INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 13, Issue 12, (2023) E-ISSN: 2222-6990

Developing A Model for The Security of Malaysian Youth Privacy Data: MyPROTECT

Shariffah Mamat[1], Wan Amizah Wan Mahmud[2], Arina Anis Azlan[3] & Asyraf Afthanorhan[4]

[1]Institute for Youth Research Malaysia, Ministry of Youth and Sports Malaysia, 62570 Putrajaya, MALAYSIA, [2,3]Universiti Kebangsaan Malaysia, 43650 Bangi, Selangor, MALAYSIA, [4]Faculty of Business and Management, Universiti Sultan Zainal Abidin (UniSZA), 21300 Gong Badak, Terengganu, MALAYSIA

Email**:** shariffah@iyres.gov.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v13-i12/19793 DOI:10.6007/IJARBSS/v13-i12/19793

Published Date: 05 December 2023

Abstract

The personal data safety of cyber users is a threat in today's digital world. The public knows that the Covid-19 pandemic has become a catalyst for the digital technology transformation in the history of human civilization. This article aspires to test a model created to examine the factors protecting the safety of Malaysian youth's data. The questionnaire is circulated online among young people aged 19 years to 30 years using multistage random sampling. A total of 535 respondents were selected from Putrajaya and Cyberjaya as a free trial spot area provided by the government. The instruments are developed based on 11 constructs attitude, subjective norms, behavioral control, intention, environment support, usefulness, ease of use, trust, treatment assessment, coping skills, and self-efficacy. The model was analyzed using Structural Equation Modeling with IBM-SPSS AMOS 27.0 software. This approach is employed to test the developed model yielded from several established theories such as the Theory of Planned Behavior (TPB), Decomposed Theory of Planned Behavior (DTPB), Protection Motivation Theory (PMT), and Social Cognitive Theory (SCT). The results of this study show that all constructs referred to as MyPROTECT achieved the goodness fit model for this study.

Keywords: Security, Youth Privacy Data, Structural Equation Model, Confirmatory Factor Analysis, Fitness Index

Introduction

Communication plays a critical role in human interactions, enabling the exchange of ideas, feelings, and thoughts. It involves more than the simple transmission of information. Communication is an intricate process encompassing interpreting messages, understanding the intended meanings, and reacting accordingly (Chen, 1997). The process ofcommunication is influenced by various factors, including individual traits, social contexts, and cultural norms, which in turn shape the way we perceive and engage with others and theworld around us.

Online transactions and communication are part of the demands in today's digital technology era. Comparisons between countries based on the Global Digital Report (2018) show a rapid growth in media use prevailing in the country of Saudi Arabia. Between January 2017 and 2018, the Middle Eastern country showed social media use grew by 32% with 1% overcoming the Indian state. In Southeast Asian countries, it shows that Indonesia is in third place at 23% and Vietnam is in sixth ranking at 20%.

The impenetrability of the media without being balanced by the awareness of personal data security threats becomes a multi-party dilemma. The Global Treat Report 2022 mentioned that eCrime threats accounted for almost 49% compared to other threats. The fears about the security threat of personal data are real and even more worrying when a total of 78% were not concerned about their personal information being disclosed through social media (Chewae et al., 2015). The two main cybercrime categories include cyber-dependent crimes such as hackers, software, and attack denials and both are cybercrime crimes such as 'phishing', identity theft, cyber romance fraud, and online purchase scams (Wagen & Pieters, 2020).

In addition, the Malaysian Youth Index (MYI) coordinated by the Institute for Youth Research Malaysia (IYRES) shows that safety indicators when using the internet under the Safety Domain were at a score of 68.77 (moderate) in 2017 when compared to a score of 76.13 (satisfactory) in 2016. In 2015, this indicator was a score of 76.76 (satisfactory) (IYRES, 2017). Meanwhile, the same study in 2020 showed that the Media Breach Domain recorded a score of 59.83, which is at an unsatisfactory level (IYRES 2020) compared to a score of 60.36 or a medium level in 2019. MYI's showed that scores were declining from low level to unsatisfactory levels.

Meanwhile, the Global Security Index (GCI) (2020) reported that the Republic of Singapore recorded the highest score of 98.52 ahead of other countries by being in the first position to overcome the Indonesian state with a score of 94.88, namely from the third rank falling to the sixth rank. Furthermore, Malaysia soared to second place with a score of 98.6. GCI uses five pillars as a mechanism for measuring the stage of cyber safety in the global rankings, namely legal measures; Technical measures; Organizational measures; Capacity Development, and Cooperation.

Reflecting on this scenario, this article highlights the models to contribute to the security of privacy data for youth. The youngster is a valuable asset to a nation and should be guided by an adult. In nurturing positive youth development, the synergy between young individuals and adults creates a powerful formula for molding the future of the next generation. Indeed, young individuals require competencies such as digital literacy, communication, and problem-solving as integral components of their personal character development phase. In addition, the data findings outlined in this article play a role in supporting and fortifying the implementation of the in-force Personal Data Security Act in Malaysia 2010 (Act of 709).

A Theory for behavior change

To understand this social phenomenon, this study used the Theory of Planned Behavior (TPB) by Icek Azjen (1991) as the basis for the model formation. The decomposed Theory of Planned (DTPB) by Taylors and Todd (1995), the Protection Motivation Theory (PMT) by Ronald W. Rogers (1983), and the Social Cognitive Theory (SCT) by Bandura (1991) were used as predictors of assumptions to improve TPB. The combination of TPB and PMT is appropriate to be used to describe awareness of the security of personal data, organizational policies, and

procedures as well as the experience and involvement of individuals influencing the behavior of individuals in maintaining the security of personal data (Safa et al., 2015).

Method

Targeted Samples

The study sample was selected from Malaysian youths aged 19 years to 30 years. These 535 samples were selected using the multistage random sampling method considering gender, age, and ethnicity. Putrajaya and Cyberjaya were chosen as the study site which is the location of a free 5G service trial by the government. The selection of these locations provides an equal opportunity and probability for the target group to be selected for the study.

Instrument of Measurement

The instrument of study was developed from an adaptation of a literature review conducted by a previous scholar. There were 11 variables used in this study as a factor to protect the security of Malaysian youth data during online transactions or communication. The factors are attitude, subjective norms, behavioral control, intention, environmental support, usefulness, ease of use, trust, treatment assessment, coping skills, and self-efficacy. The instrument was divided into five sections with seven Likert scales as an answer option. Since the subject of study is a group of youths of various educational backgrounds, each item has been tested to meet the understanding and clarity of the sentence structure.

Data Analysis and Findings

IBM-SPSS AMOS 27.0 software has been used with full information maximum likelihood estimator through the parametric procedure to test the developed model which provides more information including standardized loadings, square multiple correlations, construct correlation, and fitness indexes for concluding model performance. Confirmatory Factor Analysis (CFA) became a method of choice when assessing the model performance due to its proven estimation power in confirmatory research.

Scale Validity and Reliability

The measurement model was validated by the CFA method to assess the construct reliability and validity of each construct of the measurement model. The construct validity in the measurement model is examined through convergent validity and discriminant validity. Specifically, the convergent validity can be checked in two ways namely Average Variance Extracted (AVE) and standardized loadings (the minimum acceptable value is 0.60; (Afthanorhan et al., 2019). For construct reliability, the measurement model was tested using composite reliability (CR).

Discriminant Validity

The discriminant validity is achieved through the Discriminant validity index summary to prove that all constructs in the study are discriminatory to each other (Awang et al., 2018). There are two calculation methods for analyzing this test which are the Fornell and Larcker (1981) criterion and Heterotrait-Monotrait method (HTMT). In this study, the Fornell and Larcker criterion was applied as recommended by many scholars (Afthanorhan et al., 2020).

The SEM procedure used in this study has followed the criteria suggested by the scholars Fornell & Larcker criterion. A good model is achieved at a discriminant value when it reaches

a correlation value of less than 0.85 and a diagonal value higher than the value of each correlation between the constructs used (Fornell & Larcker, 1981).

Average Variance Extracted (AVE) and Composite Reliability (CR)

In this procedure, three tests were conducted to analyze the reliability to achieve convergence validity requirement which is, Cronbach's Alpha analysis (descriptive for scale if item deleted); composite reliability (CR) analysis, and average variance extracted (AVE) analysis. The execution of this analysis aimed to determine the ability of trust based on the mode of investigation (Jimmi et al., 2021). The Cronbach's Alpha test is performed to test internal reliability Aftharnohan (2014) and is achieved when the score is greater than 0.70 (> 0.70) (Nunnally, 1978; Pallant, 2011; Hair et al., 2010).

Model Fitness

Based on the previous scholar's suggestion, the model studied needs to achieve a goodness of fit index as detailed in Table 1.

Table 1
Model fitness index

Goodness Index	Level of Acceptance	Literature
Absolute fit		
Root Means Square of Error Approximation (RMSEA)	>.08 - 1.0 (ideal)	Browne & Cudek, 1993; Awang, Hui & Zainudin, 2018
Incremental Fit		
The Goodness of Fit Index (GFI)	> .85 - .90 (ideal)	Joreskog & Sorbo n, 1984; Awang, Hui & Zainudin, 2018
Adjusted goodness-of-fit Index (AGFI)	> .85 - .90 (ideal)	Tanaka & Huba, 1985; Awang, Hui & Zainudin, 2018
Comparative Fit Index (CFI)	> .85 - .90 (ideal)	Bentler, 1990; Awang, Hui & Zainudin, 2018
Tucker-Lewis Index (TLI)	> .85 - .90 (ideal)	Bentler & Bonett 1980); Awang, Hui & Zainudin, 2018
Normed Fit Index (NFI)	> .85 - .90 (ideal)	Bollen, 1986; Awang, Hui & Zainudin, 2018
Parsimonious fit		
Chi-square/degree of freedom (df)	< 5.0, < 3.0 (ideal)	Marsh & Hocevar, 1985; Awang, Hui & Zainudin, 2018

***Source**: Awang, Hui & Zainudin, 2018*

Results and Discussion

Analysis of the data

Based on the objectives of the study, the CFA exam was carried out by taking all SEM-AMOS analysis procedures. In this study, the 11 dimensions are attitude (7 items), subjective norms (5 items), behavioral control (4 items), an environment supportive (2 items), intention (3 items), usefulness (4 items), ease of use (4 items), trust (4 items), treat assessment (5 items), coping skills (7 items) and self-efficacy (7 items). The loading factor for each item must be >.6

to achieve a goodness fit index (Hair et al., 2010). Table 2 shows items before and after analysis in the one-dimensionality approach.

Table 2
Unidimensionality result

	No. of the item before deleted item	**No. of the item after delete**
Environment supportive	2 items	2 items
Usefulness	4 items	4 items
Ease of use	4 items	4 items
Trust	4 items	4 items
Attitude	7 items	7 items
Subjective norms	5 items	5 items
Behavioral control	4 items	4 items
Treat assessment	5 items	5 items
Coping skill	7 items	6 items
Self-efficacy	7 items	6 items
Intention	3 items	3 items

The pooled CFA model was conducted based on a conceptual framework of this study involving 11 constructs. Then the model is acknowledged as the Model of Malaysian Youth Personal Data Security (MYPROTECT). Table 3, Figure 1, and Figure 2 indicate the number of items representing the 11 constructs used in the analysis to achieve a goodness fit index.

Table 3
Goodness fit index

Model MyPROTECT	**Absolutefit**	**Incrementalfit**			**Parsimoniousfit**
	RMSEA	**CFI**	**TLI**	**NFI**	**X^2/df**
Before (52 items)	.013	.993	.993	.919	1.084
After (50 items)	.012	.995	.994	.925	1.071
Result			Achieved		

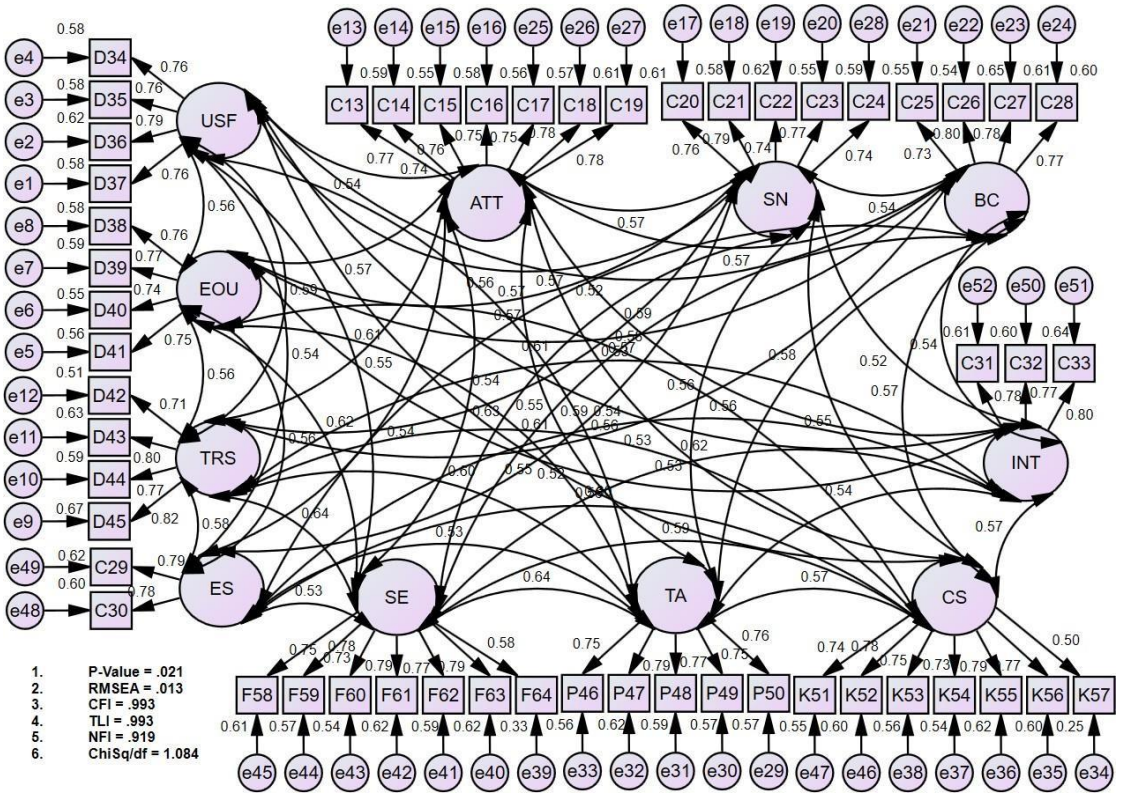

Figure 1
Pooled-CFA before the deleted item

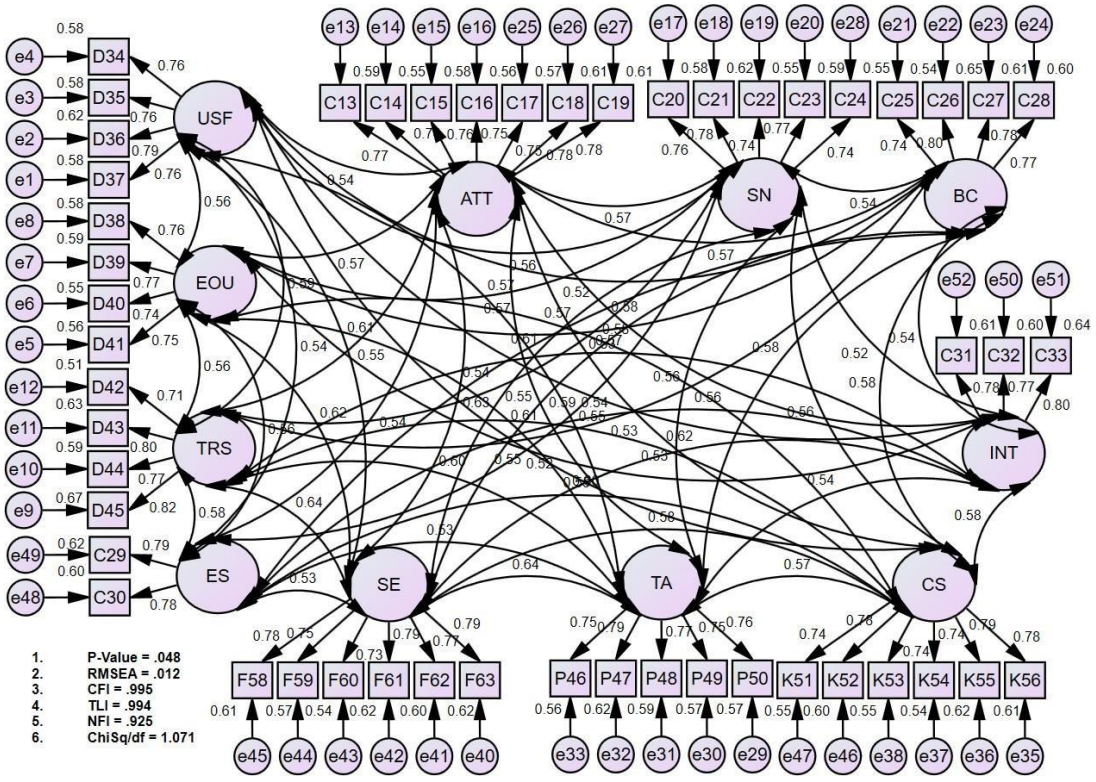

Figure 2
Pooled-CFA after deleted item

As shown in the model, the analysis results indicate the model has achieved the index requirement value for all measurement indices used. Figures 1 and 2 showed the RMSEA index recorded .012 meeting the suggestion (Browne & Cudek, 1993) i.e. less than 0.1 (< 0.1); Chisquare/df is 1,071. Furthermore, the CFI value is .995; the TLI value is .994 and the NFI value is .925 with 50 items. All three indices exceed .90 (Bentler, 1990; Bentler & Bonett, 1980). The TLI and NFI indices charge a larger and more complicated score to achieve than the CFI but only one of the corresponding statistical values is reported to be highly related (Kenny, 2014). Additionally, CFI is more often used in reporting and is better than TLI. Both the CFI and the NFI need to be reported in the AMOS output, but Bentler (1990) argues that the CFI should be the preferred reporting index (Byrne, 2010).

Convergent Validity

Table 4 shows that MyPROTECT was successfully achieved after performing the index-matching procedure as recommended. The results of the analysis show that Cronbach's Alpha value for each latent variable meets criteria above 0.70 where, ATT is .892; NS is .891; BC is .892; INT is .894; ES is .899; USF is .892; EOU is .892; TRS is .891; TA is .889; CS is .892 and SE is .887. Furthermore, the CR value of MyPROTECT has met the requirements of convergence validity and reliability which exceeds the value of 0.6. The findings showed that the ATT factor recorded a value of 0.906; NS recorded a value of 0.872; BC recorded a value of 0.856; INT recorded a value of 0.828; ES recorded a value of 0.761; USF recorded a value of 0.853; The EOU recorded a value of 0.841; TRS recorded a value of 0.857; TA recorded 0.875; CS recorded a value of 0.892 and SE recorded a value of 0.897. Lastly, the AVE value of MyPROTECT shows that all latent variables record a value of more than 0.5. These latent variables were found to meet the validity of convergence and composite reliability with a balance between AVE and CR (Fornell & Larckel, 1981). The latent variable that achieved the AVE score was ATT which is 0.580; SN which is 0.578; BC which is .0598; INT which is 0.617; ES which is 0.615; USF which is 0.592; EOU which is 0.570; TRS which is 0.600; TA which is 0.584; CS which is 0.578 and SE which is 0.592.

Table 4
Convergent validity of the construct

Construct	Item	Factor loading	Cronbach'sAlpha	CR	AVE
ATT	C13	.768	.892	0.906	0.580
	C14	.739			
	C15	.759			
	C16	.748			
	C17	.755			
	C18	.783			
	C19	.778			
SN	C20	.761	.891	0.872	0.578
	C21	.785			
	C22	.742			
	C23	.768			
	C24	.744			
BC	C25	.735	.892	0.856	0.598

	C26	.804				
	C27	.779				
	C28	.773				
INT	C31	.778	.894		0.828	0.617
	C32	.803				
	C33	.775				
ES	C30	.778	.899		0.761	0.615
	C29	.790				
	D37	.763				
USF	D36	.790	.892		0.853	0.592
	D35	.761				
	D34	.764				
EOU	D41	.747	.892		0.841	0.570
	D40	.743				
	D39	.766				
	D38	.764				
TRS	D45	.820				
	D44	.766	.891		0.857	0.600
	D43	.796				
	D42	.712				
TA	S50	.758	.889		0.875	0.584
	S49	.752				
	S48	.770				
	S47	.789				
	S46	.750				
CS	S57	Deleted		.892	0.892	0.578
	S56	.780				
	S55	.785				
	S54	.738				
	S53	.742				
	S52	.777				
	S51	.739				
SE	F64	Deleted	.887		0.897	0.592
	F63	.786				
	F62	.772				
	F61	.788				
	F60	.734				
	F59	.755				
	F58	.781				

Discriminant Validity

Table 5 shows the discriminant validity result. There are two numerous techniques to establish the discriminant validity namely Fornell & Larcker, and Hetero Trait Mono-trait ratio criterion. In common factor-based SEM as applied for this study, the Fornell & Larcker criterion is highly recommended to determine the usefulness of each construct (Afthanorhan, Ghazali & Rashid, 2021). The model is considered discriminant if the construct correlation is below 0.85 and the diagonal values (bold) are higher than all correlations. In this case, the discriminant validity for this model is valid and suitable for further investigation.

Table 5
Discriminant validity for MyPROTECT

	ESF	**UOF**	**EAU**	**TRS**	**ATT**	**SN**	**BC**	**TA**	**CS**	**SE**	**INT**
ESF	**0.784**										
UOF	0.537	**0.770**									
EOU	0.562	0.563	**0.755**								
TRS	0.585	0.589	0.556	**0.775**							
ATT	0.537	0.539	0.574	0.550	**0.762**						
SN	0.518	0.558	0.566	0.555	0.572	**0.760**					
BC	0.574	0.516	0.528	0.531	0.568	0.541	**0.773**				
TA	0.530	0.571	0.543	0.596	0.605	0.559	0.581	**0.764**			
CS	0.552	0.546	0.582	0.555	0.532	0.557	0.577	0.574	**0.760**		
SE	0.529	0.609	0.623	0.639	0.628	0.609	0.581	0.640	0.584	**0.770**	
INT	0.545	0.590	0.597	0.573	0.563	0.523	0.537	0.545	0.576	0.621	**0.785**

Structural Model

Figure 3 shows a standardized structural model for MyPROTECT. After deleting two items from the model due to poor factor loading, the rest of the items meet the acceptable limit of 0.60. In addition to that, the fitness indexes namely Chisq/df = 1.431 < 3.0; RMSEA= 0.028 < 0.08; CFI = 0.966 > 0.90; TLI=0.964 > 0.90; and NFI = 0.897 > 0.85 meet the threshold values. The construct correlation is also lower than 0.85 suggesting that the proposed model is free from any redundancy issues. To test the construct reliability and validities, the descriptive for scale if item deleted, composite reliability, average variance extracted, and discriminant validity were conducted.

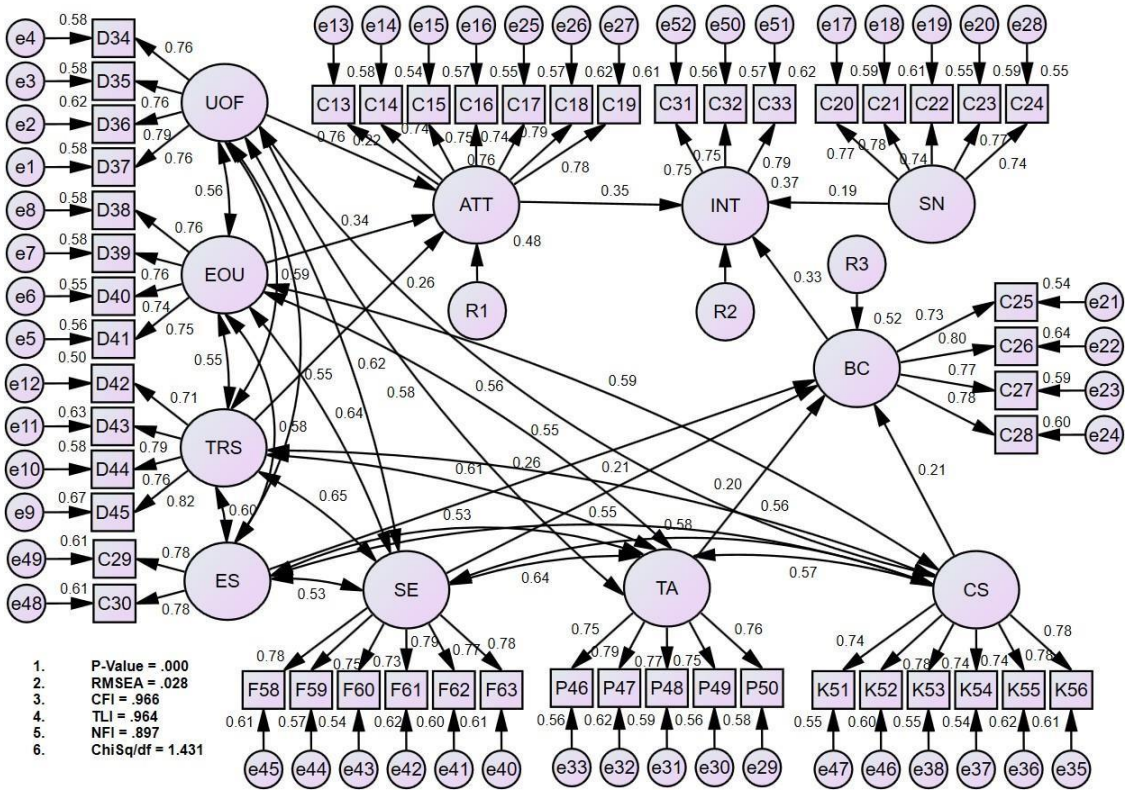

Figure 3
MyPROTECT standardized structural model

Table 6 shows the hypothetical results of this study for MyPROTECT. The findings show that ATT has a positive and significant relationship with the USF variable with its value (β = .220, p< 0.05); against EOU with its value i.e. (β = .362, p< 0.05) and against TRS with values (β =.233, p< 0.05). Further, BC showed a positive and significant relationship to relationship with ES (β = .237, p< 0.05); against SE (β = .211, p< 0.05); against TA (β = .187, p< 0.05) and against CS (β = .192, p< 0.05). INT shows a positive and significant relationship with ATT i.e. (β = .345, p< 0.05); against SN (β = .197, p< 0.05) and against BC i.e. (β = .338, p< 0.05).

Table 6
Hypothesis result

	Result		Estimate	S.E.	C.R.	P	Significant
ATT	<---	UOF	.220	.056	3.958	***	par_38
ATT	<---	EOU	.362	.060	6.015	***	par_39
ATT	<---	TRS	.233	.049	4.757	***	par_40
BC	<---	ES	.237	.054	4.402	***	par_44
BC	<---	SE	.211	.060	3.536	***	par_45
BC	<---	TA	.187	.056	3.343	***	par_46
BC	<---	CS	.192	.052	3.720	***	par_47
INT	<---	ATT	.345	.052	6.625	***	par_41
INT	<---	SN	.197	.046	4.301	***	par_42
INT	<---	BC	.338	.054	6.202	***	par_43

Discussion

Based on the current situation and the probability of personal data security threats being exposed to different ages, it is recommended that the study be conducted more comprehensively. Researchers also recommended that this study be conducted at the national level to enable policymakers to receive more comprehensive input. This is because the researchers used only two locations for this academic study. The study of several locations in Malaysia by a group of researchers also suggested that further studies be carried out to find out which geographical positioning factors have different implications (Arifain et al., 2021).

In this specified context, the results of this study will suggest to the Government to broaden the scope of research data collection, encompassing not just the youth but extending to all Malaysians, without being confined to the age range of 15-30 years. Drawing from the collected data it is anticipated that the government and its stakeholders in Youth Development will utilize this information to formulate strategic plans, policies, or programs, adapting them for more impactful and efficient implementation.

Moreover, in preventing personal data dissemination issues, the European Union Agency for Network and Information Security (2017) has outlined four levels of impact of personal data security threats on individuals namely low, medium, high, and very high impact. Low impact is defined as individuals may face minor difficulties that they will overcome without any problems such as wasting time, distraction, discomfort, etc. Moderate impact i.e. the individual may face significant difficulties that will be overcome despite some difficulties such as additional costs, denial of access, fear, lack of understanding, stress, minor physical illness, and others. High impact is defined as individuals who may face significant consequences that must be overcome with serious difficulties such as misuse of funds, being blacklisted by financial institutions, property damage, job loss, impaired health, and others. Lastly, the impact is very high i.e. individuals who may face significant or insurmountable consequences such as work disabilities, long-term psychological or physical illness, death, and others.

Rather than dealing with the repercussions of the severe impacts faced after becoming a victim of cyber threats, it is more effective to take measures to prevent them. The strategy is to create awareness and skills at an earlier stage for youths before they become victims of cybercrime. Precisely, the impact of this severity can be avoided if youths have the skills to change their behavior of protecting the security of their data while making transactions or communicating online.Consumerinfo.my (2020) recommends seven simple steps or methods to protect the personal data and privacy of users online i.e. by using a virtual private network (VPN); using anti-virus software; carefully sharing it on social media and the internet; using a stronger and different password for each online account; observing search sites that suddenly make advertising; update applications and operating systems regularly and always be on duty using Wi-Fi facilities in public places.

Blog Data Privacy Manager (2021) i.e. One blog site also gives almost the same recommendation which is to build a strong password; use different passwords for different social media accounts; change passwords frequently; avoid using a public computer or borrow a friend's phone to access social media accounts; be wary of using public Wi-Fi in case of accessing social media accounts; using a VPN, avoid sharing devices to access social media accounts, avoiding accessing social media links even if shared by friends; protect the device with a password to protect your social media from being stolen or invaded by unscrupulous people. Surprisingly, not all youths acquire proficiency in utilizing digital technology. Formal educational institutions, whether at the school or university level, should be the primary setting for acquiring strategies that involve technical skills.

Internet adoption or net citizens always need to remind themselves that the internet is synonymous with the public, no personal information can be hidden after an individual has uploaded information in the form of personal data or pictures even on an online platform (Kumar et al., 2013). In short, if you don't want to be seen then in no case should you upload personal information using your social media. Personal data breaches are often associated with human error factors (Hammouchi et al., 2019). It is therefore very important to raise individuals' awareness of knowledge that can protect the security of their data.

Conclusion

The security of personal data is a concern throughout the world community, especially in the face of the Covid-19 pandemic. This study supports significantly and positively the behavioral intent to practice e-commerce (Agarwal & Barn, 2016). A study of e-government services in Malaysia found that e-government users are more comfortable using e-government services in their way which is admittedly more user-friendly. Users can do it on their own even if no one gives guidance to use e-government services at any time (Suki & Ramayah, 2010).

The same goes for the findings of studies on young people in Mexico and Colombia that show that there is a positive relationship between attitudes toward privacy and security when communicating or transacting online (Gastelú et al., 2020). Individuals tend to show a positive attitude if a third party asks for permission to use their data for other service marketing purposes (Tsang et al., 2004). Meanwhile, according to Shih & Kwoting (2004), the variable of intent using internet banking can be explained through attitude variables. Attitude is a psychological bias manifested through the expression of likes or dislikes towards a behavior (Alice & Shelly, 1993).

In addition, this study also proves that the findings of this study are in line with the main theory used in this study, TPB. Wherein, the intention is to influence the changing behavior of protecting the security of Malaysian youth's data positively and significantly while conducting banking transactions or communicating online. Meanwhile, the use of PMT for the construct of coping skills is a strong predictor of the intention of protecting the security of personal data online (Tsai et al., 2016).

In addition, the findings of a study on the use of online learning among students found that factors are easy to use and very useful to students of higher learning institutions in Malaysia (Ramayah et al., 2003). These findings are in line with the combination of the use of TPB and DTPB in the context of protecting the security of personal data among youth.

This study is important to verify and develop the theory in the social science discipline in the context of protecting the security of personal data among youths aged 19 to 30 years. Through this study, TPB can be improved with forecasters from DTPB, PMT and SCT specifically in the context of protecting the security of youth's data. The idea of this study which combines four theories, namely TPB, DTPB, PMT, and SCT with the application of Malaysian youth studies, is a contribution to the development of social sciences. This approach develops and tests theoretical models to validate the use of theory in research disciplines based on communication knowledge. This combination of theories is produced to expand these theories by illustrating the extent to which these theories can influence the behavior of human's behavior protecting the security of their data in the face of the needs and challenges of the digital world.

The use of different study subjects in research not only supports the original model developed by a scholar but also releases the opportunity to further expand existing constructs in different contexts and situations (Xue et al., 2021).

Acknowledgment
A bouquet of flowers to everyone who is involved in the completion of this article directly and indirectly. Especially to the members of MENTION, the National University of Malaysia (UKM), and my friend from the Institute for Youth Research Malaysia (IYRES), Ministry of Youth and Sports Malaysia for the moral support.

Reference

Afthanorhan, A., Awang, Z., Rashid, N., Foziah, H., and Ghazali, P. L. (2019). Assessing the effects of service quality on customer satisfaction. *Management Science Letters, 9*(1), 13-24.

Afthanorhan, A., Awang, Z., & Aimran, N. (2020). An extensive comparison of cb-sem and pls-sem for reliability and validity. *International Journal of Data and Network Science, 4*(4), 357-364. https://doi.org/10.5267/j.ijdns.2020.9.003.

Afthanorhan, A., Ghazali, P. L., & Rashid, N. (2021). Discriminant validity: A comparison of CBSEM and consistent PLS using Fornell & Larcker and HTMT approaches. Paper presented at the Journal of Physics: Conference Series, 1874(1). https://doi.org10.1088/1742-6596/1874/1/012085

Afthanorhan, W. (2014) Hierarchical Component Using Reflective-Formative Measurement Model in Partial Least Square Structural Equation Modeling (Pls-Sem*). International Journal of Mathematics, 2*, 33-49.

Agarwal & Bansal. (2016). Application of Decomposed Theory of Planned Behavior for M-commerce Adoption in India. Proceedings of the 18th International Conference on Enterprise Information Systems (ICEIS 2016), (2), 357-367.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211.

Alice, E., and Shelly, C. (1993). The psychology of attitudes. Harcourt Brace. Fort Worth, TX.

Arifain, S. M. K., Yusof, F., Aziz, S., Suhaini, N., Suhaini, N. (2021). The Influence of Social Support on Marriage Satisfaction among Working Women in Selangor, Negeri Sembilan and Melaka*. International Journal of Academic Research in Business and Social Science, 11*(2), 587–595. Doi.10.6007/IJARBSS/v11-i2/8874.

Awang, Z., Hui, L. S., & Syahira, N. F. (2018). Pendekatan mudah SEM: Structural Equation Model. MPSW Rich Resources Sdn. Bhd. Bandar Baru Bangi. 978-967-0942-58-2.

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational behavior and human decision processes, 50*(2), 248-287.

Bentler, P. M. and Bonnet, D. C. (1980). Significance Tests and Goodness of Fit in the Analysis of Covariance Structures. *Psychological Bulletin, 88*(3), 588-606.

Bencheikh, I., Azoulay, K., Mabrouki, J., Hajjaji, S. E., Moufti, Labjar, N. (2021). The use and the performance of chemically treated artichoke leaves for textile industrial effluents treatment. *Chemical Data Collections, 31*(2021), 100597. doi.org/10.1016/j.cdc.2020.100597.

Blog Data Privacy Manager. (2021). How to Protect Your Privacy on Social Media? https://dataprivacymanager.net/how-to-protect-your-privacy-on-social-media.

Browne, M. W., & Cudeck, R. (1993). Alternative ways of assessing model fit. In K. A. Bollen and J. S. Long (Eds.), Testing structural equation models (pp. 136-162). Newbury Park, CA: Sage.

Byrne, B. M. (2010). Structural equation modelling with AMOS: Basic concept, application and programming (2nd. ed). Routledge/Taylor & Francis Group.

Chewae, M., Hayikader, S., Hasan, M. H. & Ibrahim, J. (2015). How much privacy do we still have on social network? *International Journal of science and research publication, 5* (1).

Consumerinfo.my. (2020). How to protect your online privacy and privacy data. Digital World. https://consumerinfo.my/lindungi-data-peribadi-privasi-dalam- talian/?lang=ms

Copriadya, J., Zulnaidi, H., Alimin, M., Albeta, S. W. (2021). In-service training and teaching resource proficiency amongst Chemistry teachers: the mediating role of teacher collaboration. *Heliyon 7*. Doi.10.1016/j.heliyon.2021.e06995

European Union Agency for Network and Information Security. (2017). Handbook on Security of Personal Data Processing. Doi.10.2824/569768

Fornell & Larcker. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error Author(s). *Journal of Marketing Research, 18*(1), 39- 50.

Gastelú, C. A. T., Zanabria, L. F. M., and Armenta, J. A. (2020). The attitude of Latin American Youth towards Online Security and Privacy. *International conference on virtual campus (JIVC)*. 1-5. Doi: 10.1109/JICV51605.2020.9375820.

Global Digital Report 2018. (2018). Digital in 2018: World's internet users pass the 4 Billion Mark. https://wearesocial.com.

Global Cybersecurity Index 2018. (2019). International Telecommunication Union. Available at https://www.itu.int.

Global Cybersecurity Index. (2020). 4. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate Data Analysis. 7th ed. New Jersey, USA: Pearson Education, Inc, Prentice Hall.

Hammouchi, H., Cherqia, O., Mezzoura, G., Ghoghoa, M., Koutb, M. E. (2019). Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches Over Time. *Procedia Computer Science. 151*, 1004-1009.

Institute for Youth Research Malaysia. (2020). Facts and figures Malaysian Youth Index 2020. Ministry of Youth and Sports Malaysia. Putrajaya. Malaysia.

Institute for Youth Research Malaysia. (2017). Facts and figures Malaysian Youth Index 2017. Ministry of Youth and Sports Malaysia. Putrajaya. Malaysia.

Joreskog, K., & Sorbon, D. (1999). Interactive LISREL. User's Guide, Scientific Software

Internatiol. (1998). Prelis: A Program for Multivariate Data Screening and Data Summarization, Second edition, Scientific Software International, Inc., Mooresville.

Kumar, A., Gupta, S. K., Rai, A. K., Sinha, S. (2013). Social networking sites and their security issues. *International Journal of Scientific and Research Publications, 3*(4), 1-5.

Nunnally, J. C. (1978). Psychometric theory (2nd ed.). New York: McGraw-Hill.

Pallant, J. (2011). SPSS Survival Manual: A step by step guide to data analysis using SPSS 4ed. Allen & Unwin. Australia.

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

Shih, Y. Y., & Kwoting, F. (2004). The use of a decomposed theory of planned behavior to study Internet banking in Taiwan. *Internet Research, 14*(3), 213-223.

Suki, N. M., & Ramayah, T. (2010). User Acceptance of the E-Government Services in Malaysia: Structural Equation Modelling Approach. *Interdisciplinary Journal of Information, Knowledge, and Management, 5*, 395-423.

Taylor & Todd. (1995). Understanding information technology usage: A test of competing models. *Information system research, 6*(2), 144-176.

The Crowdstrike. (2022). Global Treat Report 2022. https://go.crowdstrike.com/global-threat-report-2022-thank-you.html

Tsai, M. J., Alhabash S., LaRose R., Rifon N. J., and Cotton S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers and Security, 59*, 138-150.

Tsang, M. M., Ho, S. H., and Liang, T. P. (2004). Consumer Attitudes Toward Mobile Advertising. *International Journal of Electronic Commerce, 83*(3), 65-78.

Ramayah, T., Aafaqi, B., & Jantan, M. (2003). Internet usage among students of an institution of higher learning: The role of motivational variables. The Proceedings of the 1st International Conference on Asian Academy of Applied Business Conference, Sabah, Malaysia 10-12 July, 2003.

Sadasivuni, K. K., Panchal, H., Awasthi, A., Israr, M., Essa, F. A., Shanmugan, S., and Khechekhouche, A. (2020). Groundwater treatment using solar radiation-vaporization and condensation techniques by solar desalination system. *International Journal of Ambient Energy, 1*-7

Stewart, E. J. (2012). Growing unculturable bacteria. *Journal of Bacteriology, 194*(16), 4151-4160.

Wagen & Pieters. (2020). The hybrid victim: Reconceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology, 17*(4), 480-497.

Xue, B., Warkentin, M., Mutchler, L. A., & Balozian, P. (2021). Self-efficacy in Information Security: A Replication Study. *Journal of Computer Information Systems*. DOI: 10.1080/08874417.2021.2015725.