j.ijdns.2022.7.001

widespread usage of mobile devices in various environments. BYOD is generally the usage of personal mobile devices for medical education and healthcare delivery purposes (Dimond et al., 2016; O'Connor et al., 2014).

Mobile technologies are clearly an outstanding and prized invention by man (Al-Emran, 2020). Mobile devices as a constituent of mobile technologies, comprise wireless information and communications technologies, allowing users from various places to be consistently connected with one another simultaneously, and at all times (Zaidi et al., 2021). Through these technologies, people could acquire knowledge as well, at any time and from any place. Indeed, mobile devices allow information processing and contribution among users (Al-Emran, 2020). Notably, smartphones and tablets, mobile devices, are increasingly useful in the workplace, and in fact, the policy of Bring Your Own Devices (BYOD) is a current trend among organizations. BYOD involves the use of smartphones, mobile phones, laptops, and tablets by organization members including employees. The use of these devices allows more flexibility in task completion – the employees could complete their tasks even when they are not at the office.

BYOD and IT consumerization co-exist as these personal mobile devices have become part of business and government operation (Weeger et al., 2020). In BYOD policy, members of an organization or institution use their mobile devices in their work completion. In this regard, smartphones are increasingly being used as the tool for accessing the internet resources (Oberlo, 2020). Turner (2021) accordingly reported that in the year 2021, there would be approximately 6.3 billion smartphone users all over the world, and about 5.22 billion users would be using their mobile devices to complete their work-related tasks. In describing a BYOD environment, Hughes (2016) explained that employees would utilize their devices to gain access to the networks of their organizations, and to obtain the work related data. To this end, the use of mobile devices like smartphones would save employees from having to bring various devices for work and personal use, and from having to use numerous device makes and models.

The outbreak of COVID-19 pandemic has intensified the trend of BYOD, owing to the switch from the conventional work-from-office policy to the work-from-home policy, among government institutions and corporate bodies all over the world (Vrhovec & Markelj, 2018). The switch from the work-from-office policy to work-from-home policy was mainly factored by movement restrictions and social distancing regulations as among the methods to curb the spread of COVID-19. In this regard, organizations adopted BYOD so that employees could still perform their work as usual, despite the severity of the pandemic. Among universities, the use of mobile devices in learning and teaching is increasingly popular. Like other institutions, universities also have been making attempts to leverage on the advantages of personal mobile device usage. Hence, the use of BYOD policy in the delivery of education is increasingly common in universities today.

Despite the effectiveness and benefits of BYOD policy in several institutions, this policy has not been adequately examined. In fact, there has been a lack of research covering this subject. As such, the present study attempted to fill the void. With concern over the issue of safety in BYOD, the present study attempted to identify the factors affecting BYOD usage protection intention and its effect on mobile learning (ML) behavioral usage. Accordingly, a comprehensive model was proposed in this study. The model was grounded upon some common acceptance theories namely ATT, SN, ISA and BUPI. The impact of BYOD on ML behavioral intention to use was explored. Also, based on TBP theory, this study examined how the factors can affect ML behavior usage. Notably, the present study would be the first one exploring BYOD on ML usage.

2. Literature review and hypothesis development

The present study examined the determinants of students' protection intention and their protection behavior in their devices usage within the environment of BYOD. Accordingly, a model was proposed in this study, as can be viewed in the following Fig. 1. The model was underpinned by TRA as its major underpinning theory, and TRA has been applied in studies on information security. Social behavioral theories were also included in the model, in addition to the inclusion of the factors of attitude, subjective norm, information security awareness, protection intention and behavior use intention.

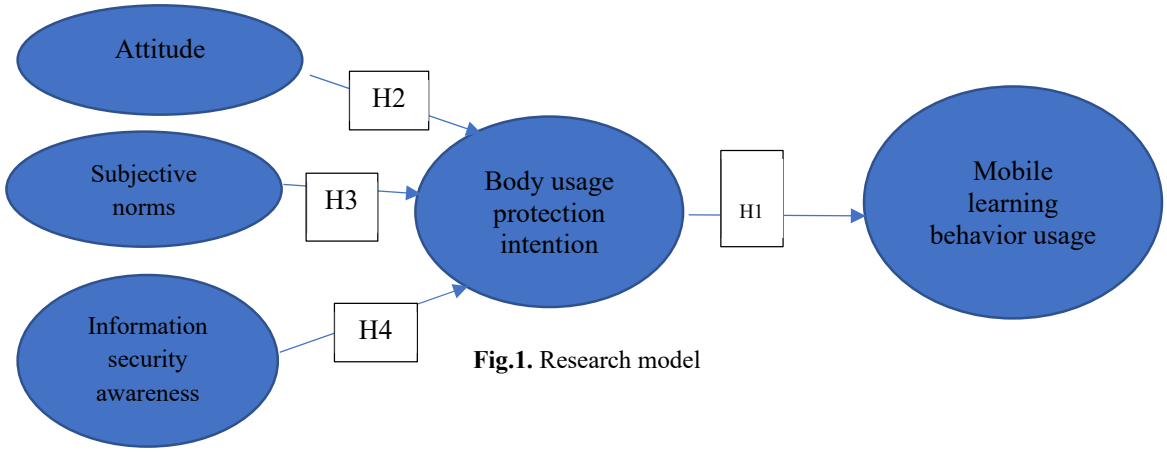

Fig.1. Research model

3.1 Theory of reasoned action (TRA)

Theory of reasoned action (TRA) (Fishbein & Ajzen, 1980) illustrates the behaviors of people under the control of individuals. TRA posits that the behavior of a person is mainly determined by his or her intention to execute that behavior. In essence, it encompasses how far the person is willing to perform that behavior. There are two factors affecting behavioral intention namely the attitude of the person towards that behavior, and subjective norms (Ajzen, 2020). The former concerns the evaluation of the person towards the consequences of performing that behavior, while the latter concerns the viewpoint of the person towards social pressure on performing (or not performing) that behavior (Fishbein & Ajzen, 1980).

TRA proposes a linear relationship, whereby attitude and subjective norm affect behavioral intention, and thus, both factors determine a person's actual behavior. As such, greater social pressure and better attitude towards certain behavior will increase the likelihood of performing the behavior. Among the strong points of TRA are: it is simple, has good explanatory power, and able to use various combinations of factors in linearly and sequentially determining an individual's behavior (Boxer & Thompson, 2020; Ajzen, 2020).

TRA posits that behavior is determined by the intentions to perform the behavior, but intention has been used as a dependent variable in past studies. In other words, intention has been often determined by other variables. Hence, in describing protection intention (PI), it could be understood as a protection motive that sustains, guides, and initiates the intentions of individuals to perform the precautionary behavior proposed (Milne et al., 2002). Therefore, the present study hypothesized that:

H_1: *BYOD usage protection intention has a positive influence on mobile learning behavioral usage.*

Attitude (ATT) refers to the general evaluation of a person towards performing the actual behavior, and attitude can be either positive or negative (Hina & Dominic, 2017; Ifinedo, 2012). Among users of social networks, their behavior (attitude) is influenced by factors like age, gender, and career (Dhawan et al., 2014). Relevantly, an Information Security Culture (ISC) model was introduced by Nasir et al. (2019), with the purpose of increasing the effectiveness of employees' protection behavior in an organization. The model included seven characteristics that investigate its impact on workers' Information Security Policy (ISP) compliance behavior, and attitude was one of the model's characteristics. ISP was expected to affect the attitude of employees towards ISP compliance, while the intention of employees to comply with ISP was affected by their attitude towards ISP compliance, and so, this study proposed the following:

H_2: *Attitude has a positive influence on BYOD usage protection intention*.

Subjective Norms (SN) are the belief that the surrounding individuals could influence a person in performing certain behavior (Thompson et al., 2017). In their study on the impacts of subjective norms on behavior intention, Martens et al. (2019) found subjective norms a strong predictor of protective behavior. Meanwhile, Safa et al. (2015) found significant impact of information security policies on the establishment of subjective norms on information security behavior in an organization. The hypothesis below was therefore proposed:

H_3: *Subjective norm has a positive influence on BYOD usage protection intention*.

Information Security Awareness (ISA) relates to the level to which all employees are aware of the value of information security policies, rules, and regulations, and feel accountable in safeguarding the information of their organization via displaying appropriate behaviors (Kaur & Mustafa, 2013; McCormac et al., 2017). Meanwhile, in their study, Ortiz et al. (2017) classed ISA into two categories as follows: general information security awareness (GISA) and information security policy awareness (ISPA). Between both, ISA is crucial in removing security breaches risks in organizations. As such, the present study established the following hypothesis:

H_4: *Information security awareness positively influences BYOD usage protection intention*.

4. Methodology

4.1 Sample and data collection procedure

Jordanian residents aged 18 and above, with understanding of mobile learning behavioral usage (at least) made up the study population. These specific Jordanians were chosen as the study population because, in general, an 18-year-old would have sufficient understanding of the technology. However, as affirmation, the potential participants were to answer the criteria fulfillment questions in the questionnaire; there were two exit questions to be answered by the respondents, one being the question on their age and residency, while the other being an affirmation question on their familiarity with mobile learning behavioral usage.

A sampling frame with a complete list of potential mobile learning consumers in Jordan was impossible to obtain, and so, this study had opted to utilize convenience sampling method as it was the most appropriate one for the study context. A total of 425 respondents were involved in this study, and 400 valid responses were obtained (94.1% response rate). The items in the questionnaire were equipped with a seven-point Likert scale (1 to denote "Strongly Disagree" to 7 to denote "Strongly Agree"). Specifically: items on mobile learning behavioral usage were based on Ameen et al. (2021) and Thompson et al.

(2017); items on BYOD usage protection intention were based on Chon et al. (2018) and Bulgurcu et al. (2010); items on attitude were based on Ameen et al. (2021) and Musarurwa et al. (2019); items on subjective norms were based on Ameen et al. (2021) and Herath and Rao (2009); and items on information security awareness were based on D'Arcy et al. (2009) and Haeussinger and Kranz (2013).

4.2 Respondents' demographic profile

From the data obtained: the majority of respondents were male at 52.2%; the majority (53.7%) were of the age of 20 or less; half of the overall respondents were high school leavers or had lower educational qualifications; and 150 respondents (37.5%) expressed that their knowledge of technology was of high level. Fig. 2 presents the details.

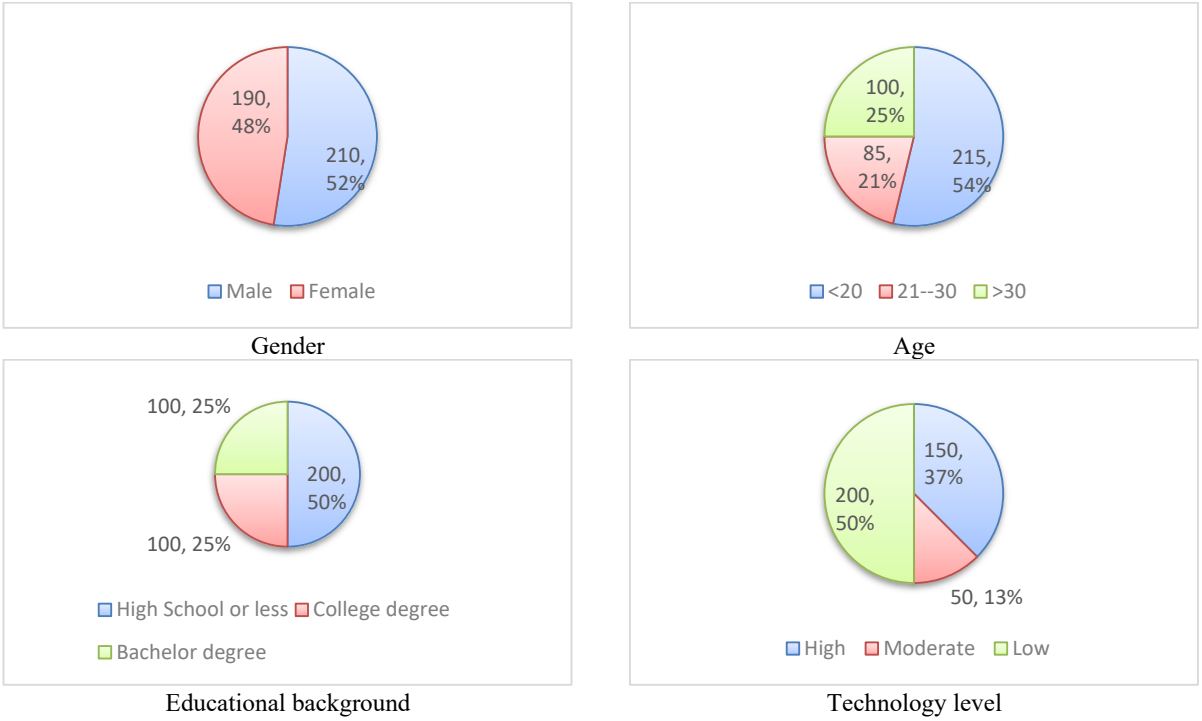

Fig. 2. Characteristics of the respondents. (N = 400)

5. Data Analysis and Result

SEM was used in this study, and prior to its execution, the reliability of correlation was measured using Cronbach's Alpha. Hair et al. (2019) had recommended the values between 0.60 and 0.70 for Cronbach's Alpha for reliability affirmation. As displayed in Table 1, the scored values were between 0.84 and 0.91, and thus, reliability was affirmed. Further, as shown in Table 3, the compound reliability values were between 0.73 and 0.94, which were larger than the proposed cutoff value of 0.60. In the measurement model, constructs' validity needs to be ascertained, particularly in terms of convergent validity and discriminant validity, as detailed below.

Table 1
Reliabilities of the scales (N = 400)

Constructs	Number of items	Indicators	Cronbach's alpha
Attitude	5	ATT1-ATT5	0.91
Subjective norms	5	SN1-SN5	0.87
Information security awareness	6	ISA1-ISA6	0.84
Body usage protection intention	4	BUPI1-BUPI4	0.88
Mobile learning behavior usage	5	MLBU1-MLBU5	0.90

5.1 Convergent Validity

Convergent validity is affirmed if the scale indicators load together on one construct. Schwab (1982) indicated that convergence is affirmed when standard regression weights are significant. Schwab (1982) further added that high load factor denotes strong representation of the scales of the combinations. The standard regression weights of the research indicators were examined, and low load was found among the underlying variables – values smaller than 0.50 would be considered as low load (Newkirk & Lederer, 2006), as can be viewed for ATT3, ATT4, SN5, ISA6 and MLBU5. Those items with low load were removed. The details can be viewed in Table 2.

5.2 Discriminant Validity

Test of discriminant validity is carried out to affirm that the items absolutely measure different constructs and are absolutely evaluating different constructs. Several tests can be used in testing the discriminant validity. For instance, Fronell and Larker (1981) proposed evaluating the extracted mean co-contrast (AVE) by latent combinations. Equally, discriminant validity can be determined by examining the relations between research structures to identify any significant correlations between them. Here, if extremely large correlations exist, the model can be said to lack discriminant validity. Fronell and Larcker (1981) stated that discriminant validity can be affirmed if the AVE for each construct is greater than the square link between that construct and any other structures. Fronell and Larker's (1981) formula was used in this study, in determining the model's discriminant validity. Hence, the mean variance extracted from a latent structure was computed, and as shown in Table 3, the values were all between 0.65 and 0.81, and so, the combinations explained 50 percent or more of the variance. As such, discriminant validity was affirmed. Additionally, as can be viewed in Table 3, the AVE values were all greater than the square associations for each set of structures, demonstrating the significant differentiation of the structures by the study measures.

Table 2
Reliability and factor loadings.

Construct	Factor loading	Composite reliability
Attitude		0.92
ATT1	0.633	
ATT2	0.511	
ATT5	0.568	
Subjective norms		0.73
SN1	0.577	
SN2	0.644	
SN3	0.559	
SN4	0.538	
Information security awareness		0.81
ISA1	0.501	
ISA2	0.520	
ISA3	0.504	
ISA4	0.641	
ISA5	0.711	
Body usage protection intention		0.94
BUPI1	0.562	
BUPI2	0.633	
BUPI3	0.546	
BUPI4	0.555	
Mobile learning behavior usage		0.83
MLBU1	0.550	
MLBU2	0.576	
MLBU3	0.632	
MLBU4	0.644	

5.3 Assessment of Measurement Model

Maximum probability (ML) estimate was used in this study in determining the statistical effect on the model's suitability model for the dataset. ML is regarded as fitting for SEM because ML is appropriate for small sample sizes (100 to 200). Further, ML as a commonly used estimation method, can be used in estimating all model parameters concurrently. Another indicator is the $\chi 2$ / df ratio. Its application necessitates three values or less, in order that the model could be regarded as acceptable. Here, smaller the percentage value is sought because it means better fit. James et al. (1982) had recommended the ratio of 2-5 for better fit. In this study, AGFI, NFI, IFI, TLI, and CFI values should fall in the range between 0.80 and 0.90 to be classed as acceptable. Meanwhile, RMSEA value considers the model's goodness-of-fit, with value between 0.05 and 0.08 as acceptable. Table 4 accordingly presents the details of the measurement model fit.

Table 3
AVE and square of correlations between constructs.

	ATT	SN	ISA	BUPI	MLBU
ATT	0.65				
SN	0.773	0.81			
ISA	0.512	0.572	0.77		
BUPI	0.801	0.507	0.632	0.72	
MLBU	0.741	0.533	0.655	0.71	0.67

(Note: Diagonal elements are the average variance extracted for each of the five constructs. Off-diagonal elements are the squared correlations between constructs.)

Table 4
Fit indices for measurement and structural model.

Quality of fit measure	Recommended value	Measurement model	Structural model
x2/df	2 to 5	1.21	2.9
AGFI	0.80 to 0.90	0.41	0.85
CFI	0.80 to 0.90	0.53	0.96
TLI	0.80 to 0.90	0.55	0.86
IFI	0.80 to 0.90	0.61	0.88
NFI	0.80 to 0.90	0.78	0.84
RMSEA	0.05 to 0.08	0.014	0.070

Hypotheses Testing and Result of the Study

Table 5 shows the hypotheses test results, including the CR estimate for each parameter. As shown, H1 was supported, which affirmed the positive significant impact of BOYD usage protection intention on mobile learning behavioural usage (P = 0.014).

Another supported hypothesis was H3, which affirmed the positive significant impact of subjective norms on BOYD usage protection intention (P = ***). Contrariwise, H2 was unsupported because the results were showing insignificant impact of attitude on BOYD usage protection intention (P =0.114). H4 was unsupported as well, which means that information security awareness did not have a significant impact on BOYD usage protection intention (P = 0.221).

Table 5
Summary of proposed results for the theoretical model

Research proposed paths	t-value (CR)	Coefficient value (std. estimate)	P-value	Results
BUPI → MLBU	3.16	1.13	0.014	Supported
ATT → BUPI	2.110	1.133	0.114	Not Supported
SN → BUPI	2.531	1.20	***	Supported
ISA → BUPI	2.100	3.144	0.221	Not Supported

(***P ≤ 0.005, **P ≤ 0.01, *P ≤ 0.05). Notes: Path = Relationship between independent variable on dependent variable; C.R = Critical ration; S.E = Standard error; P = Level of significance.

6. Discussion

The study results affirmed the aptness of TRA as a promising theoretical framework for comprehending the factors determining the decision of employees to be involved in BYOD protection behaviors. It was predicted in H1 that intentions to perform protection behaviors can significantly affect actual protection behavior, and the results affirmed the prediction. Hence, employees with the intention to safeguard their devices in a BYOD environment will have greater inclination to show protection behavior. As predicted in H3, subjective norms would significantly impact protection intention, and the results affirmed this prediction. This result affirms the findings of some past studies that employees are impelled by the decisions of their peers and superior in BYOD's usage and in complying to BYOD's protection policies of their organization (Thompson et al., 2017; Rajab & Eydgahi, 2019).

Meanwhile, the results show no significant impact of information security awareness on protection intention (H4), and this contradicted the findings of Sommestad et al. (2019) who found that employees are well aware of the potential risks and security threats when they use their personal devices. Another unsupported prediction was on the impact of attitude on protection intention (H2), as the results show non-significant influence of attitude. This contradicts Tsai et al.,2016, Topa and Karyda (2015) and Nasir et al. (2019) who reported that attitude can significantly impact protection intention and protection behavior.

7. Implication

This study increases the theoretical knowledge on the factors affecting the protection intention relating to BYOD usage protection behaviors. Specifically, this study initiated the empirical scrutiny of the factors of BYOD protection intentions affecting BYOD protection behaviors. In this regard, the proposed conceptual model could increase the awareness of organizations of the determinants of BYOD protection intentions enterprises and facilitate in dealing with the impacts of these factors on employee behavior. Past studies on BYOD were mostly focusing on technological problems faced during BYOD implementation, while the human factors were not addressed, in assuring information security (Palanisamy et al., 2020; Grassegger & Nedbal, 2021). Somehow, it is not enough to focus solely on the technical elements in assuring information security (Grassegger & Nedbal, 2021).

In practice, this study would be of value to both policymakers and strategists, owing to the importance of understanding the causes of BYOD protection behaviors among employees, as this could prevent problems like data leakage, as it could happen either intentionally or unintentionally. It is the responsibility of employers and organizations to assure secured data assets, which could be achieved through BYOD usage protection. With the widespread use of smartphones, BYOD policy is only natural. For decision-makers, the findings of this study could facilitate them in fostering protection behavior among organization members. Among government personnel especially, the increased BYOD usage security behavior could increase performance.

8. Conclusion, limitation and further research

The present study identified and evaluated the determinants of BYOD use protection intentions that affect BYOD usage protection behaviors. The results show a positive impact of BYOD usage protection intention on mobile learning behavioral usage, while ATT showed insignificant impact on BODY usage protection intention. SN significantly affected BYOD usage protection intention, while ISA showed insignificant impact on BYOD usage protection intention. For this purpose, a conceptual model was proposed. Notably, the present study examined BYOD usage at an individual level, and so, similar studies should be carried out at the organizational level. This could facilitate the improvement of the strategies for BYOD protection policy at both levels (individual and organizational).

References

Ajzen, I. (2020). The theory of planned behavior: Frequently asked questions. *Human Behavior and Emerging Technologies, 2*(4), 314-324. https://doi.org/10.1002/hbe2.195

Al Ayubi, S. U., Pelletier, A., Sunthara, G., Gujral, N., Mittal, V., & Bourgeois, F. C. (2016). A mobile app development guideline for hospital settings: Maximizing the use of and minimizing the security risks of" bring your own devices" policies. *JMIR mHealth and uHealth*, *4*(2), e4424.

Al-Emran, M. (2020). Mobile learning during the era of COVID-19. *Revista Virtual Universidad Católica Del Norte*, *61*, 1–2.

Ally, M. (2013). Mobile learning: From research to practice to impact education. *Learning and Teaching in Higher Education: Gulf Perspectives*, *10*(2), 3-12.

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior, 114*(April 2020), 106531. 39 https://doi.org/10.1016/j.chb.2020.106531

Boxer, M., & Thompson, N. (2020). Herd behaviour in cryptocurrency markets. *31st Australasian Conference on Information Systems, Wellington.* https://espace.curtin.edu.au/handle/20.500.11937/81762

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), 523-548.

Chang, I. J., Huang, R., He, W., Zhang, S. K., Wang, S. M., Zhao, F. H., ... & Qiao, Y. L. (2013). Effect of an educational intervention on HPV knowledge and vaccine attitudes among urban employed women and female undergraduate students in China: a cross-sectional study. *BMC Public Health, 13*(1), 1-8.

Chon, B. S., Lee, J. K., Jeong, H., Park, J., & Park, J. (2018). Determinants of the Intention to Protect Personal Information among Facebook Users: *ETRI Journal, 40*(1), 146–155. https://doi.org/10.4218/etrij.2017-0082.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Dhawan, S., Singh, K., & Goel, S. (2014). Impact of privacy attitude, concern and awareness on use 2 of online social networking. *Proceedings of the 5th International Conference on Confluence 2014: 3 The Next Generation Information Technology Summit,* 14–17. 4

Dimond, R., Bullock, A., Lovatt, J. and Stacey, M. (2016). Mobile learning devices in the workplace: 'as much a part of the junior doctors' kit as a stethoscope?. *BMC Medical Education, 16*(1), 1-9.

Disterer, G., & Kleiner, C. (2013). BYOD bring your own device. *Procedia Technology, 9*, 43-53.

Fishbein, M., & Ajzen, A. (1980). *Understanding attitudes and predicting social behaviour.* Englewood Cliffs: Prentice Hall.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, *18*(1), 39-50.

Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science, 181*(2019), 59–66.

Haeussinger, F., &Kranz, J. (2013). Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior. *In Proceedings of the 34th International Conference on Information Systems (ICIS), Milan, Italy. Paper 1149*.

Hair, J. F., Page, M., & Brunsveld, N. (2019). *Essentials of business research methods*. Routledge.

Hardyman, W., Bullock, A., Brown, A., Carter-Ingram, S. and Stacey, M. (2013). Mobile technology supporting trainee doctors' workplace learning and patient care: an evaluation. *BMC Medical Education, 13* (1), 1-10.

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.

Hina, S., & Dominic, D. D. (2017). Need for information security policies compliance: A perspective in Higher Education Institutions. *International Conference on Research and Innovation in Information Systems, ICRIIS*, 1–6.

Hughes. (2016). BYOD and the Medical Practice.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security, 31*(1), 83–95.

James, L., Mulaik, S., & Brett, J. (1982). *Causal Analysis: Assumptions, Models, and Data.* Sage Publications, Beverly Hills.

Kaur, J., Mustafa, N. (2013). Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. *International Conference on Research and Innovation in Information Systems, ICRIIS,* 2013, 286–290.

Lewis, T.L., & Wyatt, J.C. (2014). MHealth and mobile medical apps: a framework to assess risk and promote safer use. *Journal of Medical Internet Research, 16*(9), 1-8.

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, *92*, 139-150.

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., & Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in responses. *Australasian Journal of Information Systems*, *21*, 1-12.

Meneghetti, A. (2013). Challenges and benefits in a mobile medical world: institutions should create a set of BYOD guidelines that foster mobile device usage. *Health management technology*, *34*(2), 6-7.

Milne, S., Orbell, S., & Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British journal of health psychology*, *7*(2), 163-184.

Musarurwa, A., Flowerday, S., & Cilliers, L. (2019). The bring-your-own-device unintended administrator: A perspective from Zimbabwe. *The Electronic Journal of Information Systems in Developing Countries, 85*(4), e12076.

Nasir, A., Abdullah Arshah, R., & Ab Hamid, M. R. (2019). A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. *Information Security Journal: A Global Perspective*, *28*(3), 55-80.

Newkirk, H. E., & Lederer, A. L. (2006). The effectiveness of strategic information systems planning under environmental uncertainty. *Information & Management*, *43*(4), 481-501.

Nguyen, H. V. (2019). *Cybersecurity strategies for universities with bring your own device programs* (Doctoral dissertation, Walden University).

O'Connor, P., Byrne, D., Butt, M., Offiah, G., Lydon, S., McCinerney, K., Stewart, B. and Kerin, M.J. (2014), "Interns and their smartphones: use for clinical practice", *Postgraduate Medical Journal, 90* (1060), 75-79.

Oberlo. (2020). How Many People Have Smartphones in Number of Smartphone Users in Advanced and Emerging Economies.

Ortiz, J., Chang, S. H., Chih, W. H., & Wang, C. H. (2017). The contradiction between self-protection and self-presentation on knowledge sharing behavior. *Computers in Human Behavior*, *76*, 406-416.

Palanisamy, R., Norman, A. A., & Kiah, M. L. M. (2020). Compliance with Bring Your Own Device security policies in organizations: A systematic literature review. *Computers & Security*, *98*, 101998.

Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, *80*, 211-223.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78.

Schwab, J. J. (1982). *Science, curriculum, and liberal education: Selected essays*. University of Chicago Press.

Sommestad, T., Karlzén, H., & Hallberg, J. (2019). The Theory of Planned Behavior and Information Security Policy Compliance. *Journal of Computer Information Systems, 59*(4), 344–353.

Thompson, N., McGill, T. J., & Wang, X. (2017). Security begins at home": Determinants of home computer and mobile device security behavior. *computers & security*, *70*, 376-391.

Topa, I., & Karyda, M. (2015). Identifying factors that influence employees' security behavior for enhancing ISP compliance. In *International Conference on Trust and Privacy in Digital Business* (pp. 169-179). Springer, Cham.

Tran, K., Morra, D., Lo, V., Quan, S.D., Abrams, H., & Wu, R.C. (2014). Medical students and personal smartphones in the clinical environment: the impact on confidentiality of personal health information and professionalism. *Journal of Medical Internet Research, 16* (5), 1-8.

Tsai, S., Lv, N., Xiao, L., & Ma, J. (2016). Gender differences in weight-related attitudes and behaviors among overweight and obese adults in the United States. *American journal of men's health*, *10*(5), 389-398.

Turner, F. (2021). From counterculture to cyberculture. In *From Counterculture to Cyberculture*. University of Chicago Press.

Vrhovec, S., & Markelj, B. (2018). Relating mobile device use and adherence to information security policy with data breach consequences in hospitals. *Journal of Universal Computer Science, 24*(5), 634–645.

Wani, T.A., Mendoza, A., & Gray, K. (2020). Hospital bring-your-own-device security challenges and solutions: systematic review of gray literature. *JMIR mHealth and uHealth, 8* (6), e18175.

Weeger, A., Wang, X., & Gewald, H. (2016). IT consumerization: BYOD-program acceptance and its impact on employer attractiveness. *Journal of Computer Information Systems, 56* (1), 1-10.

Williams, J. (2014). Left to their own devices how healthcare organizations are tackling the BYOD trend. *Biomedical Instrumentation & Technology*, *48*(5), 327-339.

Zaidi, S. F. H., Osmanaj, V., Ali, O., & Zaidi, S. A. H. (2021). Adoption of mobile technology for mobile learning by university students during COVID-19. *International Journal of Information and Learning Technology*, *38*(4).