Fortifying Against Cyber Fraud: Instrument Development with the Protection Motivation Theory

Norhasyimatul Naquiah Ghazali, Syahida Hassan, Rahayu Ahmad
School of Computing, Universiti Utara Malaysia (UUM), Kedah, Malaysia

***Abstract*—Cybersecurity has become a trending topic in this technological era. Crimes keep happening in this medium and bring challenges for researchers and IT professionals worldwide to find the best solution to overcome this issue. Crimes primarily related to fraud on e-services have become a red alert that needs to be a concern for netizens. Instead of simply believing in the human-created network and system, individuals or users should acquire and implement protective behaviours for themselves. Thus, a few factors such as source credibility, perceived value of data, wishful thinking, perceived threat severity, perceived threat vulnerability, maladaptive rewards, and response efficacy have been investigated in this study, and the Protection Motivation Theory is used to counter cybersecurity issues faced by users. A tool has been created to facilitate the collection of empirical data necessary for verifying the proposed model. Analysis such as Content validity index (CVI) and Scale-level CVI (S-CVI) have been used to validate the item. The findings indicate that one of the items does not meet the criteria, however, it has been suggested by experts to revise and make it comprehensible to use for the main study. This paper also includes a discussion part regarding the implications of the experts' evaluation. This study, in particular, can help boost the understanding of cyber fraud and the proper methods, a user can employ to avoid becoming a victim.**

Keywords*—Cyber security; cyber fraud; e-services; instrument development; content validity; Protection Motivation Theory (PMT)

I. INTRODUCTION

Nowadays, people live in a networked culture where cyber technology has enabled cloud computing, online shopping, and other activities [1]. Despite the various advantages of technology in terms of commerce, communication, education, and entertainment, as noted by Bulgurcu et al. [2], it also presents some drawbacks. The unbridled expansion of digital technology has contributed to the correspondingly burgeoning problem of cyber fraud. This development is inextricably linked to intricate complications and perils that are engendered by the anonymous and rapid nature of the internet, which has been mentioned by Khalifa et al. [3] resulting in an ever-widening conundrum of cyber criminality. Annually, Kuru and Bayraktar [4] stated that cybercriminals devise novel tactics and techniques to deceive potential targets. People around the world are concerned about various issues due to cyber fraud [5], which also occurs in Malaysia. Although many countries have taken steps to make the cyber world more secure, Sorell and Whitty [6] agreed that there is still much work to be done to find a long-term solution to the security issues that plague cyberspace.

In the meantime, some consumers are unaware that they use e-services in their everyday lives. e-Services, which encompass all electronic services such as online bill-paying applications, government e-services, online banking, and online shopping [7] make it easier for users to conduct any online activity. Although the government of Malaysia has put in place various controls and safeguards to protect its citizens online, the rate at which cybercrimes are committed continues to rise in tandem. For instance, in 2022, there were 4,912 reported cases of the Macau Scam, also known as impersonation or fraud calls, which caused a loss of RM199.8 million, whereas e-commerce crimes accounted for 5,397 cases and a loss of RM71.6 million.

Furthermore, e-financial fraud or phishing has racked up as many as 543 cases, resulting in a loss of RM40.5 million [62]. Additionally, e-government, e-health, online shopping, and online banking have gradually changed into e-services which have been stated by Yesuf and Probst [8] throughout domains and industries as a means of optimising processes and facilitating engagement with both established and cutting-edge services of organisations. They also agreed [8] that the new systems and related services contain vulnerabilities that fraudsters might exploit to cause billions of dollars in losses to the global economy. In addition, [8] also mentioned the e-services platform developed for users' convenience has become insecure in recent years.

Fraud involving a cyber-aspect has shown a marked rising tendency, but traditional fraud has only declined a little. This pattern is expected to persist as more online transactions and banking are conducted. This tendency has made individuals fearful of online transactions, but not everyone takes action or realises the severity of the consequences when they become victims. According to a previous study by Button et al. [9], [10], being a victim of cyber fraud has negative consequences, such as psychological impact, financial losses, theft of intellectual property, invasion of privacy, and a loss of confidence and trust. Therefore, it is imperative to reduce the likelihood of becoming a target of fraudulent activities.

Next, Section II will provide a review of the relevant literature. Section III will discuss the methodology that has been employed, followed by Section IV, which presents the analysis and results. In Section V, the paper will deliberate on the research findings and acknowledge the study's constraints. Finally, Section VI will offer a conclusion, including recommendations for potential future research.

II. Related Work

A. Underpinnings Theory

According to previous studies, there has been some investigation into the association between individual safety and protection motivation behaviour. Such as Anderson and Agarwal [11] discussed factors of computer safety, Li et al. [12] investigate factors of cybersecurity behaviour, Belanger et al. [13] explore factors in information security, Boss et al. [14] examine factors that motivate protective security behaviour, Chen et al. [15] discuss online scams and protection behaviour, Haag et al. [16] discuss protection motivation in information and lastly, Martens et al. [17] comparing factors intention of taking security measure against cybercrime. Protective behaviour is crucial for combating cyber threats, as people frequently experience connectivity issues when establishing connections between their devices and internet-based systems. Furthermore, Liang and Xue [18] stated that it plays a vital role in ensuring the safety of those who use the internet via various electronic devices in their daily lives. Multiple theories, including the theory of planned behaviour (TPB), rational choice theory (RCT), general deterrence theory (GDT), technology threat avoidance theory (TTAT), routine activity (RAT), and protection motivation theory (PMT), have been employed by information security researchers. For instance, Fansher and Randa used (RAT) [19], Kirwan et al.,[20] also used RAT, Rogers and Prentice-Dunn used PMT [21], Chen and Liang used TTAT [22], Tan et al. [23] used TPB, and last but not least Martens et al. [17] also using PMT to explain the reasons behind people's protective behaviours and intentions. These hypotheses are grounded in various disciplines, including computer science, criminology, business, and psychology. The cybersecurity issue has also been addressed by integrating and adapting the system to the current environment.

However, despite all the theories, this study discusses PMT, one of the most commonly used to examine protection behaviour. For instance, Haag et al. [16] use PMT to investigate information security, Martens et al. [17] use PMT for comparing scams, malware and cybercrime in general, Mohammed et al. [24] use PMT to identify dimension of protection behaviour, Warketin et al. [25] use PMT to explore protective behaviour, Jansen and Schaik [26] use PMT to study on phishing, and last but not least De Kimpe et al. [27], use PMT in cybercrime context. As protection behaviour is crucial in the digital world nowadays, a problem may arise if one does not know how to protect oneself when connecting with this digital world. Few studies also contend that it is unclear regarding the decision-making process individuals undergo when determining whether or not to take measures to safeguard themselves against cybercrime [27], [28]. Meanwhile, another study by Warkentin et al. [25] stated that PMT also plays a vital role in developing communication techniques that encourage individuals to take precautions against cyber threats. Thus, it is necessary to investigate what factors influence individual intentions regarding protection behaviour.

B. PMT in Comparison with Past Studies

PMT consists of two appraisals, which are threat and coping. In PMT, threat appraisal was initially defined as a cognitive process by which an individual assesses a specific threat and the risk it poses [17]. It consists of two factors [17]: perceived severity and vulnerability. Perceived severity is the extent to which individuals perceive that the implications of a risk would be harmful, which increases their desire to take precautions [28]. Studies such as Dang-Pham and Pittayachawan [29], Losonczi [30], and Jansen et al. [31] have supported this statement.

Meanwhile, perceived vulnerability refers to the likelihood of being victimised by a particular threat. A previous study by Li et al. [32] found that users' ability to perceive the risk of a cyber-attack incident and identify effective preventive measures was insufficient, which subsequently affected their protective behaviour. This outcome holds notable significance. Another study by Thompson et al. [33] also had significant results where a user thought they were expected to have security risks and implied protection behaviours in their computing. Many studies such as Haag et al. [16], [24], [34] indicate that this construct plays an important role and is also one of the direct indicators that influence the motives for protection studies.

Besides, maladaptive rewards are also of crucial part of intention protection behaviour [35]. Maladaptive rewards mean users can save time or money by ignoring secure information management best practices [14], [21]. However, previous research such as Hassandoust et al. [35], Fisher-Prebler et al. [36], Chenoweth et al. [37] and Bax et al. [38] have not addressed how maladaptive rewards affect intention protection behaviours Furthermore, although PMT has been used to investigate several aspects of information security, researchers have focused on information security challenges in organisational contexts rather than specific ones. In addition, prior studies [18], [39] employing PMT to explore individuals' information security protective behaviours have yielded contradictory findings about the significance of the protection motivation mechanism. Therefore, this study aims to examine if maladaptive rewards affect the intended protection behaviour of e-services users.

As previously indicated, threat appraisal and maladaptive rewards have been discovered to influence protection. However, there is a lack of clarity on the antecedent elements that influence threat appraisal and maladaptive rewards. This issue has come to the attention of [16], who pointed out that most PMT research has concentrated on coping strategies and threat evaluation rather than antecedent variables. Additionally, as time progresses and technology keeps improving, it may become vital to investigate the antecedents to discover knowledge-enhancing insights. Therefore, this study proposes three antecedents for threat appraisal: (i) source credibility, (ii) perceived value of data, and (iii) wishful thinking, which will be explained next.

First, it is crucial to identify the origins of information since this can be an essential aspect of user protection and the initial step in determining the following action or behaviour. People are rationally more likely to defend themselves when

the source is unknown, and vice versa when the source's credibility can be verified. This study will investigate email source credibility in terms of where information comes from, as it has been recently highlighted as an unstudied issue in cybersecurity [16], [40].

Secondly, to analyse how they respond to a threat, it is necessary to comprehend their perception of data's value. Individuals possessing substantial wealth demonstrate a heightened awareness of security risks and are proactive in implementing preventive measures to mitigate such threats [41], [42]. Several past studies by [42], [43], have highlighted the perceived value of data from personal devices, which has a significant effect on intention protection. Considering that Western and Eastern societies have different levels of cultural and economic development, there is a pressing need for additional research in the context of Malaysia's growth.

Additionally, this study will investigate wishful thinking (WT) as an antecedent, which identifies beliefs as a factor that can influence maladaptive rewards. Wishful thinking is defined as an individual's "wish" that the IT threat would go away by itself without taking action [22], [44]. As a result, people become less concerned about information accuracy or objective probabilities [22]. For example, when users' wishful thinking is high, they will think that cyber threats do not severely impact them and will go away without action. As maladaptive rewards are about avoiding any safety or prevention measures to protect the individual from threats, this wishful thinking will significantly result in maladaptive rewards.

The previous paragraphs outlined the antecedents of threat appraisal and maladaptive rewards that will be investigated in this research. Alongside this, the appraisal of coping constructs will be examined. A coping appraisal is defined as the process by which an individual examines numerous protective techniques and avoids the threat [17]. Initially, PMT includes an individual's self-efficacy (the personal ability to implement a protection method), response efficacy (the effectiveness of approaches), and response cost (the concern about the potential expense associated with performing a recommended protective response) as the original constructs of the coping appraisal [16], [17], [26], [45]. These constructs influence a person's coping mechanisms towards cyber fraud. However, several studies have neglected to operationalize response costs due to their intricate and uncertain nature, as highlighted by [25], [46]. Moreover, current research indicates that self-efficacy has diminished explanatory power, resulting in a lack of significance and an inverse relationship [17], [29], [47], [48]. Therefore, this study only includes response efficacy as the coping appraisal.

III. METHODOLOGY

A. Instrument Development

The instrument is essential because it lets individuals know how well a study was done. If the criteria for the instrument are good, then the quality of the research is also good. If the criteria are flawed, then the quality of the research will be questionable. As the instrument turns fact into data, using a good one that is valid, reliable, and has a good level of difficulty will get data that reflects the facts or actual environments in the field [49]. However, a poor instrument will cause poor results in the study. In that case, the information gathered is also wrong or does not match the field's facts, leading to the wrong conclusion. Consequently, the development of instruments, as stated by Sekaran and Bougie [50] is an essential component of any research project and part of the research procedure.

This study aims to develop a data collection instrument that can be used to evaluate a proposed model and analyse the influence of relevant factors on the intention to protect behaviour. To create the instrument, the variables of the suggested model are operationalized within the context of the study. The instrument is used to gather empirical evidence to test the proposed framework as shown in Table I and Fig. 1.

TABLE I. DEFINITION OF CONSTRUCT

Construct	Definition	Source
Sources credibility	The information that a user receives from a person, authority, or source that they assume to be a reliable source of information	[38], [45]
Perceived value data	The emotional and monetary values of a user's data that are stored in e-services applications are referred to as perceived value data.	[29]
Wishful thinking	A person "wishes" that an information technology threat will disappear without requiring any action from him or her	[22], [44]
Perceived threat severity	The degree to which he or she recognises the presence of cyber fraud elements that represent a significant risk to him or her. The circumstance may prompt the user to take protective action.	[51], [52]
Perceived threat vulnerability	Relates to a user's perception of information security risks	[26]
Maladaptive Rewards	Refer to a circumstance in which a user feels he or she will receive additional benefits without adopting precautions.	[14], [29], [53]
Response efficacy	Relates to a user's reliance on the effectiveness of a cybersecurity suggestion	[54]
Intention protection behaviour	A term used to describe a user's instinct to protect themselves from an apparent danger	[14]

After that, the researchers extract the original measurements used in past literature across several different fields and turn them into items. Due to that, the reliability of the instrument can be established [55]. Nevertheless, to increase the validity of the instrument, content validity testing needs to be carried out by experts.

B. Content Validity

Content validity determines and assesses the degree to which the dimensions and components of a concept can be accurately and effectively defined [50]. An additional purpose of content validity is to ascertain the validity of each instrument item that corresponds to the measured construct [56]. Construct validity offers evidence or information to demonstrate that the items in a scale are interrelated and accurately measure the intended construct [49]. The greater the amount of content validity evidence gathered, including expert evaluation, the greater the researcher's confidence in

the constructed instruments' validity [57]. The panel of specialists can be classified into two groups, namely, professional experts and field experts [58].

Thus, before the process of determining the content validity of this study began, four expert panels were employed to evaluate the items and ensure the content validity of the instrument. A small discussion with four field experts regarding the item was conducted. This is to ensure the construct is well organised and the item represents the dimensions' possible measures. The clarity and relevance of the item have also been analysed. The four panels of professional university experts involved two senior lecturers and two associate professors.

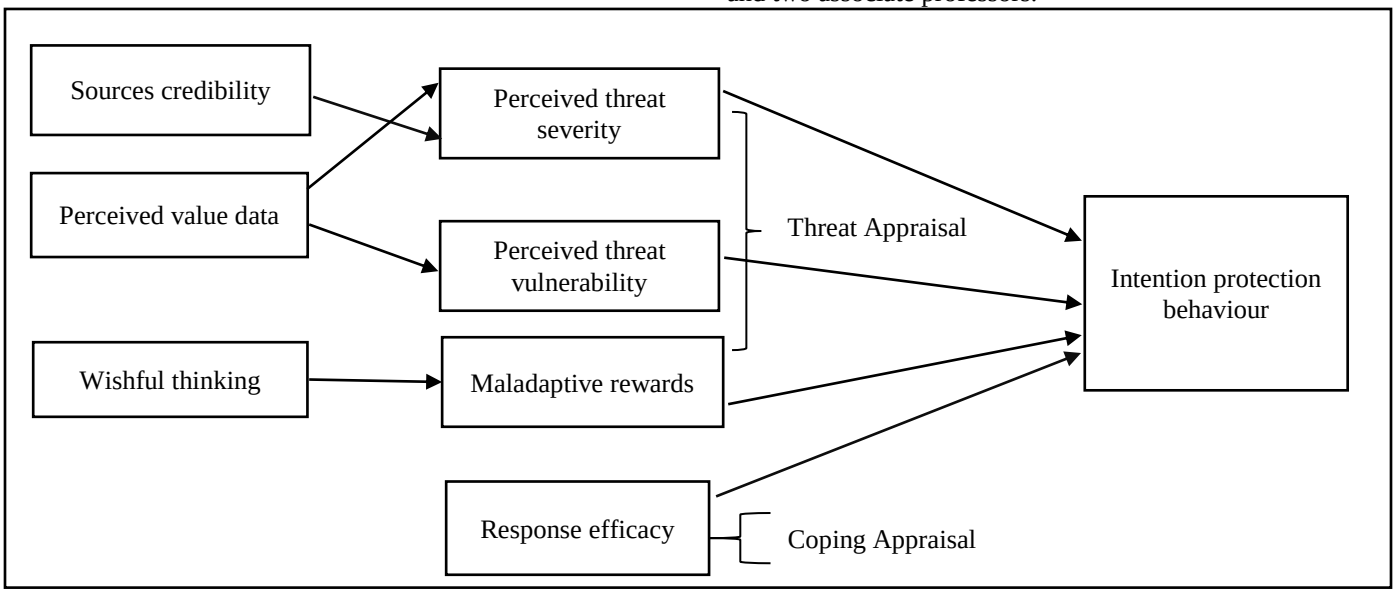

Fig. 1. This study aims to develop.

In order to make the evaluation of the content validity easier, a form was designed to allow the experts to evaluate the relevance and clarity of the measurements. The form was designed by assigning a number (1, 2, or 3); 1 means the item is a Poor Match (remove item), 2 means a Modest Match maintain item but needs some refining), and 3 means a Perfect Match (maintain the item as it is) so that the experts can evaluate the relevance and clarity of each item as shown in Table III.

IV. Analysis and Result

A. Validity Analysis

An analysis was conducted on the relevance and clarity assessments made by the experts for each item of the construct. CVI contains two components: Item-level CVI (I-CVI), which pertains to the content validity of individual items, and Scale-level CVI (S-CVI) evaluates the content validity of the entire scale [59]. The calculation of I-CVI involves dividing the number of experts who deemed the item relevant by the total number of experts who provided ratings. There are two techniques to calculate the S-CVI. One is known as S-CVI/UA and requires approval from all the experts. It is the proportion of elements on an instrument for which all experts acknowledge they are relevant. The other method is calculating the average I-CVI over all of the items, referred to as the S-CVI/Ave. The CVI for the current study instrument was determined, considering the relevance and clarity of each item. An overview of the CVI indices and a summary of the number agreement among experts may be found in Table II.

TABLE II. Content Validity of Individual Items (I-CVI)

Construct	Item No.	Summarize of No. Agreement		I-CVI	
		R	C	R	C
Source credibility	1	3	3	1	1
	2	2	2	0.5	0.5
	3	3	3	1	1
Perceived value data	1	3	3	1	1
	2	3	3	1	1
	3	3	3	1	1
Wishful thinking	1	3	3	1	1
	2	3	3	1	1
	3	3	3	1	1
Perceived threat severity	1	3	3	1	1
	2	3	3	1	1
	3	3	3	1	1
	4	3	3	1	1
Perceived threat vulnerability	1	3	3	1	1
	2	3	3	1	1
	3	3	3	1	1
Maladaptive rewards	1	3	3	1	1
	2	3	3	1	1
	3	3	3	1	1

	4	3	3	1	1
	5	3	3	1	1
Response efficacy	1	3	3	1	1
	2	3	3	1	1
	3	3	3	1	1
Intention protection motivation	1	3	3	1	1
	2	3	3	1	1
	3	3	3	1	1
	4	3	3	1	1
	5	3	3	1	1
R= Relevance C=Clarity					

The results demonstrate that the I-CVI for one question does not meet the criteria for item acceptability recommended by [59], [60], which states that it must be 1 for 3-5 experts to be considered acceptable. This pertains to the relevance of the items. According to the S-CVI figures, SCVI/UA and S-CVI/Ave are 0.97 and 0.98, respectively (see Table III). The lowest value of acceptability for S-CVI as determined by [61] is 0.80, and these results are significantly higher than that limit.

Besides that, the results of calculating the I-CVI for the clarity of the items suggest that one of the items is not clear enough (0.5) (see Table II). The experts gave their feedback to help make the items more comprehensible. In addition, the S-CVI/UA and S-CVI/Ave ratios for the items' clarity reveal satisfactory levels with corresponding values of 0.97 and 0.98. (See Table III).

TABLE III. SCALE-LEVEL CONTENT VALIDITY INDEX (S-CVI)

	Relevance	**Clarity**
S-CVI/Ave	0.98	0.98
Total agreement	28/29	28/29
S-CVI/UA	0.97	0.97

Hence, the instrument was amended in line with the expert's feedback. Table IV indicates the updated scale measurements.

TABLE IV. UPDATED MEASUREMENTS

Constructs	Original	Revised
Source credibility	I believe emails from the Malaysian government domain (.gov) are credible.	I believe emails from all e-Services domains (.gov.my; .edu.my; .com.my) are credible.
	I believe emails from the Malaysian government domain (.gov) tend to be free from grammatical errors.	I believe emails from all e-Services domains (.gov.my; .edu.my; .com.my) tend to be free from grammatical errors.
	I believe emails from the Malaysian government domain (.gov) tend to have a sense of urgency.	I believe emails from all e-Services domains (.gov.my; .edu.my; .com.my) tend to have a sense of urgency.
Perceived value data	I perceive the importance of regarding the security protection of my data in e-services.	I perceived the importance of security protection towards my data in e-Services
	I am aware of the potential risk of monetary loss if there are breaches of my personal data**.**	I am aware of the potential risk of monetary loss if there are breaches of my personal data.
	I perceived the e-services highly guarantee the confidentiality of my personal data.	I perceived the e-services could fully guarantee the confidentiality of my personal data
Wishful thinking	I wish I could use e-services without increasing my security protection.	I wish I could use e-Services without increasing my security protection.
	I wish that the threat would go away or somehow not affect me.	I wish that the threat would go away by itself.
		I wish that the threat would not affect me.
	I hope I will not encounter any cyber threat situations.	I hope I will not encounter any cyber threat situations.
Perceived threat severity	I believe that being a victim of cyber fraud in e-services is a serious problem for me.	I believe that being a victim of cyber fraud in e-services is a serious problem for me.
	I believe that the time/masa loss to recover the damages (e.g., money loss, data loss) after being a victim of cyber fraud is a serious problem.	I believe that the time lost to recover the damages after being a victim of cyber fraud is a serious problem.
	I believe that my productivity/effort loss to recover the damages (e.g., loss of income) from being a victim of cyber fraud is a serious problem.	I believe that my productivity/effort loss (e.g., loss of income) to recover the damages from being a victim of cyber fraud is a serious problem.
	I believe that the data/information loss from being a victim of cyber fraud is a serious problem.	I believe that the data/information loss from being a victim of cyber fraud is a serious problem.
Perceived threat vulnerability	I am exposed to the cyber fraud threats of e-services.	I am exposed to the cyber fraud threats of e-Services.
	I am at risk of being victimised by cyber fraud attackers.	I am at risk of being victimized by cyber fraud attacker
	I will likely become a victim of cyber fraud.	I can become a victim of cyber fraud
Maladaptive rewards	I can save my time if I'm not using any preventive countermeasures application (e.g.: antivirus, anti-malware).	I can save my time if I am not using any preventive countermeasures application (e.g.: antivirus, anti-malware).
	I can save my money if I'm not using any preventive countermeasure applications.	I can save my money if I am not using any preventive countermeasure applications.
	I will be better informed of the security risk if I'm using	I think it is a waste of effort to spend more money on

	any preventive countermeasure applications.	anti-virus software to increase the protection against cyber fraud
	I will spend less effort if I do not perform the recommendations of the preventive countermeasure applications.	I will spend less effort if I do not perform the recommendations of the preventive countermeasure applications.
	I will feel less stressful if I do not perform the recommendations of the preventive countermeasure applications.	I will feel less stressful if I do not perform the recommendations of the preventive countermeasure applications.
Response efficacy	When using a preventive countermeasures application, a computer's data is more likely to be protected.	When using preventive countermeasures applications, computer data is more likely to be protected.
	Performing any cybersecurity recommendations would reduce the chance of myself from becoming a cyber fraud victim.	Performing any cybersecurity recommendation would reduce the chance of me from becoming a cyber fraud victim.
	Performing any of the provided recommendations make me feel safe from cyber fraud attack.	Performing any of the provided recommendations makes me feel safe from a cyber fraud attack
Intention protection Motivation	I will update my knowledge to use e-services safely.	I will update my knowledge to use e-Services safely.
	I will likely engage in activities that protect my personal information from cyber fraud when I use e-services.	I will likely engage in activities that protect my personal information from cyber fraud when I use e-services.
	I intend to protect myself from cyber fraud when I use e-services.	I intend to protect myself from cyber fraud when I use e-Services.
	I am willing to spend more in order to protect myself from cyber fraud when I use e-services.	I am willing to spend more money in order to protect myself from cyber fraud when I use e-Services
	I will likely take precaution that protects my personal information from cyber fraud when I use e-services.	I will likely take precaution that protects my personal information from cyber fraud when I use e-Services.

V. DISCUSSION

Using the PMT point of view, through this instrument development, this study aims to investigate the factors of human behaviour that can lead to the intention to protect oneself from becoming a victim of cyber fraud while participating in online activities. In the first part of this research study, an investigation into the influence of threat appraisal on the intention protection behaviour of the user when utilising e-services will be carried out. In addition, maladaptive rewards will also be investigated, [14], [16], [37], [38] as there have been numerous debates over this issue in past studies.

Practically, the results of this study will be beneficial to individuals in the sense that they will gain an understanding of the kinds of factors that can make them susceptible to fraudsters and the kinds of responses they should make when confronted with a situation in which they are at risk of being victims of cyber fraud. Before becoming the next victim of cyber fraud, consumers must recognise how their habits can either help or threaten them. With these characteristics, enhanced protection can be created, preventing consumers from falling prey to fraudsters. In addition, these studies will have made significant contributions to the development of PMT-based information security research. It will investigate new antecedent factors incorporated into PMT as new components.

In addition, this research creates a tool for measuring the model's constructs. The items for each construct were drawn from relevant theories and literature and then revised to reflect the topic of the study. The validity of the measurement may be compromised by adapting the original items to the context of the study. Therefore, content validation was done to verify that the items adequately reflected the subject domain. Initial evidence of construct validity is provided by content validity. In addition, it gives indicators of the items' representativeness and clarity and contributes to the enhancement of the instrument by considering the suggestions of experts [62].

In the current study, four experts evaluated the items' relevance and clarity. The results indicated that 28 items were accepted, except one item was not considerably clear (in terms of wording); hence, the item was graded as "keep it but refine it to the corresponding construct". These elements were updated in response to the feedback of the experts. All item and construct comments were considered in the amended version of the instrument. These components were extracted from the relevant literature, considering the cyber fraud environment's setting.

Lastly, despite the careful expert selection, the study can be enhanced by involving a more diverse range of experts for additional insights and improvements.

VI. CONCLUSION

To summarise, the findings of this study can provide a new instrument construct base for future studies. All 29 items will be subjected to a pilot testing phase by administering the questionnaire to the designated participants. Subsequently, this pilot study will entail subjecting the items to further rigorous statistical analyses aimed at substantiating their reliability and validity for inclusion in the primary research investigation.

Academically, this study would benefit the body of knowledge, including institutions, colleges, and universities, because it can provide new knowledge for academics who intend to publish it in an open-access journal or send it to a publisher. The entire variable will be examined, and the results might be used to increase the output of research on this subject in Malaysia, specifically for academic institutions. In addition, it enables academicians to create substantial countermeasures against cyber fraud in Malaysia.

Besides that, in order to enhance the explanatory capacity of the model, it may be expedient to incorporate supplementary variables to expand the framework. This could involve broadening the scope of constructs beyond those pertaining to source credibility, maladaptive rewards, wishful thinking, perceived vulnerability, perceived severity, and

response efficacy. Lastly, a greater understanding of this kind of behaviour will aid professionals in designing, developing, and executing new methods or enhancements for e-service users. This study was conducted in support of a government aiming to develop and maintain a safer cyberspace to achieve national sustainability, social well-being, and wealth creation. Perhaps this research will aid in reducing the losses incurred by the government as a consequence of cyber fraud.

ACKNOWLEDGMENT

This research was supported by Ministry of Higher Education (MoHE) of Malaysia through The Fundamental Research Grant Scheme for Research Acculturation of Early Career Researchers (RACER/1/2019/ICT04/UUM//2)

REFERENCES

[1] Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," Procedia Economics and Finance, vol. 28, no. January, pp. 24–31, 2015, doi: 10.1016/s2212-5671(15)01077-1.

[2] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," MIS Quarterly, vol. 34, no. 3, pp. 523–548, Sep. 2010, doi: 10.2307/25750690.

[3] N. H. S. Khalifa Sultan Khalifa Humaid; Al-kumaim, "A conceptual model for prevention of e-financial crimes in UAE: a review paper," Academic of Strategic Management Journal, vol. 20, no. Special Issue 6, pp. 1–11, 2021.

[4] D. Kuru and S. Bayraktar, "The effect of cyber-risk insurance to social welfare," J Financ Crime, vol. 24, no. 2, pp. 329–346, 2017, doi: 10.1108/JFC-05-2016-0035/FULL/PDF.

[5] S. Ye and K. K. W. Ho, "Would you feel happier if you have more protection behaviour? A panel survey of university students in Japan," Behaviour and Information Technology, vol. 38, no. 4, pp. 422–434, 2019, doi: 10.1080/0144929X.2018.1544275.

[6] T. Sorell and M. Whitty, "Online romance scams and victimhood," Security Journal, no. 0123456789, 2019, doi: 10.1057/s41284-019-00166-w.

[7] T. Kvasnicova, I. Kremenova, J. Fabus, and B. Babusiak, "E-commerce user experience: Do we feel under pressure during online shopping?," in WMSCI 2016 - 20th World Multi-Conference on Systemics, Cybernetics and Informatics, Proceedings, 2016.

[8] A. S. Yesuf and C. W. Probst, "Estimating the Risk of Fraud Against E-Services," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018. doi: 10.1007/978-3-030-03638-6_19.

[9] M. Button, C. M. N. Nicholls, J. Kerr, and R. Owen, "Online frauds: Learning from victims why they fall for these scams," Australian and New Zealand Journal of Criminology, vol. 47, no. 3, pp. 391–408, 2014, doi: 10.1177/0004865814521224.

[10] D. H. Shih, B. Lin, H. Sen Chiang, and M. H. Shih, "Security aspects of mobile phone virus: A critical survey," Industrial Management and Data Systems, vol. 108, no. 4, pp. 478–494, 2008, doi: 10.1108/02635570810868344/FULL/PDF.

[11] C. L. Anderson and R. Agarwal, "Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions," MIS Q, 2010, doi: 10.2307/25750694.

[12] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," Int J Inf Manage, vol. 45, pp. 13–24, Apr. 2019, doi: 10.1016/j.ijinfomgt.2018.10.017.

[13] R. Crossler and F. Bélanger, "An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument," Data Base for Advances in Information Systems, 2014, doi: 10.1145/2691517.2691521.

[14] S. R. Boss, D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak, "What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors," MIS Q, 2015, doi: 10.25300/MISQ/2015/39.4.5.

[15] H. Chen, C. E. Beaudoin, and T. Hong, "Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors," Comput Human Behav, 2017, doi: 10.1016/j.chb.2017.01.003.

[16] S. Haag, M. Siponen, and F. Liu, "Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future," Data Base for Advances in Information Systems, vol. 52, no. 2, pp. 25–67, May 2021, doi: 10.1145/3462766.3462770.

[17] M. Martens, R. De Wolf, and L. De Marez, "Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general," Comput Human Behav, vol. 92, no. May 2018, pp. 139–150, 2019, doi: 10.1016/j.chb.2018.11.002.

[18] H. Liang and Y. Xue, "Understanding security behaviors in personal computer usage: A threat avoidance perspective," J Assoc Inf Syst, 2010, doi: 10.17705/1jais.00232.

[19] A. K. Fansher and R. Randa, "Risky Social Media Behaviors and the Potential for Victimization: A Descriptive Look at College Students Victimized by Someone Met Online," Violence Gend, vol. 6, no. 2, pp. 115–123, 2019, doi: 10.1089/vio.2017.0073.

[20] G. H. Kirwan, C. Fullwood, and B. Rooney, "Risk Factors for Social Networking Site Scam Victimization among Malaysian Students," Cyberpsychol Behav Soc Netw, vol. 21, no. 2, pp. 123–128, 2018, doi: 10.1089/cyber.2016.0714.

[21] R. W. Rogers and S. Prentice-Dunn, "Protection Motivation Theory," in Handbook of health behavior research 1: Personal and social determinants, 1997, pp. 113–132. doi: 10.4135/9781483332222.n225.

[22] D. Q. Chen and H. Liang, "Wishful Thinking and IT Threat Avoidance: An Extension to the Technology Threat Avoidance Theory," IEEE Trans Eng Manag, 2019, doi: 10.1109/TEM.2018.2835461.

[23] K.-L. Tan, Y. Liu, and Q. Ye, "A gendered discourse on truthful disclosure of financial fraud practices among accountants in China: implications to corporate governance," Accounting Research Journal, vol. 36, no. 2/3, pp. 230–250, Jan. 2023, doi: 10.1108/ARJ-07-2022-0160.

[24] I. Mohammed Al-harthy, F. Abdul Rahim, A. Ali, and A. P. Singun Jr, "Dimensions of protection behaviors: A systematic literature review," J Theor Appl Inf Technol, vol. 15, p. 17, 2020, [Online]. Available: www.jatit.org

[25] M. Warkentin, A. C. Johnston, J. Shropshire, and W. D. Barnett, "Continuance of protective security behavior: A longitudinal study," Decis Support Syst, vol. 92, no. May 2018, pp. 25–35, 2016, doi: 10.1016/j.dss.2016.09.013.

[26] J. Jansen and P. van Schaik, "Persuading end users to act cautiously online: a fear appeals study on phishing," Information and Computer Security, vol. 26, no. 3, pp. 264–276, 2018, doi: 10.1108/ICS-03-2018-0038.

[27] L. De Kimpe, M. Walrave, P. Verdegem, and K. Ponnet, "What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context," Behaviour and Information Technology, vol. 0, no. 0, pp. 1–13, 2021, doi: 10.1080/0144929X.2021.1905066.

[28] B. W. Reyns, R. Randa, and B. Henson, "Preventing crime online: Identifying determinants of online preventive behaviors using structural equation modeling and canonical correlation analysis," Crime Prevention and Community Safety, vol. 18, no. 1, pp. 38–59, 2016, doi: 10.1057/cpcs.2015.21.

[29] D. Dang-Pham and S. Pittayachawan, "Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach," Comput Secur, vol. 48, pp. 281–297, 2015, doi: 10.1016/j.cose.2014.11.002.

[30] P. Lošonczi, "Importance of Dealing with Cybersecurity Challenges and Cybercrime in the Senior Population," Security Dimensions, vol. 26, no. 26, pp. 173–186, 2018, doi: 10.5604/01.3001.0012.7249.

[31] J. Jansen and P. van Schaik, "The design and evaluation of a theory-based intervention to promote security behaviour against phishing," Int J

Hum Comput Stud, vol. 123, pp. 40–55, Mar. 2019, doi: 10.1016/j.ijhcs.2018.10.004.

[32] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," Int J Inf Manage, vol. 45, pp. 13–24, 2019, doi: 10.1016/j.ijinfomgt.2018.10.017.

[33] N. Thompson, T. J. McGill, and X. Wang, "'Security begins at home': Determinants of home computer and mobile device security behavior," Comput Secur, 2017, doi: 10.1016/j.cose.2017.07.003.

[34] M. Grimes and J. Marquardson, "Quality matters: Evoking subjective norms and coping appraisals by system design to increase security intentions," Decis Support Syst, vol. 119, no. February, pp. 23–34, 2019, doi: 10.1016/j.dss.2019.02.010.

[35] F. Hassandoust and A. A. Techatassanasoontorn, "Understanding users' information security awareness and intentions: A full nomology of protection motivation theory," Proceedings of the 22nd Pacific Asia Conference on Information Systems - Opportunities and Challenges for the Digitized Society: Are We Ready?, PACIS 2018, 2018.

[36] D. Fischer-Preßler, D. Bonaretti, and K. Fischbach, "A Protection-Motivation Perspective to Explain Intention to Use and Continue to Use Mobile Warning Systems," Business and Information Systems Engineering, vol. 64, no. 2, pp. 167–182, Apr. 2022, doi: 10.1007/S12599-021-00704-0/TABLES/3.

[37] T. Chenoweth, T. Gattiker, and K. Corral, "Adaptive and Maladaptive Coping with an It Threat," https://doi.org/10.1080/10580530.2018.1553647, vol. 36, no. 1, pp. 24–39, Jan. 2019, doi: 10.1080/10580530.2018.1553647.

[38] S. Bax, T. McGill, and V. Hobbs, "Maladaptive behaviour in response to email phishing threats: The roles of rewards and response costs," Comput Secur, vol. 106, p. 102278, 2021, doi: 10.1016/j.cose.2021.102278.

[39] B. Hanus and Y. "Andy" Wu, "Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective," Information Systems Management, 2016, doi: 10.1080/10580530.2015.1117842.

[40] A. Appelman and S. S. Sundar, "Measuring Message Credibility: Construction and Validation of an Exclusive Scale," http://dx.doi.org/10.1177/1077699015606057, vol. 93, no. 1, pp. 59–79, Oct. 2015, doi: 10.1177/1077699015606057.

[41] S. Chai, S. Bagchi-Sen, C. Morrell, H. R. Rao, and S. J. Upadhyaya, "Internet and online information privacy: An exploratory study of preteens and early teens," IEEE Trans Prof Commun, 2009, doi: 10.1109/TPC.2009.2017985.

[42] S. Srisawang, M. Thongmak, and A. Ngarmyarn, "Factors affecting computer crime protection behavior," in Pacific Asia Conference on Information Systems, PACIS 2015 - Proceedings, 2015.

[43] I. Mahmud, T. Ramayah, Md. M. H. Nayeem, S. M. M. M. Islam, and P. L. Gan, "Modelling Cyber-Crime Protection Behaviour among Computer Users in the Context of Bangladesh," in Design Solutions for User-Centric Information Systems, 2016. doi: 10.4018/978-1-7998-2466-4.ch021.

[44] S. Folkman, R. S. Lazarus, C. Dunkel-Schetter, A. DeLongis, and R. J. Gruen, "Dynamics of a Stressful Encounter. Cognitive Appraisal, Coping, and Encounter Outcomes," J Pers Soc Psychol, 1986, doi: 10.1037/0022-3514.50.5.992.

[45] S. Milne, S. Orbell, and P. Sheeran, "Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions," Br J Health Psychol, 2002, doi: 10.1348/135910702169420.

[46] M. O. Lwin, B. Li, and R. P. Ang, "Stop bugging me: An examination of adolescents' protection," J Adolesc, 2012.

[47] P. Menard, G. J. Bott, and R. E. Crossler, "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory," Journal of Management Information Systems, vol. 34, no. 4, pp. 1203–1230, 2017, doi: 10.1080/07421222.2017.1394083.

[48] H. Y. S. Tsai, M. Jiang, S. Alhabash, R. Larose, N. J. Rifon, and S. R. Cotten, "Understanding online safety behaviors: A protection motivation theory perspective," Comput Secur, vol. 59, pp. 138–150, 2016, doi: 10.1016/j.cose.2016.02.009.

[49] N. Ghazali, M. S. Nordin, and T. B. Tunku Ahmad, "Development and Validation of Student's MOOC-efficacy Scale: Exploratory Factor Analysis," Asian Journal of University Education; Vol 17 No 4 (2021): AJUE Vol 17 No 4 October 2021DO - 10.24191/ajue.v17i4.16182 , Nov. 2021.

[50] U. Sekaran and R. Bougie, "Research Methods for Business 6th United Kingdom," 2014.

[51] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," J Exp Soc Psychol, 1983, doi: 10.1016/0022-1031(83)90023-9.

[52] K. Witte, "Putting the fear back into fear appeals: The extended parallel process model," Commun Monogr, vol. 59, no. 4, pp. 329–349, 1992, doi: 10.1080/03637759209376276.

[53] D. L. Floyd, S. Prentice-DFloyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. Journal of Applied Social Psychology. https://doi.org/10.1111/j.1559-1816.2000.tb02323.xunn, and R. W. Rogers, "A meta-analysis of research on protection motivation theory," J Appl Soc Psychol, 2000, doi: 10.1111/j.1559-1816.2000.tb02323.x.

[54] J. Ophoff and M. Lakay, "Mitigating the Ransomware Threat: A Protection Motivation Theory Approach," in Communications in Computer and Information Science, 2019. doi: 10.1007/978-3-030-11407-7_12.

[55] N. K. Agarwal, "Verifying survey items for Construct Validity: A two-stage Sorting Procedure for Questionnaire Design in Information Behavior Research," 2011. doi: https://asistdl.onlinelibrary.wiley.com/doi/full/10.1002/meet.14504801166.

[56] L. A. Miller, R. L. Lovler, and S. A. McIntire, "Foundations of psychological testing : a practical approach," p. 624, 2013.

[57] Burke. Johnson and L. B. Christensen, "Educational research : quantitative, qualitative, and mixed approaches," p. 621, 2012.

[58] D. M. G. Rubio, M. Berg-Weger, S. S. Tebb, E. S. Lee, and S. Rauch, "Objectifying content validity: Conducting a content validity study in social work research," Soc Work Res, vol. 27, no. 2, pp. 94–104, Jun. 2003, doi: 10.1093/SWR/27.2.94.

[59] M. R. Lynn, "Determination and quantification of content validity," Nurs Res, vol. 35, no. 6, pp. 382–386, 1986, doi: 10.1097/00006199-198611000-00017.

[60] D. F. Polit, C. T. Beck, and S. V. Owen, "Is the CVI an acceptable indicator of content validity? Appraisal and recommendations," Res Nurs Health, vol. 30, no. 4, pp. 459–467, Aug. 2007, doi: 10.1002/NUR.20199.

[61] L. L. Davis, "Instrument review: Getting the most from a panel of experts," Applied Nursing Research, vol. 5, no. 4, pp. 194–197, Nov. 1992, doi: 10.1016/S0897-1897(05)80008-4.

[62] M. Saiful and B. Yusoff, "ABC of content validation and content validity index calculation," Malaysian Association of Education in Medicine and Health Sciences, vol. 11, no. 2, pp. 49–54, 2019, doi: 10.21315/eimj2019.11.2.6.