Environmental Uncertainty and End-User Security Behaviour: A Study During the COVID-19 Pandemic

Popyeni Kautondokwa, Zainab Ruhwanya, Jacques Ophoff

Environmental Uncertainty and End-User Security Behaviour: A Study During the COVID-19 Pandemic

Popyeni Kautondokwa[1][0000−0001−9001−7313], Zainab Ruhwanya[1][0000−0003−2339−7154], and Jacques Ophoff[1,2][0000−0003−0634−5248]

[1] University of Cape Town, Cape Town, South Africa
KTNPOP001@myuct.ac.za, zainab.ruhwanya@uct.ac.za
[2] Abertay University, Dundee, UK
j.ophoff@abertay.ac.uk

Abstract. The COVID-19 pandemic has forced individuals to adopt online applications and technologies, as well as remote working patterns. However, with changes in technology and working patterns, new vulnerabilities are likely to arise. Cybersecurity threats have rapidly evolved to exploit uncertainty during the pandemic, and users need to apply careful judgment and vigilance to avoid becoming the victim of a cyber-attack. This paper explores the factors that motivate security behaviour, considering the current environmental uncertainty. An adapted model, primarily based on the Protection Motivation Theory (PMT), is proposed and evaluated using data collected from an online survey of 222 respondents from a Higher Education institution. Data analysis was performed using Partial Least Squares Structural Equation Modelling (PLS-SEM). The results confirm the applicability of PMT in the security context. Respondents' behavioural intention, perceived threat vulnerability, response cost, response efficacy, security habits, and subjective norm predicted self-reported security behaviour. In contrast, environmental uncertainty, attitude towards policy compliance, self-efficacy and perceived threat severity did not significantly impact behavioural intention. The results show that respondents were able to cope with environmental uncertainty and maintain security behaviour.

Keywords: Information Security · Protection Motivation Theory · Theory of Planned Behaviour · Environmental Uncertainty · COVID-19.

1 Introduction

In recent years, the world has seen an exponential rise in cybersecurity incidents, and many of these incidents can be attributed to human error [1]. Although many of these incidents have occurred in corporate environments, cybersecurity incidents, such as data breaches, have also increased in Higher Education Institutions (HEIs) [2]. A large number of HEI worldwide experienced an increase in cyber-attacks in 2020. The environmental uncertainty and fear caused

by the COVID-19 pandemic have resulted in a spike in cyber-attacks. There is an increased social engineering scam, phishing, ransomware, data harvesting malware, all exploiting the COVID-19 pandemic [3]. It is essential to understand the impact this environmental uncertainty has on security behaviour, especially at HEIs, where a significant number of staff and students have adopted new technologies and working from home patterns. In the context of information security, behaviour is the actions generally related to computer use [4]. Behaviour is an essential aspect of studying information security, and one of the research's critical end goals is to influence positive security behaviour [5].

Security behaviour is at the heart of any organisations security culture; the attitude and intentions of the individual dictate information security behaviour. Good security behaviour is typically associated with compliance to set policies and guidelines, while bad security behaviour is attributed to non-compliance [5]. Factors that motivate security behaviour are generally drawn from existing research models such as the Protection Motivation Theory (PMT) and the Theory of Reasoned Action (TRA) or Theory of Planned Behaviour (TPB). Although it is common to find constructs from research models other than these, they remain the most consistently applied in behavioural security studies [6].

This study aims to understand the factors that motivate end-user security behaviour at HEIs, considering the environmental uncertainty caused by the COVID-19 pandemic. Therefore, the research question is, *What are the factors that motivate end-user security behaviour at HEIs during the COVID-19 pandemic?* The paper proceeds with a review of the literature and the development of the research hypotheses. This is followed by a description of the research design. The results of data analysis are presented and discussed, whereafter the paper concludes with suggestions for further research.

2 Literature Review

2.1 Theories Related to Information Security Behaviour

In the following subsections, PMT and TPB and constructs thereof are examined, including how they are relevant in present studies on security behaviour and how they impact recent security behaviour studies. Many studies have used at least one factor deriving from these models to study the motivators for information security behaviour [7–10].

2.2 Protection Motivation Theory

The PMT is used to predict how individuals would respond under stress from threats [11]. This theoretical model has been effectively utilised in information security research pertaining to behaviour [9, 10]. Not only to measure individuals' intentions as the model is used in its purity, but also as one of the measures integrated with research models to obtain actions from behavioural intentions as demonstrated in previous studies [12].

In the PMT, it is argued that an individual's assessment of the severity and the vulnerability of a threat (threat appraisal) and the extent to which they can cope with this threat by steering particular human behaviour (coping appraisal) will determine the intention [13]. Self-efficacy is the individual's belief in their ability to mitigate the threat; this factor features in findings of studies in this review as an essential coping appraisal [13, 14]. Self-efficacy is one coping appraisal that is triggered across many contexts; because of how common it is, one can argue that self-efficacy can also be detrimental to an organisation or institution's security posture because an individual backing their ability to mitigate a threat may provide a false sense of security.

It is essential to note that coping appraisals were indiscriminately found to impact findings in previous studies [9, 8, 14]. In some instances, such as [15], all PMT factors were found to impact the respondents' security behaviour. Response cost is used to measure the costs incurred in adopting a specific response to a threat. The response efficacy is the effectiveness of the response to this threat; some findings have identified response cost and response efficacy as motivating factors in security behaviour [9, 8, 14].

2.3 Theory of Planned Behaviour

The TPB is adopted in many studies about information security behaviour, much more because it is possible to extract actual behaviour from intentions, making the TPB model unrestrictive than the PMT. Nevertheless, TPB has been used along with the PMT and viewed as a viable addition to the PMT. The TRA and TPB models are different but related; TPB is an extension of the TRA [16]; in information security, it is not uncommon to observe them being cited interchangeably. A revised version of the TPB has the attitude, perceived behaviour control and the subjective norms constructs.

In TRA and TPB, an attitude refers to the degree to which an individual has a positive or negative evaluation or appraisal of the behaviour in question [16]. The subjective norms construct' refers to social pressure to perform a particular action; this construct is a common feature in many studies in this review. It is seen in previous studies as motivating factors to certain security behaviours [7, 12, 17]. The behavioural control construct is seen as vital because it is noted to make the intentions to behave a particular way to actual behaviour [18]. The perceived behavioural control is the ease or the difficulty of which behaviour is acted upon, typically reflected on past experiences or the anticipated obstacles. The perceived behavioural construct is not found in the PMT, and therefore some studies have used TRA and TPB where actions can be sought from the intentions [18].

2.4 Intentions and Security Behaviour

An intention is not necessarily the act; this dilemma causes some confusion. Some researchers note that behavioural intention cannot dictate actions when the control over the action has not been completed [18]. Studies on information

security behaviour state that while actual behaviour and intentions are, in fact, related and can have the same effect, there is a difference between the intent and the behaviour in its practicality. Research models such as the PMT makes use of behavioural intentions to respond to threats to predict behaviour. However, it is said that intentions versus actual behaviour raise some research issues [19, 14].

Moreover, compliance to information security policy is a good security behaviour [14]. Commonly, the opposite of not being compliant is acting against the information security policies, and this behaviour is typically detrimental to the security posture of the said organisation. Previous studies on security behaviour focused specifically on what causes individuals to be non-compliant and intentions thereof [20, 21]. This suggests that studying compliance and attitudes towards security compliance is essential when considering that many organisations and institutions have policies. It can be argued that in many cases, compliance with security policy prevents harmful security behaviour.

3 Hypotheses Development

This study uses coping and threat appraisals from the PMT and the subjective norm adopted from the TPB to examine and discuss the environmental uncertainty and end-user security behaviour.

3.1 Protection Motivation Theory

The PMT predicts how individuals would respond under stress from threats [22]. It is argued that an individual's assessment of the severity and the vulnerability of this threat, also called a threat appraisal, and the extent to which they can cope with this threat by controlling particular human behaviour called the coping appraisal will determine their intention [13]. This study adopts all coping and threat appraisals in the PMT.

An individual's assessment of their view of the severity of the threat and their view of their susceptibility to this threat is called threat appraisals. In PMT, perceived severity would be a student's belief about the size of the threat or harm that this threat will inflict. The perceived vulnerability is the student's belief of their susceptibility to this threat [22]. Threat appraisals significantly impact readiness to perform a specific behaviour; this is noted in previous studies that have been conducted on security behaviour [8, 14]. As such, the following hypotheses are offered:

Hypothesis 1. Students' perceived vulnerability of losses by security threats positively impact their behavioural intention to practice information security.

Hypothesis 2. Students' perceived severity of losses by security threats positively impacts behavioural their intention to practice information security.

The coping appraisals in the PMT are response cost, response efficacy and self-efficacy; it is accepted that coping appraisals play an essential role in intentions to perform an action. In the context of this study, self-efficacy is the student's belief in their ability to lessen the threat that they are facing. Response cost is used to estimate the costs incurred in adopting a specific response to a threat; the response efficacy is the effectiveness of the student's response to this existing threat [11]. Students are expected to consider coping appraisals when deciding if certain technologies or measures are viable in confronting a particular security threat. The importance of coping appraisals is well noted in studies previously conducted, and their impact on behavioural intention is well observed [13]. As such, the following hypotheses are offered:

Hypothesis 3. Response efficacy positively impacts students' behavioural intention to practice information security.

Hypothesis 4. Self-efficacy positively impact students' behavioural intention to practice information security.

Hypothesis 5. Response costs negatively impact students' behavioural intention to practice information security.

3.2 Theory of Planned Behaviour

Central to TPB is the intentions to perform a specific behaviour motivated by specific factors [16]. In the TPB, the three core constructs are attitude towards the behaviour, subjective norm and perceived behavioural control, which also influences the actual behaviour. This study utilises the subjective norm and intention constructs from the TPB. Subjective norms in the context of this study are the student's acceptance of pressure from peers, fellow students and anyone close to the student to perform protective information security behaviours; it is said in previous studies that subjective norm has a significant influence on the intentions to perform a behaviour [12, 14, 23].

HEIs have security policies, rules and guidelines. This study's proposed research model uses the attitude toward compliance with an information systems security policy (ISSP) construct. It is also essential to examine if compliance with these rules and policies influence students' behaviour to practice information security. Compliance tends to be adequate security behaviour [5]; previous studies show that attitude towards ISSP compliance has a positive impact on behavioural intentions [18, 24, 25]; therefore, it is crucial to look at attitudes towards ISSP when examining an institution which has an ISSP. As such, the following hypotheses is proposed:

Hypothesis 6. Students' behavioural intention to practice information security positively impacts their information security behaviour.

Hypothesis 7. Subjective norms positively impact behavioural intention to practice information security.

Hypothesis 8. Attitude toward compliance with ISSP positively impact behavioural intention to practice information security.

3.3 Security Habit

This study's proposed research model also adopts the security habits construct with integrating constructs from the PMT and TPB. This construct has been used in previous studies and shows an impact on influencing information security behaviours [12, 26].In this study's context, security habit is the continuous action that influences information security behaviour [12, 25]. These actions tend to become routine, which makes this construct a critical moderator in examining end-user behaviour. Hence, we propose:

Hypothesis 9. Security habits positively impact students' information security behaviours.

3.4 Environmental Uncertainty

As defined by [27], uncertainty is an individual's perception of lacking sufficient information to predict accurately because of the inability to discriminate between relevant and irrelevant data and lack of knowledge of response options. An environmental uncertainty means that the source of uncertainty is external to the individual. These external events can be caused by political, economic, cultural, or global events such as the COVID-19 pandemic [3]. Environmental uncertainties affect how individuals decide in times of crisis due to the inability to understand changes, events, and causal relationships in the external environment [27].

The environmental uncertainty during the COVID-19 pandemic made it difficult for an individual to deduce relevant and irrelevant, accurate and fake COVID-19 information. An individual experienced an overload of information included in news, fake news, disinformation, misinformation, all related to the COVID-19 pandemic. Since individuals were desperate to learn about the new disease and understand the unfolding events, they were easily tricked into giving out personal information, clicking on malicious links, and fake websites with COVID-19 or corona domain names, including installing malware from attachments [3]. As the environmental uncertainty with the COVID-19 pandemic increased, individuals felt less level of behavioural intent to protect their information effectively. We thus hypothesise that:

Hypothesis 10. Environmental uncertainty negatively impacts behavioural intention to practice information security.

4 Research Design

The overall approach taken to perform an empirical test was a survey methodology for data collection. In the following subsections, we discuss the details of the instrument development and survey administration processes.

4.1 Instrument development

To improve the result's reliability and validity [28], we used previously validated and tested questions. Each item were adapted from literature, these are perceived vulnerability [12, 29], perceived severity [25], self-efficacy [25, 14], response cost [12], response efficacy [30, 25], information security behaviour [29, 25, 12], behavioural intentions [25], security habits [26], subjective norms [14], attitude toward ISSP compliance [24] and environmental uncertainty [31, 32]. The items used in this study are presented in Appendix Table A1. Each item involved a 7-point Likert scale indicating a respondent's level of agreement with the statements. A pilot test was carried out to ensure initial reliability and the questionnaire's general mechanics, notably survey instructions, completion time, and appropriate wording. The pilot was conducted with a group of graduate students at the South African HEI.

4.2 Survey Administrations & Participants

This survey was accessible online through a link distributed via e-mail to students at a research-focused South African HEI.The questionnaire setup and data collection were managed using the Qualtrics platform. This platform was used to design and create an online questionnaire and subsequently collected the results. Ethics approval was obtained before data collection proceeded. The survey was open for three weeks, from 11th September 2020 to 5th October 2020, during the COVID-19 pandemic. At the initial invitations of the study, South Africa was in the COVID-19 lockdown alert level 2. Some lockdown restrictions were lifted at level two, including visits to family and friends, and all inter-provincial travel was permitted while adhering to physical distancing. The transition to the lockdown alert level 1 on the 20th September 2020 occurred while the survey is still running; at this level, the lockdown rules were relaxed, and most normal activities were resumed, and international travel was allowed with precautions and health guidelines followed at all times. Nevertheless, HEIs in South Africa were still teaching under emergency remote teaching; some students received invitations to return to their residence, and the majority were studying from home. At the end of the survey period, a total of 229 responses had been recorded [33]. However, only 222 responses were complete and considered valid for subsequent data analysis.

5 Data Analysis and Results

The data was analysed using Partial Least Squares Structural Equation Modelling (PLS-SEM). The analysis was performed using the SmartPLS software

application. The analysis first evaluated the validity and reliability of the measurement items before testing the study's hypotheses.

5.1 Respondent Demographics

The demographics for age were split into six groups: 18-24, 25-34, 35-44, 45-54, 55-64, 65+. Most respondents, 77%, were between the ages of 18-24, 16% of respondents between 25-34, 5% between 45-54, and 1% between 55-64. The gender was split into Male, Female, and Prefer not to answer; most respondents were female at 70%, with 29% being male, and 1% preferred not to answer.

5.2 Internal Consistency Reliability & Convergent Validity

There is internal consistency reliability as all indicators fall within 0.6 and 0.9 values as recommended [30], the attitude toward ISSP compliance and self-efficacy constructs are slightly above 0.9. However, this is not undesirable when values are not significantly above the 0.95 thresholds, which these two constructs are not [34]. All constructs have an AVE value of above 0.50, indicating the convergent validity of all constructs in this study. The internal consistency reliability and convergent validity for this study are shown in Table 1.

Table 1. Construct reliability and convergent validity.

	Composite Reliability	**Average Variance Extracted (AVE)**
Behavioural Intention	0.694	0.562
Information Security Behaviour	0.776	0.634
Attitude toward compliance with ISSP	0.953	0.87
Perceived severity	0.894	0.808
Perceived vulnerability	0.609	0.509
Response cost	0.841	0.725
Response efficacy	0.826	0.614
Self-efficacy	0.948	0.901
Security habits	0.619	0.514
Subjective norm	0.747	0.612
Environmental Uncertainty	0.687	0.567

5.3 Discriminant Validity

In Heterotrait Monotrait Ratio (HTMT), for discriminant validity to exist, items should have a value of less than .90. Some constructs did not meet this criterion. One way to improve discriminant validity is by eliminating items with low correlations with items measuring the same construct[35]. However, because the problematic constructs only had two measurement items, it was decided to retain them without modification.

5.4 Coefficient of Determination

The coefficient of determination, generally denoted as R-squared (R^2), is used to evaluate a research model's fitness. It is accepted that an R^2 value of 0.75 indicates a substantial fit. In contrast, any R^2 of below 0.25 indicates a weaker fit [36], Information security behaviour has an R^2 of 0.174 (17.4%), which makes it a weak fit for the model, the behavioural intentions variable has a moderate fit with an R^2 value of 0.424 (42.4%).

5.5 Hypotheses Test Results

Bootstrapping was used to get the t-values to test the hypotheses for the study. As recommended, a sub-sample of 5,000 was taken from the original sample [36]. The significance of using the bootstrap method in analysing data is that it gives the closest estimate using a simulated sample [36]. Testing of the hypotheses was conducted using a two-tailed test with a significance level of 5%. Of the ten hypotheses, four are not supported; the hypotheses that are not supported are H2—perceived severity, H4—self-efficacy, H8—attitude toward ISSP compliance, and H10—environmental uncertainty. While H1—perceived vulnerability, H5 — response cost, H3—response efficacy, H7—subjective norm and H9—security habits were are all supported. The results of the hypotheses test results are shown in Table 2.

Table 2. Construct reliability and convergent validity.

Hypothesis	**Path**	**Path coefficient**	**t-values**
H1	Perceived vulnerability →Intention	-0.195	3.162**
H2	Perceived severity → Intention	0.099	1.901
H3	Response efficacy → Intention	0.296	4.280**
H4	Self-efficacy → Intention	0.007	0.103
H5	Response cost →Intention	-0.236	4.172**
H6	Intention→ Information security behaviour	0.260	3.521**
H7	Subjective norm → Intention	0.231	3.121**
H8	Attitude toward ISSP compliance → Intention	0.029	0.423
H9	Security habits → Information security behaviour	0.284	3.963**
H10	Environmental uncertainty → Intention	0.005	0.068
Behavioural intention R^2: 0.424		* Significant at the 0.05 level	
Information security behaviour R^2: 0.174		** Significant at the 0.01 level	

6 Discussion

This study presents several key findings, each of which contributes to both theory and practice. On the theory level, we evaluate the security behaviours of students at HEI as related to information security behaviour during the COVID-19

pandemic in an integrated model that uses TPB, PMT and a new additional construct environmental uncertainty. Our results indicate that perceived vulnerability impacts behavioural intention to practice information security; these results are consistent with previous studies [37, 15]. We, however, found that perceived severity did not have a significant impact on behavioural intentions to perform information security. This hypothesis is supported in a previous study [9], but another study in a similar context did not appear to support this hypothesis [12]. Our result suggests that students' behavioural intention was influenced by their perception of susceptibility to threats; however, the severity of threats did not influence intention to practice information security protective behaviours. Our findings indicate that the response efficacy impacts behavioural intentions to practice information security. This is consistent with previous studies [9, 12]. Our result suggests that students have faith in the effectiveness of their response to threats with whatever recommended measures at their disposal.

Response cost was found to significantly impact behavioural intention to practice information security; this is consistent with previous studies [12]. This suggests that students feel that maintaining information security is an expensive exercise. In contrast, self-efficacy did not have an impact on behavioural intentions to practice information security. Self-efficacy has been found to have mixed results in the IS security literature [9, 12]. Our result suggests that students do not have faith in their abilities to mitigate threats, and this might be due to prior experiences with virus infections and security breach.

Subjective norms were also found to significantly impact intentions to perform information security; this is consistent with previous research [37]. In testing the attitude toward compliance with ISSP, it was found that attitude toward compliance with ISSP had no impact on behavioural intention to practice information security—this contradicted previous studies [28]. Our result suggests that since the study was done while students are studying remotely during the COVID-19 pandemic, students did not feel that following security policy was necessary. Consistent with previous research [12], behavioural intention to practice information security significantly impacts information security behaviour. The study findings also suggest that security habits positively impact students' information security behaviours. These results are consistent with previous research [12]. Our result shows that students' routine habits have a significant impact on their information security behaviour.

Furthermore, the study findings suggest that environmental uncertainty did not impact behavioural intention to practice information security. While not consistent with previous research [38], this shows that the study population did not feel that uncertainty was a factor in their behavioural intentions to perform information security. Our result suggests that respondents were able to cope with environmental uncertainty with resilience and success and maintain security behaviour.

On the practical level, the factors of the PMT, such as perceived vulnerability, response cost and self-efficacy, are essential in responding to security threats. So, when designing a security plan for an HEI, it would be beneficial to focus

on security training, such as technical security tools. We also found that subjective norm plays an essential role in students' intentions to perform information security. Thus, security awareness may be necessary for any future security plan for HEI students as students may significantly influence other students' security behaviour. This study also found that students' security habits play a role in information security behaviour; therefore, it would be beneficial for training to be made a routine for security habits to be positively solidified.

The limitations of this study create several opportunities for further research. The environmental uncertainty did not have statistically significant weight. The insignificant effect of environmental uncertainty on behavioural intention may be due to reasons such as; respondents may not have understood questions associated with this factor in the context of information security because of its novelty. Another explanation might be that the study population did not understand that the uncertainty about the COVID-19 pandemic, which brought the desire to search for and receive information about COVID-19/Coronavirus, also brought security issues. Reports have shown that in 2020 there was a massive increase in security breaches [3]; as people were searching for and eager to receive information about the COVID-19 pandemic, they became vulnerable to cyber-attacks. Hence future research would benefit from exploring the impact that uncertainty has had on the actual security behaviour of HEIs students during the COVID-19 pandemic and attitudes towards COVID-19 related cyber-attacks.

7 Conclusion

In this paper, we aimed to understand the factors that motivate end-user security behaviour at HEIs, considering the environmental uncertainty caused by the COVID-19 pandemic. This study determined that the PMT and TPB are indeed suitable for determining factors that motivate security behaviour. We also evaluated the effect of environmental uncertainty on security behaviour intentions. With the help of 222 responses from HEIs students, we performed an empirical test on the proposed model. Our results suggest that response efficacy, response cost, and subjective norm are likely to positively affect behaviour intention, which inturns are a significant predictor of HEIs students' information security behaviours. Also, security habits showed a significant effect on HEIs students' information security behaviours. While perceived severity, self-efficacy, and attitude toward ISSP compliance did not significantly affect behaviour intentions to practice information security.Future research would also benefit from a more comprehensive definition of attitude toward ISSP compliance. It is possible that compliance in the HEI context of this study was too simplistic, which may have influenced the results.

This study incorporated environmental uncertainty due to the ongoing COVID-19 pandemic—which is new in the context of information security. This study did not find any impact of environmental uncertainty on behavioural intentions. Future research would benefit from exploring the impact that uncertainty has

had on the actual security behaviour of HEIs students during the COVID-19 pandemic and attitudes towards COVID-19 related cyber-attacks. This study did not measure how student attitudes evolved as the pandemic developed; further research is needed to investigate this issue— investigation can be carried out with in-depth interviews and focus group discussion.

References

1. Domínguez, C.M.F., Ramaswamy, M., Martinez, E.M., Cleal, M.G.: A framework for information security awareness programs. Issues in Information Systems **11**(1), 402–409 (2010)
2. Beautement, A., Sasse, M.A., Wonham, M.: The compliance budget: managing security behaviour in organisations. In: Proceedings of the 2008 New Security Paradigms Workshop. pp. 47–58 (2008)
3. Naidoo, R.: A multi-level influence model of covid-19 themed cybercrime. European Journal of Information Systems **29**(3), 306–321 (2020)
4. Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., Calic, D.: Assessing information security attitudes: a comparison of two studies. Information & Computer Security (2016)
5. Rupere, T., Muhonde, M.: Towards minizing human factors in end-user information security (2012)
6. Nasir, A., Arshah, R.A., Ab Hamid, M.R.: The significance of main constructs of theory of planned behavior in recent information security policy compliance behavior study: A comparison among top three behavioral theories. International Journal of Engineering & Technology **7**(2.29), 737–741 (2018)
7. Dang-Pham, D., Pittayachawan, S., Bruno, V.: Why employees share information security advice? exploring the contributing factors and structural patterns of security advice sharing in the workplace. Computers in Human Behavior **67**, 196–206 (2017)
8. Tsai, H.y.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J., Cotten, S.R.: Understanding online safety behaviors: A protection motivation theory perspective. Computers & Security **59**, 138–150 (2016)
9. Holmes, M., Ophoff, J.: Online security behaviour: factors influencing intention to adopt two-factor authentication. In: ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS. p. 123 (2019)
10. Moletsane, T., Tsibolane, P.: Mobile information security awareness among students in higher education: An exploratory study. In: 2020 conference on information communications technology and society (ICTAS). pp. 1–6. IEEE (2020)
11. Maddux, J.E., Rogers, R.W.: Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of experimental social psychology **19**(5), 469–479 (1983)
12. Yoon, C., Hwang, J.W., Kim, R.: Exploring factors that influence students' behaviors in information security. Journal of information systems education **23**(4), 407–416 (2012)
13. Tu, Z., Yuan, Y., Archer, N.: Understanding user behaviour in coping with security threats of mobile device loss and theft. International Journal of Mobile Communications **12**(6), 603–623 (2014)
14. Yoon, C., Kim, H.: Understanding computer security behavioral intention in the workplace. Information Technology & People (2013)

15. Srisawang, S., Thongmak, M., Ngarmyarn, A.: Factors affecting computer crime protection behavior. In: PACIS. p. 31 (2015)
16. Ajzen, I.: The theory of planned behavior. Organizational behavior and human decision processes **50**(2), 179–211 (1991)
17. Chen, Y., Zahedi, F.M.: Individuals'internet security perceptions and behaviors: Polycontextual contrasts between the united states and china. MIS Quarterly **40**(1) (2016)
18. Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A., Herawan, T.: Information security conscious care behaviour formation in organizations. Computers & Security **53**, 65–78 (2015)
19. Johnston, A.C., Warkentin, M.: Fear appeals and information security behaviors: An empirical study. MIS quarterly pp. 549–566 (2010)
20. Cheng, L., Li, Y., Li, W., Holm, E., Zhai, Q.: Understanding the violation of is security policy in organizations: An integrated model based on social control and deterrence theory. Computers & Security **39**, 447–459 (2013)
21. Williams, A.S., Maharaj, M.S., Ojo, A.I.: Employee behavioural factors and information security standard compliance in nigeria banks. International Journal of Computing and Digital Systems **8**(04), 387–396 (2019)
22. Rogers, R.W.: A protection motivation theory of fear appeals and attitude change1. The journal of psychology **91**(1), 93–114 (1975)
23. Foltz, C.B., Newkirk, H.E., Schwager, P.H.: An empirical investigation of factors that influence individual behavior toward changing social networking security settings. Journal of theoretical and applied electronic commerce research **11**(2), 1–15 (2016)
24. Ifinedo, P.: Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management **51**(1), 69–79 (2014)
25. Workman, M., Bommer, W.H., Straub, D.: Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in human behavior **24**(6), 2799–2816 (2008)
26. Limayem, M., Khalifa, M., Chin, W.W.: Factors motivating software piracy: a longitudinal study. IEEE transactions on engineering management **51**(4), 414–425 (2004)
27. Milliken, F.J.: Three types of perceived uncertainty about the environment: State, effect, and response uncertainty. Academy of Management review **12**(1), 133–143 (1987)
28. Straub, D.W.: Validating instruments in mis research. MIS quarterly pp. 147–169 (1989)
29. Woon, I., Tan, G.W., Low, R.: A protection motivation theory approach to home wireless security (2005)
30. Ng, B.Y., Xu, Y.: Studying users' computer security behavior using the health belief model. PACIS 2007 Proceedings p. 45 (2007)
31. Chen, X., Zhang, X.: How environmental uncertainty moderates the effect of relative advantage and perceived credibility on the adoption of mobile health services by chinese organizations in the big data era. International journal of telemedicine and applications **2016** (2016)
32. Pavlou, P.A., Liang, H., Xue, Y.: Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. MIS quarterly pp. 105–136 (2007)

33. Kautondokwa, P.: Factors that motivate end-user security behaviour in higher education: A study of UCT during covid-19. [Unpublished Honours project], Department of Information Systems, University of Cape Town, South Africa (2020)
34. Hair Jr, J.F., Hult, G.T.M., Ringle, C., Sarstedt, M.: A primer on partial least squares structural equation modeling (PLS-SEM). Sage publications (2016)
35. Henseler, J., Ringle, C.M., Sarstedt, M.: A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the academy of marketing science **43**(1), 115–135 (2015)
36. Hair, J.F., Risher, J.J., Sarstedt, M., Ringle, C.M.: When to use and how to report the results of pls-sem. European business review (2019)
37. Martens, M., De Wolf, R., De Marez, L.: 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 (2019)
38. Sharma, P., Leung, T.Y., Kingshott, R.P., Davcik, N.S., Cardinali, S.: Managing uncertainty during a global pandemic: An international business perspective. Journal of business research **116**, 188–192 (2020)

A Appendix

Table A1. Instrument Documentation

Construct	Items	Source
Information security behaviour	I regularly check and erase viruses and malicious software	[25].
	I instantly delete dubious e-mails without reading them	[29].
Perceived Vulnerability	There is a chance that my personal information has been leaked due to hacking.	[29]
	There is a chance that my anti-virus has not been updated in a long time.	[33]
Perceived severity	Losing data privacy as a result of hacking would be a serious problem for me	[25].
	Becoming a victim of a cyberattack would result in my losing a lot of valuable, important data	[25]
Response efficacy	Using security technologies is effective for protecting confidential information.	[25]
	Taking preventive measures is effective for protecting my personal information.	[30]
	Enabling security measures on my computer is an effective way of preventing computer data from being damaged by malicious software such as viruses.	[30]
Self-efficacy	I am able to protect my personal information from external threats.	[25]
	I am able to protect data on my computer from being damaged by external threats.	[14]
Behavioural intention	I will aggressively use security technologies to protect confidential information.	[25]
	I will never share important personal information.	[33]
Subjective norm	If I enthusiastically make use of security technologies, most of the people who are important to me would endorse	[14]
	Most important people in my life think it is a good idea to take precautionary measures to protect personal information.	[14]
Response cost	Obtaining the latest security technology to safeguard confidential information is irritating.	[12]
	Maintaining security measures (such as changing the password regularly) to protect personal information is a burden.	[12]
Security habit	I should regularly delete viruses and malicious software	[26]
	I routinely send dodgy e-mails to the recycle bin	[26]
Attitude toward compliance with ISSP	Following the institution's ISSP is a good idea	[24]
	Following the institution's ISSP is a necessity	[24]
	Following the institution's ISSP is beneficial	[24]
Environmental uncertainty	I feel that e-mails that are COVID-19 related are without a doubt safe to follow	[32]
	I feel conflicted about the need to reflect on e-mails requesting my personal information if these e-mails are COVID-19 related	[32]

Note: Items were measured on a 7-point scale from "strongly disagree" to "strongly agree."