

Predicting Schoolteachers' Intention and Behaviour of Promoting Cyber-Safety Awareness

Kagisho Mabitle and Elmarie Kritzinger

Abstract—School learners are attractive candidates for cyber-safety attacks. Advances in Information and Communications Technology (ICT) devices, and the surge in Internet usage, poses significant risks to users with poor cyber-safety awareness and security practices. An example of such users are school learners. Therefore, school learners should be made aware of cyber-safety or safe Internet usage, through awareness programmes as early as possible. Applying the classical Theory of Planned Behaviour in a survey of 109 schoolteachers across 18 schools in 2 districts, the results of a multiple regression analysis unveil that: 1) attitude does not predict the schoolteachers' intention to raise cyber-safety awareness at their schools in the next 12 months, nor does it predict the schoolteachers' behaviour of raising cyber-safety awareness in their teaching; and 2) subjective norms and perceived behavioural control predict the schoolteachers' intention and behaviour. In light of this, the South African Department of Basic Education (DBE) is encouraged to identify influential schoolteachers (i.e. phase heads, sports and cultural coordinators, principals and their deputies, etc.), and to groom them into cyber-safety awareness advocates, for the purposes of influencing other teachers or their peers. Also, the DBE should provide teachers with the requisite resources, opportunities, and support which facilitates cyber-safety awareness in schools, to empower teachers to adopt this highly desired behaviour.

Index Terms—Cyber-safety, awareness, schools, learners, teachers, theory of planned behaviour.

I. INTRODUCTION

The growth and range of Internet usage by children and youth is steadily rising [1]. Since mobile Internet connection is the most popular form of Internet connection in South Africa [2], with 34 million mobile Internet users out of a total of 36 million Internet users [3], a majority of South African school learners are correspondingly now able to access the Internet through their handy mobile phones [4]. With such effortless access to a global network of communication, school learners are susceptible to cyber-risks such as anxiety [5], cyber-bullying [6], human trafficking [7], identity theft [8], and phishing [9], to mention but a few. Therefore, school learners need to be made aware of cyber-safety or safe Internet usage, through awareness programmes as early as possible [10]. Such programmes should teach learners how to use Information and Communications Technology (ICT) and associated ICT devices safely and responsibly.

Manuscript received May 22, 2020; revised December 24, 2020. This work was financially supported by the Directorate of Student Funding of the University of South Africa, and the South African Department of Higher Education and Training.

The authors are with the Department of Information Systems, School of Computing, College of Science, Engineering and Technology, University of South Africa, South Africa (e-mail: mabitk@unisa.ac.za).

Cyber-safety awareness could ensure that learners have the necessary attitude towards cyber-safety, as well as the knowledge and skills to deal with real-life cyber-safety threats and risks [4]. Without cyber-safety awareness, learners will remain prone to a myriad of cyber-risks. Cyber-safety awareness and educational programmes can be seen as a defence mechanism for protecting information and other assets [11]. Given the importance of raising cyber-safety awareness, schools in general, and teachers in particular are required to participate in teaching school learners about cyber-safety [12].

Schoolteachers are cited as key role players in the cyber-safety education of learners. Their role, *inter alia*, is identified as the deliverers of cyber-safety awareness messages to school learners [13]. As such, this study applies the Theory of Planned Behaviour (TPB) with the objective of revealing which construct/s predict the South African schoolteachers' intention and behaviour of raising cyber-safety awareness. This insight is particularly needed and important, as it unveils the predictive power of the respective TPB constructs in our context. With this insight, school cyber-safety awareness campaigns can be enhanced as a result of improved understanding and planning.

II. THE THEORY OF PLANNED BEHAVIOUR

Although the Theory of Reasoned Action (TRA) is not the theoretical framework for the current study, it provides valuable insights into the TPB's journey as a leading social scientific theory used to study intention and behaviour [14]. Introduced by Fishbein in 1967, the TRA explains the development of the TPB, which is the theoretical framework for this study. The TRA states that the two main determinants of intention are an individual's attitude toward the behaviour, and the perceived pressures of subjective norms. Together, these forces determine intention [14], which subsequently determines behaviour. Generally, individuals will intend to perform a behaviour when they evaluate it positively, and when they believe important 'others' think or expect them to perform the behaviour [15]. However, social scientists concede that the relative weights of attitude and subjective norms may vary, based on intention, and across individuals [15]. The TRA has been effective in a variety of settings [16]. Yet, there are concerns about its generality. For instance, the model omits explaining research findings that the best predictor of future behaviour is past behaviour [17]. Also, the model does not account for volitional control (i.e. perceived behavioural control). It is this particular deficiency which led to the extension of the TRA, called the TPB.

The TPB duly uses attitude, subjective norms, and

perceived behavioural control to predict intention and behaviour relatively accurately [18]. The theory assumes that a person's intention, plus perceived behavioural control, will help predict behaviour with greater accuracy. Both the TRA and TPB assume that behaviour is a conscious decision to act in a particular manner. Yet, there is a critical difference between these two theories. Unlike the TRA, the TPB, depicted in Fig. 1, considers volitional control as a variable. By definition, volitional control means that a person must have the requisite resources, opportunities, and support available to perform a specific behaviour. As depicted in Fig. 1, the TPB comprises three conceptually independent antecedents, namely; attitude, subjective norms, and perceived behavioural control [18].

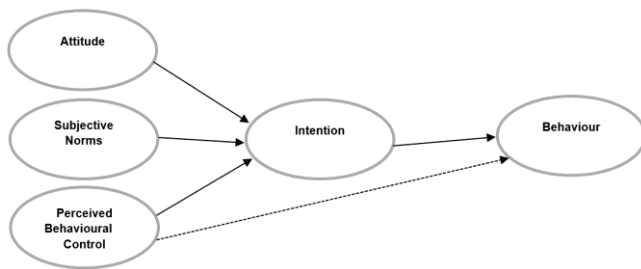


Fig. 1. Theory of Planned Behaviour (TPB).

A. Attitude

Attitude is the degree to which the performance of a particular behaviour is positively or negatively evaluated by an individual [14], [18]. This evaluation is said to encompass two main components; one that is instrumental in nature (i.e. valuable vs. worthless), and one that is related to experiential quality (i.e. pleasant vs. unpleasant) [14]. For instance, schoolteachers may commit to raising cyber-safety awareness at their schools because they might perceive it as valuable, since they are aware of its importance.

B. Subjective Norms

Peers and other key people in an individual's life have their own perceptions of whether or not an individual should perform a particular behaviour. These perceptions are the individual's subjective norms. Subjective norms refer to the perceived social or peer pressure to engage or not to engage in a behaviour. It is assumed that subjective norms are determined by normative beliefs concerning the expectations of important referents. These referents are certain groups of people that would approve or disapprove of the individual performing a particular behaviour [18]. For instance, schoolteachers whose parents, spouses, children, or peers approve of them raising cyber-safety awareness at their schools, will be more likely to adopt this behaviour.

C. Perceived Behavioural Control

Perceived behavioural control refers to an individual's perceptions of whether or not they can perform a particular behaviour. This includes an assessment of the feasibility of performing a particular behaviour, considering the requisite resources, opportunities and support. The construct encompasses the perceived ease or difficulty a person associates with a specific task or behaviour [18]. For instance, schoolteachers who have received adequate cyber-safety

awareness training, or those who have the corresponding instructional media or delivery methods, might perceive the task as easy, and will be more likely to raise cyber-safety awareness at their schools.

D. Intention and Behaviour

Intention is an indication of a person's readiness to perform a particular behaviour or action. Intention is considered to be the immediate antecedent of behaviour [14], [18]. This intention is based on the predictors attitude, subjective norms, and perceived behavioural control as depicted in Fig. 1. As applied in this study, intention refers to the schoolteachers' intention of raising cyber-safety awareness at their schools in the next 12 months. Behaviour is a conscious decision to act in a particular manner [14], and in this study, it refers to the schoolteachers' behaviour of raising cyber-safety awareness in their teaching. Intention predicts behaviour [18].

E. Utility of the Theory of Planned Behaviour

The TPB is a well-established and useful model, which has been applied in numerous social scientific studies. Having received substantial research support [19], the main strength of the TPB lies in its application to a variety of behaviours in different contexts, including diverse areas such as health communications, environmental concerns, risk communication, mass transit use, and technology adoption [14]. For instance, [20] used the model to examine the relationship between privacy and online purchasing. Reference [21] used the model to explore the factors which predict students' decisions to select an online course, as opposed to a face-to-face (i.e. contact) course. Reference [22] used the theory to study teachers' decisions to create and deliver lessons using computing technology. Reference [23] used the theory to examine students' intentions to use podcasts as a learning tool.

Another strength of the TPB is its accessibility. This is an important characteristic, because the simplicity of a theory is a quality associated with its strength and utility [24]. The use of the TPB has increased significantly in the last decade, with over a thousand published studies utilising this theory [14]; the current study being only one of these.

III. RESEARCH METHODOLOGY

A survey questionnaire was distributed to teachers in the Sedibeng West and East school districts of the Gauteng Province of South Africa, to explore their cyber-safety awareness intention and behaviour. The study adapted and used a questionnaire which had been piloted and used by [14] in an American doctoral study, confirming the questionnaire's validity. Across 18 schools, 12 primary and 6 secondary schools in the 2 districts, a total of 180 questionnaires were distributed. Twenty (20) questionnaires were disseminated via email, and 160 were disseminated in hardcopies. Qualtrics was used as the data capture software. The dissemination resulted in a net of 109 completed, usable responses. This translated to a 61% positive survey response rate, with 0 responses from the email dissemination.

SPSS was used as the statistical software for the quantitative data analysis. Seventy-two percent (72%) of the

responses were from public, government schools; whilst 28% were from private, independent schools. Multiple regression analysis was used to assess the predictive power of the TPB constructs (i.e. attitude, subjective norms, and perceived behavioural control), in relation to the schoolteachers' intention and behaviour of raising cyber-safety awareness. Cronbach's coefficient α was used to measure the internal reliability of the items measuring the respective TPB constructs.

The following 7 items (α of 0.898) assessed the *attitude* of schoolteachers:

1) For me, raising cyber-safety awareness at my school in the next 12 months would be (circle a number for each statement):

- Good: ___3___ : ___2___ : ___1___ : ___0___ : ___-1___ : ___-2___ : ___-3___ : Bad
- Foolish: ___-3___ : ___-2___ : ___-1___ : ___0___ : ___1___ : ___2___ : ___3___ : Wise
- Pleasant: ___3___ : ___2___ : ___1___ : ___0___ : ___-1___ : ___-2___ : ___-3___ : Unpleasant
- Unenjoyable: ___-3___ : ___-2___ : ___-1___ : ___0___ : ___1___ : ___2___ : ___3___ : Enjoyable
- Useful: ___3___ : ___2___ : ___1___ : ___0___ : ___-1___ : ___-2___ : ___-3___ : Useless
- Unimportant: ___-3___ : ___-2___ : ___-1___ : ___0___ : ___1___ : ___2___ : ___3___ : Important
- Desirable: ___3___ : ___2___ : ___1___ : ___0___ : ___-1___ : ___-2___ : ___-3___ : Undesirable

The following 5 items (α of 0.634) assessed the *subjective norms* of schoolteachers, using the scale below:

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
-------------------	----------	-------------------	----------------------------	----------------	-------	----------------

- 1) Most people who are important to me would think that I should raise cyber-safety awareness at my school in the next 12 months.
- 2) It is expected of me that I would raise cyber-safety awareness at my school in the next 12 months.
- 3) The people in my life whose opinions I value would approve of me raising cyber-safety awareness at my school.
- 4) Most teachers at my school currently raise cyber-safety awareness.
- 5) Most teachers at my school would be comfortable raising cyber-safety awareness.

The following 4 items (α of 0.657) assessed the *perceived behavioural control* of schoolteachers, using the same scale:

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
-------------------	----------	-------------------	----------------------------	----------------	-------	----------------

- 1) For me to raise cyber-safety awareness at my school would be possible.
- 2) If I wanted to, I could raise cyber-safety awareness at my school.
- 3) I have complete control over raising cyber-safety awareness at my school.
- 4) It is mostly up to me whether or not I raise cyber-safety awareness at my school.

The following 4 items (α of 0.878) assessed the *intention* of schoolteachers, using the same scale:

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
-------------------	----------	-------------------	----------------------------	----------------	-------	----------------

- 1) I would use additional resources such as frameworks, to help me raise cyber-safety awareness at my school.
- 2) I intend on raising cyber-safety awareness at my school in the next 12 months.
- 3) I have decided to raise cyber-safety awareness at my school in the next 12 months.
- 4) I am determined to raise cyber-safety awareness at my school in the next 12 months.

The following item assessed the *behaviour* of schoolteachers, using the scale below:

Never	Rarely	Sometimes	Most of the time	Always
-------	--------	-----------	------------------	--------

- 1) How often in the last 12 months did you raise awareness about cyber-safety in your teaching?

IV. RESULTS AND DISCUSSIONS

In the initial part of the data analysis, a standard multiple regression analysis is used to test the relationship between the TPB constructs (i.e. attitude, subjective norms, and perceived behavioural control), and the teachers' intention to raise cyber-safety awareness at their schools in the next 12 months. In essence, attitude is not revealed as a predictor of intention, whilst subjective norms and perceived behavioural control are. The results of this analysis are depicted in Table I.

TABLE I: MULTIPLE REGRESSION (TPB CONSTRUCTS AND INTENTION)

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.778 ^a	.606	.594	.71347

a. Predictors: (Constant), Perceived_Beh_Contr, alpha = .68, Attitude measure, alpha = .90, Subjective Norms measure, alpha = .63

ANOVA ^a						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	82.126	3	27.375	53.779	.000 ^a
	Residual	53.448	105	.509		
	Total	135.575	108			

a. Dependent Variable: Intention, alpha = .88

b. Predictors: (Constant), Perceived_Beh_Contr, alpha = .68, Attitude measure, alpha = .90, Subjective Norms measure, alpha = .63

Coefficients ^a					
Model		Unstandardized Coefficients		Standardized Coefficients	t
		B	Std. Error	Beta	
1	(Constant)	-.937	.525		-1.786
	Attitude measure, alpha = .90	.086	.067	.085	1.279
	Subjective Norms measure, alpha = .63	.565	.092	.448	6.158
	Perceived_Beh_Contr, alpha = .68	.515	.077	.453	6.691

Coefficients ^a			
Model			Sig.
1	(Constant)		.077
	Attitude measure, alpha = .90		.204
	Subjective Norms measure, alpha = .63		.000
	Perceived_Beh_Contr, alpha = .68		.000

a. Dependent Variable: Intention, alpha = .88

A. Attitude and Intention

The multiple regression analysis between attitude and intention reveals that attitude does not predict intention [$\beta = 0.09$, $n = 109$, $p > 0.05$], nor is the relationship statistically significant [$p = 0.204$]. These results imply that the schoolteachers' attitude [$M = 5.6820$] towards raising cyber-safety awareness, is not a predictor of their intentions

to raise cyber-safety awareness at their schools in the next 12 months. This means that the positive, neutral, or negative evaluation by teachers of raising cyber-safety awareness does not predict their intention of doing so in the next 12 months. The results could be attributable to the weaker correlation [$r = 0.26, n = 109, p < 0.05$] between attitude and intention. Contrary to this study and consistent with [25], [26] found that attitude significantly predicted the intention to accept modern agricultural biotechnology [$\beta = 0.84, n = 220, p = 0.000$].

B. Subjective Norms and Intention

The multiple regression analysis between subjective norms and intention divulges that subjective norms do predict intention [$\beta = 0.45, n = 109, p < 0.05$]. This relationship is statistically significant [$p = 0.000$]. These results imply that subjective norms (i.e. influences by peers and significant others) [$M = 5.1982$] in relation to raising cyber-safety awareness, predict the schoolteachers' intentions to raise cyber-safety awareness at their schools in the next 12 months. This means that the perceptions of the teachers' colleagues, parents, spouses, and children, etc., predict their intention of raising cyber-safety awareness in the next 12 months. These results can be attributable to the strong correlation [$r = 0.66, n = 109, p < 0.05$] between subjective norms and intention. Consistently, [26] found that subjective norms significantly predicted the acceptance of modern agricultural biotechnology [$\beta = 0.40, n = 220, p = 0.000$]. These findings of subjective norms being a predictor of intention are consistent with [14] and [27].

C. Perceived Behavioural Control and Intention

The multiple regression analysis between perceived behavioural control and intention shows that perceived behavioural control also predicts intention [$\beta = 0.45, n = 109, p < 0.05$] like subjective norms. This relationship is also statistically significant [$p = 0.000$]. These results imply that perceived behavioural control (i.e. additional resources and opportunities) [$M = 5.1982$] in relation to raising cyber-safety awareness, predicts the schoolteachers' intentions to raise cyber-safety awareness at their schools in the next 12 months. The results can similarly be attributable to the strong correlation [$r = 0.64, n = 109, p < 0.05$] between perceived behavioural control and intention. Consistently, [26] found that perceived behavioural control significantly predicted the intention to accept modern agricultural biotechnology [$\beta = 0.53, n = 220, p = 0.000$]. These findings of perceived behavioural control being a predictor of intention are consistent with [28] and [25], but contrary to [29].

D. Intention and Behaviour

Reviews of the relationship between intention and behaviour have been conducted by [15], [30], [31], and [32]. In the final part of the data analysis, a standard multiple regression analysis is similarly used to test the relationship between intention and behaviour. The results of this analysis are depicted in Table II. The relationship between the TPB constructs (i.e. attitude, subjective norms, and perceived behavioural control), and the teachers' behaviour of raising cyber-safety awareness in their teaching, is also tested here. The results of this analysis are depicted in Table III. In

essence, intention is found to be a predictor of behaviour, as hypothesized by [18]. Furthermore, attitude is not found to be a predictor of behaviour, whilst subjective norms and perceived behavioural control are found to be predictors.

TABLE II: MULTIPLE REGRESSION (INTENTION AND BEHAVIOUR)

Model Summary					
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	
1	.480 ^a	.230	.223	.985	

a. Predictors: (Constant), Intention, alpha = .88

ANOVA ^a						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	31.010	1	31.010	31.967	.000 ^b
	Residual	103.797	107	.970		
	Total	134.807	108			

a. Dependent Variable: How often in the last 12 months did you raise awareness about cyber-safety in your teaching?

b. Predictors: (Constant), Intention, alpha = .88

Coefficients ^a						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.295	.443		.665	.507
	Intention, alpha = .88	.478	.085	.480	5.654	.000

a. Dependent Variable: How often in the last 12 months did you raise awareness about cyber-safety in your teaching?

TABLE III: MULTIPLE REGRESSION (TPB CONSTRUCTS AND BEHAVIOUR)

Model Summary					
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	
1	.492 ^a	.242	.221	.986	

a. Predictors: (Constant), Perceived_Beh_Contr, alpha = .68, Attitude measure, alpha = .90, Subjective Norms measure, alpha = .63

ANOVA ^a						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	32.663	3	10.888	11.192	.000 ^b
	Residual	102.145	105	.973		
	Total	134.807	108			

a. Dependent Variable: How often in the last 12 months did you raise awareness about cyber-safety in your teaching?

b. Predictors: (Constant), Perceived_Beh_Contr, alpha = .68, Attitude measure, alpha = .90, Subjective Norms measure, alpha = .63

Coefficients ^a						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-1.300	.726		-1.792	
	Attitude measure, alpha = .90	.141	.093	.140	1.514	
	Subjective Norms measure, alpha = .63	.317	.127	.252	2.499	
	Perceived_Beh_Contr, alpha = .68	.312	.106	.275	2.936	

Coefficients ^a						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)					.076
	Attitude measure, alpha = .90					.133
	Subjective Norms measure, alpha = .63					.014
	Perceived_Beh_Contr, alpha = .68					.004

The R^2 value for intention and behaviour is 0.230, which means that intention accounts for 23% of the variation in the schoolteachers' behaviour of raising cyber-safety awareness in their teaching. The multiple regression analysis between intention and behaviour further reveals that intention predicts behaviour [$\beta = 0.48, n = 109, p < 0.05$]. This positive relationship is statistically significant [$p = 0.000$]. These results, depicted in Table II, imply that the schoolteachers' intention [$\alpha = 0.88$] of raising cyber-safety awareness, is a predictor of their behaviour of raising cyber-safety awareness at their schools and in their teaching. Using multiple regression and AMOS path analysis, [26] confirmed that the intention to accept modern agricultural biotechnology significantly predicted the behaviour of accepting this technology. This finding is consistent with the current study,

and supports previous studies that have found intention to be a strong predictor of behaviour [33]-[36]. The relationship between the three main constructs of the TPB (i.e. attitude, subjective norms, and perceived behavioural control) and behaviour is depicted in Table III.

E. Attitude and Behaviour

The R^2 value of 0.242 implies that attitude, subjective norms and perceived behavioural control together account for 24.2% of the variation in the schoolteachers' behaviour of raising cyber-safety awareness in their teaching. The multiple regression analysis between attitude and behaviour divulges that attitude does not predict behaviour [$\beta = 0.14, n = 109, p > 0.05$]. This positive relationship is not statistically significant [$p = 0.133$]. These results, depicted in Table III, imply that the schoolteachers' attitude [$\alpha = 0.90$] towards raising cyber-safety awareness, is not a predictor of their behaviour of raising cyber-safety awareness at their schools and in their teaching. This finding is in the context of a weak, positive correlation between attitude and intention [$r = 0.26, n = 109, p < 0.05$], and that attitude does not predict intention [$\beta = 0.09, n = 109, p > 0.05$].

F. Subjective Norms and Behaviour

The multiple regression analysis between subjective norms and behaviour discloses that subjective norms predict behaviour [$\beta = 0.25, n = 109, p < 0.05$]. This positive relationship is statistically significant [$p = 0.014$]. These results, also depicted in Table III, suggest that the schoolteachers' subjective norms [$\alpha = 0.63$] (i.e. views of significant others), are a predictor of their behaviour of raising cyber-safety awareness at their schools and in their teaching. This finding is in the context of a strong, positive correlation between subjective norms and intention [$r = 0.66, n = 109, p < 0.05$], and that subjective norms do predict intention [$\beta = 0.45, n = 109, p < 0.05$].

G. Perceived Behavioural Control and Behaviour

The multiple regression analysis between perceived behavioural control and behaviour unveils that perceived behavioural control similarly predicts behaviour [$\beta = 0.28, n = 109, p < 0.05$]. This positive relationship is statistically significant [$p = 0.004$]. These results, also depicted in Table III, suggest that the schoolteachers' perceived behavioural control [$\alpha = 0.68$] (i.e. additional resources and opportunities which facilitate cyber-safety awareness), are a predictor of the schoolteachers' behaviour of raising cyber-safety awareness at their schools and in their teaching. This finding is in the context of a strong, positive correlation between perceived behavioural control and intention [$r = 0.64, n = 109, p < 0.05$], and that perceived behavioural control also predicts intention [$\beta = 0.45, n = 109, p < 0.05$] along with subjective norms.

V. CONCLUSION

The results of this study confirm that social and peer pressure on the teacher by significant others and influential schoolteachers, will positively: 1) influence their intention to raise cyber-safety awareness at their schools in the next 12

months; and 2) influence their behaviour of raising cyber-safety awareness in their teaching. The results of a stepwise regression analysis depicted in Appendix A corroborate this finding, and confirm that subjective norms are the strongest predictor of intention ($\Delta R^2 = 0.370$). In light of this, the South African Department of Basic Education (DBE) is encouraged to identify influential schoolteachers (i.e. phase heads, sports and cultural coordinators, principals and their deputies, etc.), and to groom them into cyber-safety awareness advocates, for the purposes of influencing other teachers or their peers. These advocates should be provided frequent, adequate cyber-safety awareness training, which is school grade-appropriate, for sharing with other teachers.

The results of this study further find that should the South African DBE provide teachers with requisite resources, opportunities, and support which facilitates cyber-safety awareness (i.e. media selection models, time, paraphernalia, training, incentives, recognition, etc.), this will also positively: 1) influence their intention to raise cyber-safety awareness at their schools in the next 12 months; and 2) influence their behaviour of raising cyber-safety awareness in their teaching. The results of the stepwise regression analysis corroborate this finding, and confirm perceived behavioural control as the second strongest predictor of intention ($\Delta R^2 = 0.168$).

The evaluation (e.g., value or pleasure) of raising cyber-safety awareness by teachers was not found to predict the schoolteachers' intention to raise cyber-safety awareness at their schools in the next 12 months, nor did it predict the schoolteachers' behaviour of raising cyber-safety awareness in their teaching. The results of the stepwise regression analysis also corroborate this finding, and confirm attitude as the weakest predictor of intention ($\Delta R^2 = 0.067$). As such, efforts should be expanded to optimise teachers' and learners' attitudes, by enhancing the instrumental evaluation (e.g., value or worth), and experiential quality (e.g., pleasure or fun) of raising cyber-safety awareness at schools. This can be achieved by highlighting the relevance and importance of cyber-safety awareness, and making it more enjoyable through the use of game-based and simulation-led delivery methods. For future research, the current study can be replicated for comparative reasons.

APPENDIX

STEPWISE REGRESSION ANALYSIS FOR ATTITUDE, SUBJECTIVE NORMS, PERCEIVED BEHAVIOURAL CONTROL AND INTENTION

Model Summary						
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics	
					R Square Change	F Change
1	.259 ^a	.067	.059	1.08709	.067	7.723
2	.662 ^b	.438	.427	.84809	.370	69.805
3	.778 ^c	.606	.594	.71347	.168	44.776

Model Summary			
Model	Change Statistics		
	df1	df2	Sig. F Change
1	1	107	.006
2	1	106	.000
3	1	105	.000

a. Predictors: (Constant), Attitude measure, alpha = .90
 b. Predictors: (Constant), Attitude measure, alpha = .90, Subjective Norms measure, alpha = .63
 c. Predictors: (Constant), Attitude measure, alpha = .90, Subjective Norms measure, alpha = .63, Perceived_Beh_Contr, alpha = .68

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

EK supervised the master's full dissertation, from which this article emerged. EK also contributed towards sections I and II. KM collected and analysed the data, and also contributed towards sections III, IV, and V. Both authors had approved the final version of the article.

ACKNOWLEDGMENT

We thank the research participants for their invaluable time and effort. We thank Anja Groenewald Vorster for input in the data analysis. We also thank the Gauteng Department of Education for the approval to conduct the research in their school districts.

REFERENCES

- [1] Ł. Tomczyk and K. Kopecký, "Children and youth safety on the Internet: Experiences from Czech Republic and Poland," *Telematics and Informatics*, vol. 33, no. 3, pp. 822-833, 2016.
- [2] T. Oyedemi, "Participation, citizenship and internet use among South African youth," *Telematics and Informatics*, vol. 32, no. 1, pp. 11-22, 2015.
- [3] Statista. South Africa: Digital population as of January 2020. Statista.com. [Online]. Available: <https://www.statista.com/statistics/685134/south-africa-digital-population/>
- [4] E. Kritzinger, "Cultivating a cyber-safety culture among school learners in South Africa," *Africa Education Review*, vol. 14, no. 1, pp. 22-41, 2017.
- [5] A. K. Przybylski, K. Murayama, C. R. DeHaan, and V. Gladwell, "Motivational, emotional, and behavioral correlates of fear of missing out," *Computers in Human Behavior*, vol. 29, no. 4, pp. 1841-1848, 2013.
- [6] Q. Li, "New bottle but old wine: A research of cyberbullying in schools," *Computers in Human Behavior*, vol. 23, no. 4, pp. 1777-1791, 2007.
- [7] A. P. Sykiotou, "Trafficking in human beings: Internet recruitment. Misuse of the Internet for the recruitment of victims of trafficking in human beings," 2007.
- [8] K. A. Farina, "Cyber-crime: Identity theft," *International Encyclopedia of the Social & Behavioral Sciences*, vol. 2, no. 5, pp. 633-637, 2015.
- [9] N. A. G. Arachchilage and S. Love, "A game design framework for avoiding phishing attacks," *Computers in Human Behavior*, vol. 29, no. 3, pp. 706-714, 2013.
- [10] S. Livingstone, L. Haddon, A. Görzig, and K. Ólafsson, "Risks and safety on the internet: The perspective of European children. Full findings," LSE, London: EU Kids Online, 2011.
- [11] H. A. Kruger, L. Drevin, S. Flowerday, and T. Steyn, "An assessment of the role of cultural factors in information security awareness," *2011 Information Security for South Africa*, Johannesburg, 2011, pp. 1-7.
- [12] S. Koultis, "Improving security knowledge, skills and safety," *Computer Fraud & Security*, vol. 2016, no. 4, pp. 12-14, 2016.
- [13] S. Solms and R. Solms, "Towards cyber-safety education in primary schools in Africa," in *Proc. 8th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014)*, Plymouth, United Kingdom, 2014, pp. 185-197.
- [14] A. Knabe, "Applying Ajzen's theory of planned behavior to a study of online course adoption in public relations education," Ph.D. thesis, Marquette Univ., Milwaukee, WI, 2012.
- [15] I. Ajzen and M. Fishbein, *Understanding Attitudes and Predicting Social Behavior*, Englewood Cliffs, NJ: Prentice-Hall, 1980.
- [16] A. H. Eagly and S. Chaiken, *The Psychology of Attitudes*, Belmont, CA: Thomson-Wadsworth, 1993.
- [17] L. Aiken, *Attitude and Related Psychosocial Constructs*, Thousand Oaks, CA: Sage Publications, 2002.
- [18] I. Ajzen, "The theory of planned behavior," *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179-211, 1991.
- [19] G. D. Sideridis, A. Kaissidis, and S. Padelidiu, "Comparison of the theories of reasoned action and planned behavior," *British Journal of Educational Psychology*, vol. 68, no. 4, pp. 563-580, 1998.
- [20] J. F. George, "Influences on the intent to make Internet purchases," *Internet Research*, vol. 12, no. 2, pp. 165-180, 2002.
- [21] R. P. Robinson and D. Doverspike, "Factors predicting the choice of an online versus a traditional course," *Teaching of Psychology*, vol. 33, no. 1, pp. 64-68, 2006.
- [22] J. Lee, F. A. Cerreto, and J. Lee, "Theory of planned behavior and teachers' decisions regarding use of educational technology," *Educational Technology & Society*, vol. 13, no. 1, pp. 152-164, 2010.
- [23] N. D. Moss, E. L. O'Connor, and K. M. White, "Psychosocial predictors of the use of enhanced podcasting in student learning," *Computers in Human Behavior*, vol. 26, no. 3, pp. 302-309, 2010.
- [24] P. D. Reynolds, *A Primer in Theory Construction*, Indianapolis: Bobs Merrill Company, 1971.
- [25] G. Godin and G. Kok, "The theory of planned behavior: A review of its applications to health-related behaviors," *American Journal of Health Promotion*, vol. 11, no. 2, pp. 87-98, 1996.
- [26] C. Makaure, "An analysis of public perception towards consuming genetically modified crops and the acceptance of modern agricultural biotechnology: A South African case study," M.A. dissertation, Univ. of South Africa, Pretoria, 2019.
- [27] Y. Zhang, L. Jing, Q. Bai, W. Shao, Y. Feng, S. Yin, and M. Zhang, "Application of an integrated framework to examine Chinese consumers' purchase intention toward genetically modified food," *Food Quality and Preference*, vol. 65, pp. 118-128, 2018.
- [28] A. S. Notani, "Moderators of perceived behavioral control's predictiveness in the theory of planned behavior: A meta-analysis," *Journal of Consumer Psychology*, vol. 7, no. 3, pp. 247-241, 1998.
- [29] R. Schulze and W. W. Wittmann, "On the moderating effect of the principle of compatibility and multidimensionality of beliefs: A meta-analysis of the theory of reasoned action and the theory of planned behavior," in *Meta-Analysis: New Developments and Applications in Medical and Social Science*, R. Schulze, H. Holling and D. Bohning, Eds., Seattle, WA: Hogrefe & Huber, 2003, pp. 219-250.
- [30] I. Ajzen, *Attitudes, Personality, and Behavior*, Chicago: Dorsey Press, 1988.
- [31] D. J. Canary and D. R. Seibold, *Attitudes and Behavior: An Annotated Bibliography*, New York: Praeger, 1984.
- [32] B. H. Sheppard, J. Hartwick and P. R. Warshaw, "The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research," *Journal of Consumer Research*, vol. 15, no. 3, pp. 325-343, 1988.
- [33] I. Ajzen, "Consumer attitudes and behaviour: The theory of planned behaviour applied to food consumption decisions," *Rivista di Economia Agraria*, vol. 70, no. 2, pp. 121-138, 2015.
- [34] Y. G. Kim, S. Y. Jang, and A. K. Kim, "Application of the theory of planned behaviour to genetically modified foods: Moderating effects of food technology neophobia," *Food Research International*, vol. 62, pp. 947-954, 2014.
- [35] G. Prati, L. Pietrantoni, and B. Zani, "The prediction of intention to consume genetically modified food: Test of an integrated psychosocial model," *Food Quality and Preference*, vol. 25, no. 2, pp. 163-170, 2012.
- [36] A. Spence and E. Townsend, "Implicit attitudes towards genetically modified (GM) food: A comparison of context-free and context-dependent evaluations," *Appetite*, vol. 46, no. 1, pp. 67-74, 2006.

Copyright © 2021 by the authors. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited ([CC BY 4.0](https://creativecommons.org/licenses/by/4.0/)).



Elmarie Kritzinger joined the University of South Africa's College of Science, Engineering and Technology in 2000 and currently holds the position of professor in the School of Computing (Department of Information System). Prof Kritzinger obtained her PhD in information systems at the tender age of 29 and was awarded the "Youngest PhD" at the University of South Africa in 2008. Prof Kritzinger completed her PGCE in 2016 and is currently completing her MEd ICT in Education.

Since obtaining her PhD, Prof. Kritzinger has established herself as a mature researcher and has published in accredited national and international journals, contributed to chapters in books, and presented at peer-reviewed conferences. Although her research focuses primarily on Information

Security (Cyber) Awareness, she is cross-disciplinary skilled in the fields of information systems and education.

Founding member and project leader of a Cyber Awareness Project within the School of Computing at UNISA, her aspiration is to provide school children and communities in South Africa and Africa with cyber awareness and supporting documents to enrich their knowledge and ensure they are cyber safe. This project is multi institutional with partners in industry, academia, government and public sector. As part of her corporate citizenship, Prof Kritzinger has successfully organized colloquiums and workshops on key discussions relating to cyber awareness and have been an invited speaker for a number of workshops and conferences on the topic of Information Security Awareness and Education.

A number of honours, Master's and Doctoral students are currently under her supervision within the fields of cyber safety, information systems and education. She is currently NRF C3 rated within South Africa.



Kagisho Mabitle was born in South Africa on the 10th of May 1982. Mabitle holds the following degrees: an MSc (computing) from the University of South Africa earned in 2020; a BScHons (information systems) from the same institution earned in 2017; and a BCom (information systems; business Finance) from the University of the Witwatersrand earned in 2005. Kagisho is currently enrolled for an MBA (leadership) at the University of London. Four papers from the MSc full dissertation have been published; in this journal, *Lecture Notes in Electrical Engineering*, *Advances in Intelligent Systems and Computing*, and the *International Journal of Innovation, Management and Technology*. In 2021, Mabitle will instigate PhD studies. Beyond lecturing and tutoring computing modules at the University of South Africa, Mabitle also facilitates and leads community engagement projects on cyber-safety awareness in South African schools. Prior to becoming an academic, Mr. Mabitle was a Certified Business Analysis Professional®.