JSCDM

JOURNAL OF SOFT COMPUTING AND DATA MINING
e-ISSN: 2716-621X

Vol. 7 No. 3 (2026) 83-93
https://publisher.uthm.edu.my/ojs/index.php/jscdm

Integrating Communication Constructs into Protection Motivation Theory: Modeling the Impact of Fraud Awareness Campaigns

Akhyari Nasir[1]*, Shah Shafie Idris[1], Noor Suhana Sulaiman[1], Nor Shahida Mohd Jamail[2]

[1] *Faculty Computer, Media & Technology Management, University College TATI, Terengganu, MALAYSIA*
[2] *College of Computer and Information Sciences, Prince Sultan University, Riyadh, SAUDI ARABIA*

Author's e-mail
1st Author: akhyari@uctati.edu.my (*Corresponding Author)
2nd Author: shah@uctati.edu.my
3rd Author: suhana@uctati.edu.my
4th Author: njamail@psu.edu.sa

DOI: https://doi.org/10.30880/jscdm.2026.07.03.007

Article Info

Received: 25 November 2025
Accepted: 19 October 2026
Available online: 1 November 2026

Keywords

Fraud, scam, PMT, campaign

Abstract

Fraud and online scams have evolved to become an important global issue, resulting in billions of losses every year and eroding people's trust in the online systems. Governments around the world including Malaysia have tried to solve this problem through conducting major fraud awareness campaigns. But traditional theories have failed to provide insight into the process through which such campaigns arouse protective motivation in individuals. This research is aimed at filling this gap in the literature by expanding the Protection Motivation Theory (PMT) with the constructs related to communication. In particular, this research proposes that exposure to a campaign, understanding of the message, and message credibility be included in the PMT as the antecedent variables of threat appraisal leading to severity perception and vulnerability perception, and eventually, protective intention towards fraud. Thus, by linking PMT with the communication theory, this research develops the theoretical framework on the cognitive processes of arousal stimulated by fraud awareness campaigns. The importance of the present study is in expanding the PMT with the constructs related to communication in order to provide insight into how awareness campaigns about fraud work and what their effectiveness in terms of protecting people from scams depends on.

This is an open access article under the CC BY-NC-SA 4.0 license.

1. Introduction

In spite of the various measures that have been put in place by the government and other institutions, there has been an increase in the number of financial scams and cyber frauds that occur both in Malaysia and in the world at large. Various organizations, including CyberSecurity Malaysia (CSM), Bank Negara Malaysia, and Royal Malaysia Police (PDRM), have taken various preventive measures against these scams in Malaysia. Such measures include public awareness programs, SMS alerts, and regulation enforcement measures. Despite all the efforts, financial scams such as phishing, investment frauds, and impersonations continue to exist in the country. These scams cost Malaysia tens of millions of ringgits every year [1]. The existence of these security threats implies that the current measures might not have any impact on changing user behavior and that there is the need to identify the psychological factors that make people susceptible to such attacks. There has been a significant amount of literature on scam and fraud victimization from the perspectives of criminology, economics, and cybersecurity. Though these methods have provided valuable insights into the matter, many of them have been incapable of explaining how people behave in order to resist scammers. Behavioral theory has received more and more attention recently as researchers try to explain what motivates people to protect themselves and what makes other people fail to do so [2]– [4].

Protection Motivation Theory (PMT), among other behavioral models, has become one of the most frequently used theories in explaining user behavior in relation to threat. PMT theory suggests that a person evaluates two main factors in regards to threats – first, the nature of the threat, which includes perceived severity, vulnerability, and rewards; second, the ability of an individual to respond to the threat, including such variables as self-efficacy, response efficacy and perceived response cost [5], [6]. These variables are integrated in an individual's motivational decision to engage in protective behavior. PMT theory has proven to be effective in explaining various behaviors, including health behavior, information security, phishing prevention and social engineering [7]–[9]. In all these cases, PMT constructs showed significant correlation with both behavioral intention and behavior itself. While the effectiveness of PMT has been proven in different fields, the use of PMT in scam and fraud prevention and especially in evaluating government communications on this matter has been insufficiently explored. The existing literature tends to explore single predictors in isolation from a general theory while only limited number of researches conducted in Malaysia have investigated the relationships between psychological constructs and scam avoidance behavior in the context of public campaign. This problem is especially important since behavioral intention is influenced not only by cognitive but also situational variables, including message framing, source credibility and warnings frequency.

Having in mind the above-mentioned drawbacks, it becomes evident that it is necessary to design a conceptual model that will be able to combine the structure of cognition within PMT with environmental and communicative factors considered in previous research. That means that a model should not consider just the processes of internal assessment that result in the adoption of preventive behavior but also the ecosystem where these processes take place. This paper adds to the PMT by adding three communication variables into the concept of threat assessment – they are campaign exposure, message comprehension, and message credibility. This work creates the theoretical framework that provides an explanation of how the government-led fraud prevention campaign triggers the perceptions of perceived severity and vulnerability, which, in their turn, form protective behavioral intentions. By using the Malaysian context, the research makes a contribution both at the theoretical and practical levels, namely, it advances the PMT framework in the area of fraud prevention and contributes to the knowledge of how the design of anti-scam campaigns can help people become more resistant to scams. The following section provides the review of the relevant literature on fraud prevention campaigns, behavioral theories, and PMT applications. It is followed by the section that offers the theoretical framework and the development of the model of how the campaign concepts are added into the threat assessment stage. After that, the proposed hypotheses based on the above-mentioned theoretical framework are described.

2. Literature Review

The rise in financial scams in Malaysia in recent times has been quite alarming. In the State of Scam Report 2024, there are reports indicating consumer losses totaling approximately RM53 billion which translates to 3% of the country's GDP [10]. This is due to various types of scam methods, which include phishing, investment scams, identity theft, and impersonation. In addition, it was noted that over 70% of Malaysians face attempts to scam them every month although few do report this. This indicates weaknesses in digital habits and lack of confidence among consumers in law enforcement. With the increase in underreporting and sophistication in the methods of scammers, it is evident that there is the need for research to be done not only on the technical side but also on behavioral and psychological aspect of scam susceptibility.

Malaysian authorities and financial organizations have increased efforts in educating the public about these scams. In the collaborative effort of the national #JanganKenaScam campaign, which involves the Association of Banks in Malaysia (ABM), Bank Negara Malaysia and Royal Malaysia Police, various strategies have been adopted which includes SMS alert, television commercials, social media content, and booth awareness [11]. In an impact

J. of Soft Computing and Data Mining Vol. 7 No. 3 (2026) p. 83-93

study conducted by these organizations, it was found that over 80% of the respondents were aware of the key messages of the campaign with many of them stating that they had confidence that they could protect themselves from scams [12]. However, these impact studies only capture information on awareness and attitudes and not behavior. Many respondents, over two thirds of them stated that they were not prepared to deal with scams.

The growing body of scholarship has seen scholars looking towards behavioral science for insights into this phenomenon. Models like the PMT allow us to systematically analyze how people create intentions to avoid threats. According to the PMT theory, people's intentions to engage in protective behavior are shaped by threat appraisals (i.e., perceived severity, vulnerability, and rewards) and coping appraisals (self-efficacy, response efficacy, and response cost) [7], [13]. The PMT model has proven effective and consistent in the field of health psychology and cybersecurity. [14] found the constructs of the PMT to predict the level of online safety behavior among internet users. Similarly, [15] identified the PMT model as one of the most common and influential in information systems security research.

Even though the PMT model has shown significant potential in predicting behavior, recent research suggests that the predictive power of the model can be enhanced through the use of communication-based variables. [16] showed that the effect of security awareness messages is significantly affected by the extent to which people understand and trust the message source. Likewise, [3] developed a PMT model that included message comprehension and credibility and concluded that these factors were critical for translating risk perceptions into behavioral intention. Similarly, qualitative research in Malaysia based on the KAP model has found that the lack of clarity and credibility of the campaign messages hinders their impact on protective behavior. It is important to acknowledge the idea that the design of campaigns and the elements like exposure frequency, clarity, and source credibility must be included in theoretical modeling. Thus, we can see that campaign design significantly affects how people respond to scam-related threats.

All of these trends point to the necessity of a more integrative model of protective behavior against scams. Current scholarship shows that behavioral theories, in particular, PMT, offer a powerful basis for the analysis of individual motivation. However, these models have to be updated to account for the realistic conditions under which people receive, perceive and react to campaign messages. The next section discusses theoretical framework and model development in the light of PMT and related communication constructs.

3. Methodology and Model Development

The methodology involved the development of a conceptual framework that illustrates the role played by awareness programs on the part of the government on behavioral intentions towards protection. Fig. 1 illustrates the complete methodology framework that shows the step-by-step process from the development of the theoretical foundation to the development of the research framework. The process, which is outlined in Fig. 2, followed an orderly approach involving the development of the theoretical foundation, incorporation of campaign elements, hypothesis development, and formulation of the final model.

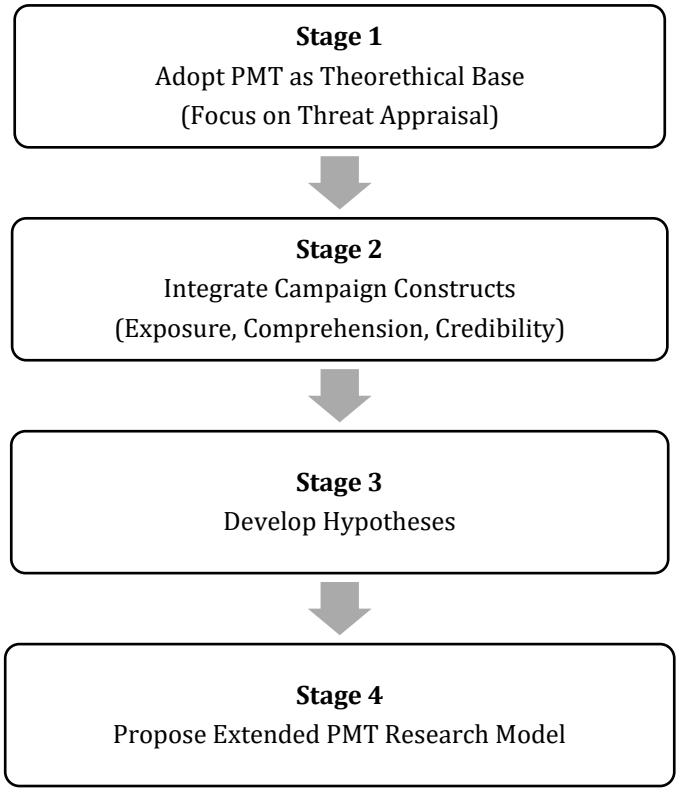


Fig. 1 *Overall methodological flow*

The first step was using PMT. PMT has been used widely to explain protective behaviors in health, cybersecurity, and risk communication. Using PMT's dual channels – threat appraisal and coping appraisal – enables a thorough examination of protective intentions. Considering that the subject of the current study is the government's awareness campaigns, the threat appraisal channel including perceived severity and perceived vulnerability, but not coping appraisal variables like self-efficacy and response efficacy was retained.

The second step was extending PMT by adding three campaign-related constructs into the theory. Specifically, campaign exposure, message comprehension, and message credibility are introduced as exogenous communication variables that trigger the threat appraisal channel. This approach is justified considering that, according to communication theories, the exposure, comprehension, and credibility of messages play an essential role in risk perception and protective motivation formation.

The third step consisted of developing hypotheses concerning relationships between campaign constructs, threat appraisal, and protective behavior intention. It has been suggested to use ten hypotheses to demonstrate the relationships between exogenous communication variables, perceived severity and vulnerability, and behavior intention. The hypotheses reflect the direct effect of campaign variables on threat appraisal variables and their mediating effect on behavior intention. The last step resulted in the creation of the extended PMT-based research model.

3.1 Protection Motivation Theory (PMT) as the Theoretical Base

PMT constitutes the underlying theoretical framework of this paper and serves as an explanatory tool for explaining the protective intentions of people with regards to scams and frauds. PMT, introduced in [13], entails two sets of parallel cognitive appraisals: the threat appraisal and the coping appraisal. Perceived severity, perceived vulnerability and perceived rewards for not protecting are included in the threat appraisal whereas the coping appraisal is composed of self-efficacy, response efficacy and response cost [7]. In the present study, attention will be paid to the threat appraisal since it is the one that would be more relevant in understanding the effect of campaign messaging on protective motivation. Several studies have validated the usefulness of PMT in phishing avoidance, cybersecurity and health behaviors. For example, [8] showed the significance of threat appraisal constructs in the avoidance of phishing attacks. Similarly, [14] reported the significance of perceived severity and perceived vulnerability in online safety behavior. A comprehensive literature review in [15] concluded that PMT has been extensively applied and validated in IS security research. In order to keep the model simple, in the present study, only perceived severity (PS) and perceived vulnerability (PV) will be kept without including the constructs from the coping appraisal.

Whereas coping appraisal constructs like response efficacy and self-efficacy are key components of numerous PMT-based investigations, their significance is greatly diminished within the scope of evaluation of awareness campaigns carried out by governments. These initiatives aim at boosting people's perception of the danger and susceptibility to it, rather than delivering training or building skills that would allow them to develop self-efficacy. In addition, response efficacy is influenced more by the policies of organizations or by instructions about behaviors to perform, not by public awareness [17], [18]. Previous empirical findings indicate that coping appraisal constructs become better predictors in case of learning or technical interventions [17], [18]. Therefore, in case of government awareness campaigns, the threat appraisal pathway is the preferable means of measuring their effect mechanisms [19], [20]. Furthermore, coping appraisal constructs have a contextual nature, since they depend on experience, technical skills, and availability of protective measures [5], [7]. This is rarely provided by government campaigns, which only seek to increase general awareness of dangers. The studies prove that self-efficacy and response efficacy influence protective behaviors in case of training, simulations, or guidelines based on policy [17], [21]. As there is no such intervention, exclusion of coping appraisal constructs would help achieve theoretical consistency.

3.2 Integrating Campaign Constructs into Threat Activation

The theory of PMT has evolved as a tool to understand the process of how fear appeals work to motivate protective behavior through communication research [6]. According to the principles of PMT, intentions of engaging in any kind of protection behavior result from two kinds of cognitive assessments called threat appraisal and coping appraisal, both of which get triggered as a result of the exposure of communications concerning the threat and the ways it could be mitigated [7]. Communication theories hold that the mode of delivery of a message plays a crucial role in shaping the assessments, as predicted by PMT [22].

Campaign exposure, defined as the frequency and reach of message contact, is crucial because greater exposure to health or safety campaigns tends to heighten risk perception [23]. For example, media exposure to COVID-19 information was observed to positively influence perceived severity and susceptibility among users, indicating that exposure can activate threat appraisal through increased salience of risk [24]. These supports including exposure as a construct that primes individuals to appraise threats more seriously.

Message comprehension pertains to the level of understanding of the information contained in a campaign. Comprehension is critical for cognition since if individuals do not comprehend the message, threat appraisal would not be possible [25]. Several empirical studies have found that comprehension of a message increases the perception of risk and behavioral intention to protect oneself in a protection motivation scenario [26]. It has also been observed recently that comprehension of organizational messages increases the motivation of employees to protect themselves [16]. The implication from such research is that comprehension serves as the informational foundation for threat evaluation. One needs to know what kind of danger it poses and who can be affected by it.

Message credibility is defined as the credibility and trustworthiness of the information given by the campaign. Credibility is based both on the source of the message and the veracity of the information in it and determines whether the audience accepts the information as credible [27]. High credibility of the message results in high threat appraisal due to trust in the fact of danger. Risk communication research has confirmed that credibility may play an important role in changing risk perception. The people, who perceive the communicator as credible, perceive the threat as valid and relevant [28]. Also, [29] reported the increase of compliance with risk messages when the communicator was perceived as credible in cases of health and emergency risks. It is also true for fraud prevention context as the people would ignore even effective warning messages when the credibility of the source and content is not high enough.

In conclusion, the use of the extension of PMT through variables such as campaign exposure, message comprehension, and message credibility increase the scope of explanation in regard to how persuasive communication influences cognitive appraisal. Exposure will make sure that there is continued contact with the message, comprehension will ensure that there is comprehension of the message, and credibility will help in creating faith in the message. Overall, all these variables come before threat appraisal and help in influencing the perception of severity and vulnerability, the two key variables that determine protection motivation.

3.3 Hypotheses Development

In line with the conceptual foundations of PMT along with the inclusion of campaign variables into the threat appraisal model, the research developed a number of hypotheses to test the impact of fraud awareness campaigns on protective behavior intentions. Exposure to campaigns, comprehension of messages, and message credibility serve as communication-related antecedent variables, which initiate the process of threat appraisal by affecting perceived severity and vulnerability.

Exposure to the campaign is believed to have positive effects on both perceived severity and perceived vulnerability. Higher frequency of exposure to anti-scam messages makes these messages more salient for individuals, who are therefore more likely to realize the severity of the risk and their vulnerability to it. Previous

research in mass communication and health communication indicates that exposure to a message increases the likelihood of perceiving it as a serious threat [23], [24]. Consequently, exposure to an anti-scam campaign is expected to positively affect both perceived severity and perceived vulnerability. It is further assumed that message comprehension will positively influence threat perception. Individuals who can easily comprehend message content are more likely to internalize the risk and personalize the threat. As has been indicated previously, research has shown that higher message clarity and understanding have direct effect on the perception of the threat severity and vulnerability to it [16], [26]. Therefore, message comprehension is expected to increase both perceived severity and perceived vulnerability. Message credibility is yet another factor that affects threat perception. When individuals believe in the accuracy and truthfulness of the message, they are more likely to accept both its main idea and its credibility. It is well known that risk communication research consistently shows that message credibility positively influences behavioral intentions and actions [28], [29].

From the perspective of the PMT, threat appraisal factors serve as powerful predictors of motivation for protective behavior. Perceived severity and perceived vulnerability are predicted to positively affect the motivation for protective behaviors, since people that consider a fraud threat to be severe and personally relevant will be motivated to behave in a preventive way [5], [7]. Moreover, since it is assumed that the campaign factors act through threat appraisal factors, mediation effects are hypothesized. More specifically, perceived severity is predicted to mediate the effect of campaign factors on protective behavioral intention, while perceived vulnerability will act in a similar way. These mediation hypotheses are based on the fundamental assumption of the Protection Motivation Theory according to which cognitive appraisals are responsible for translating communication into protective behaviors. The hypotheses are summarized in Table 1.

Table 1 *Hypotheses summary and theoretical rationale*

Hypothesis	relationship	Rationale
H1	Campaign Exposure → Perceived Severity	Frequent exposure increases recognition of threat seriousness [23], [24].
H2	Campaign Exposure → Perceived Vulnerability	Repeated exposure raises awareness of personal susceptibility [24].
H3	Message Comprehension → Perceived Severity	Clear messages improve understanding of threat consequences [26].
H4	Message Comprehension → Perceived Vulnerability	Comprehension personalizes risk and heightens vulnerability perception [16].
H5	Message Credibility → Perceived Severity	Trustworthy messages increase belief in risk seriousness [28].
H6	Message Credibility → Perceived Vulnerability	Credible communication enhances acceptance of personal risk [29].
H7	Perceived Severity → Protective Behavioral Intention	Belief in high severity motivates protective action [7].
H8	Perceived Vulnerability → Protective Behavioral Intention	Feeling personally at risk drives protective behavior [6].
H9	Perceived Severity mediates CE, MC, CR → Protective Behavioral Intention	Severity appraisals transmit campaign effects to behavioral intention [7].
H10	Perceived Vulnerability mediates CE, MC, CR → Protective Behavioral Intention	Vulnerability appraisals mediate campaign influence on protective behavior [6].

4. Results and Discussion

This paper constructs a conceptual framework to measure the efficacy of government interventions aimed at reducing people's vulnerability to scam and fraud. The conceptual framework is based on the PMT and augmented by communication constructs and identifies the psychological mechanisms through which the communication messages influence people's protective intentions. Figures are shown below to explain the conceptual framework and mediation process.

J. of Soft Computing and Data Mining Vol. 7 No. 3 (2026) p. 83-93

4.1 Research Model for Evaluating Campaign Effectiveness

The research model is illustrated in Fig. 2 and includes three constructs related to communication – campaign exposure, message comprehension, and message credibility, all in the context of the PMT framework. The constructs are expected to affect two major appraisal constructs of cognition – perceived severity and perceived vulnerability, which predict behavioral intention.

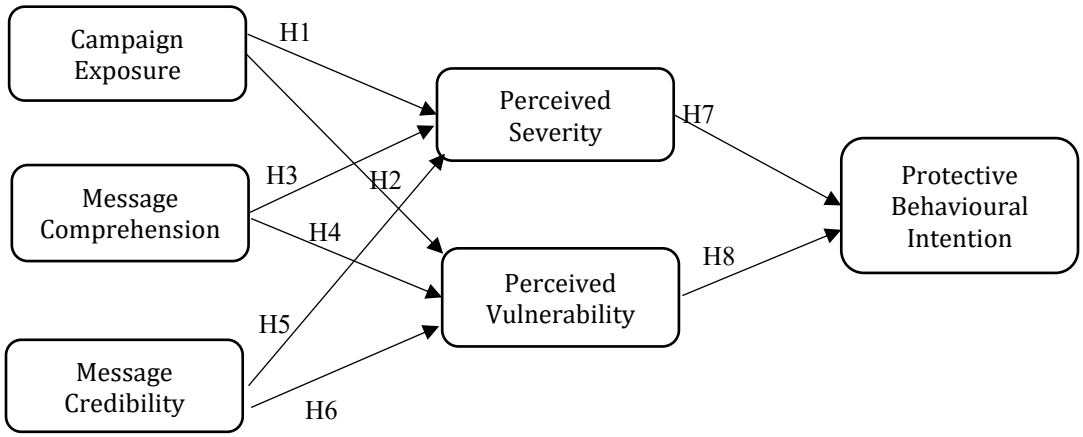


Fig. 2 *Research model for evaluating the effectiveness of government campaigns in scam and fraud prevention*

Firstly, this research model fills the literature gap in the existing body of literature based on Protection PMT. Most of the existing studies based on the Protection Motivation Theory focus on the role of internal cognitive components of threat perception such as perceived severity, vulnerability, and coping appraisal. On the contrary, those studies rarely pay attention to the external communication components that start the process of threat appraisal. Constructs such as message exposure, comprehension, and credibility are usually ignored even though the mentioned components have an impact on how people perceive certain risks and threats [9], [15].

The design of the proposed research model is justified through the theoretical studies that indicate the need to put the Protection Motivation Theory in the context of a broader perspective of persuasive communication. The combination of cognitive appraisals along with external message components gives researchers an opportunity to understand how people react to the actions taken by governments to protect citizens from scam [7], [29]. In this case, the model allows analyzing not only the effectiveness of anti-scam campaigns but also the processes leading to changes in motivational behavior.

Secondly, the major contribution of this research is connected with the fact that the proposed model is empirically proven to link external communication components with the internal psychological processes. Thus, the introduction of campaign exposure, comprehension, and credibility proves the fact that people's protective intentions are not created only due to the internal cognitive components of the perception but due to the external communication inputs as well. Unlike many previous PMT studies in the field of health and cybersecurity, the study focuses on the role of message delivery and puts that process in the center of the research. This way the model can be used as a diagnostic tool for policymakers who want to understand what parts of the campaign should be improved to increase its effectiveness.

4.2 Mediation Role of Perceived Severity

Fig. 3 illustrates the proposed mediating role of perceived severity in the relationship between campaign constructs and protective behavioral intention. The model suggests that the influence of campaign exposure, message comprehension, and message credibility on behavior is channeled through individuals' assessment of the seriousness of the scam threat.

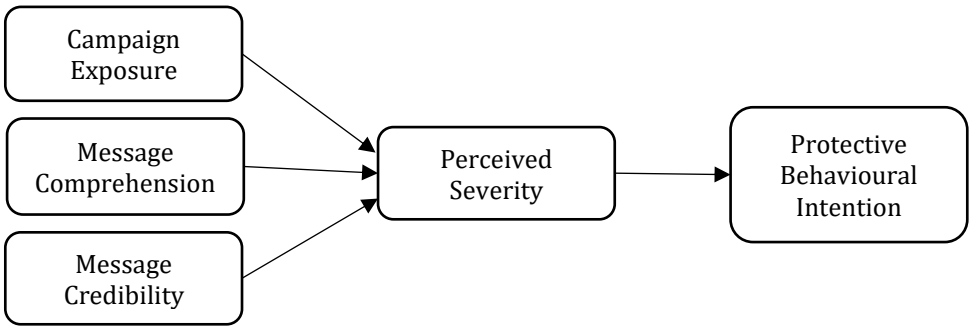


Fig. 3 *Mediation model for perceived severity (H9)*

This mediation route corresponds with PMT, which sees perceived severity as one of the major motivators of intention formation. Previous studies have shown that people who recognize the severity of a threat tend to engage in preventive behavior [9], [26]. Practically, this means that campaigns should emphasize possible consequences, regardless of frequency of messaging and reliability of sources, as otherwise messages may remain ineffective even when they possess all other features. Mediation model allows determining whether campaigns activate the severity element of threat appraisals.

Mediation analysis based on the perception of severity confirms expectations about the fact that activation of behavioral intentions takes place at the stage of understanding the serious nature of fraud threats. While campaign constructs can prime people, their effect on protective motivation is maximal if people feel the consequences of scams. Consistently, there is empirical evidence suggesting that increased perception of disease severity always predicts preventive measures, including vaccination and health screening among others. Similarly to public health campaigns, citizens who participate in the prevention of fraud need to recognize the serious consequences of scams in order to protect themselves.

From the standpoint of campaign design, this means that government may be wrong in the emphasis on the number of scams and neglect the severity of possible consequences. In addition, previous experience of campaigns suggests that campaigns which use vivid frames such as the description of experiences of the victims, statistics of national financial losses and the illustration of long-term consequences are much more effective. In general, perceived severity serves as an opportunity to improve campaigns' effects.

4.3 Mediation Role of Perceived Vulnerability

Fig. 4 presents the second mediation model, in which perceived vulnerability serves as the intermediary between campaign constructs and behavioral intention. This component reflects how individuals perceive their personal risk of falling victim to scams.

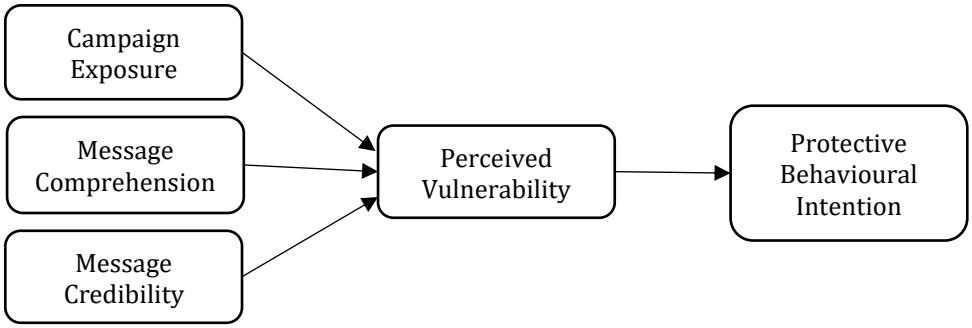


Fig. 4 *Mediation model for perceived vulnerability (H10)*

Like the PMT theory states, perceived vulnerability is an important mediator in the activation of protective motivation [7], [13]. The more likely individuals believe they are going to be affected by something, the higher the probability they will undertake some preventive actions. [16] also prove the relevance of vulnerability appraisals when dealing with digital threats, such as frauds and social engineering. In this case, it is necessary to make sure that campaign messages should not only inform but also personalize the risk of the danger. Some general or too

technical statements might not find the response from a particular audience, especially the one with low levels of digital literacy.

As far as the second mediation pathway via vulnerability is concerned, it is necessary to mention that the perception of the serious nature of a threat is useless until people are aware of their vulnerability to it. This means that protective intentions grow substantially when people perceive a risk of being scammed personally. As it can be seen from the patterns found during digital security training sessions, the same applies to the feeling of vulnerability towards phishing or malware attacks. Thus, the research provides empirical support for the PMT theory and its usage in the context of national efforts to prevent fraud.

In practice, it means that campaigns should be adjusted to the specificities of certain demographics. For example, older adults, young students, and rural communities may have different understandings of their vulnerability to frauds depending on their digital literacy and previous experiences. Campaigns which will try to address different demographic groups using personalized stories or narratives will succeed in increasing vulnerability appraisals better than others. Otherwise, messages will be left abstract and will not affect the intended target.

4.4 Contribution to Theory and Application

Collectively, the three figures presented in this section provide a theory-driven and application-oriented model for evaluating anti-scam campaigns. The framework contributes to PMT research by clarifying the role of external communication factors in activating internal cognitive appraisals that guide protective behavioral intentions. By combine campaign exposure, message comprehension, and message credibility into the PMT structure, this study advances theoretical understanding of how persuasive communication translates into protection motivation, thereby addressing a gap in prior studies that largely focused on internal cognitive pathways alone. This integration positions the model as an important extension of PMT, demonstrating that external message characteristics function as necessary antecedents to threat valuation.

Theoretically, the current investigation also makes a substantial contribution to the field of communication research as it establishes a link between variables of campaign design and their mediating psychological role in determining protective behavior. Following the recent trends in literature, this study proposes a way of integrating models of persuasive communication with behavioral theories as means of providing an overall view of the process of individual reactions to governmental scam prevention campaigns. This conceptual framework can become an important guide for future researchers on the issue.

In practical terms, the proposed framework of analysis is extremely valuable for public agencies and policymakers. Being informed about the specific mechanisms of psychological mediation by which a particular campaign influences people's responses, it becomes possible to create a set of measures necessary to optimize this process. For instance, the exposure of the campaign can be improved by using several ways of disseminating it; comprehension may be facilitated by adjusting the level of literacy of the targeted audience and its credibility may be increased by partnering with reputable organizations. Thus, using this model in practice allows designing more efficient anti-scam campaigns not only in terms of raising the level of awareness but also of inducing certain behavioral intentions. Indeed, despite the existing attempts to counteract scammers and the rise of scams among the general population, the problem still requires considerable attention and solutions.

5. Conclusion and Future Work

This study constructs a conceptual research model to evaluate the effectiveness of anti-fraud publicity campaigns implemented by national governments, based on PMT. In response to the growing complexity of fraud threats and their expanding harm, three core communication variables—publicity reach, information comprehension, and information credibility—are added to the original PMT model as external antecedent variables for threat assessment. By integrating these new variables with the original PMT dimensions of perceived severity and perceived vulnerability, this study establishes a theoretical analytical framework that can explain how anti-fraud publicity shapes the public's willingness to adopt protective behaviors.

The importance of this study can be seen in two aspects. First of all, the paper highlights an important gap in the existing literature in terms of the interdependence between message-level factors and cognitive and behavioral responses to these messages. While the previous literature focused on the evaluation of protection motivation theory in the absence of any communication context, the proposed model shows the whole chain of cognitive processes in terms of receiving the message and making an intention. Second, it offers a practical theoretical framework that can be used in empirical studies as well as in the design of campaigns.

Taking into consideration that the paper deals with the development of the concept, the empirical test of the proposed model is one of the crucial tasks for the future research. Therefore, future studies should include the process of defining the constructs, designing the instruments to measure them and obtaining quantitative data to validate the hypotheses. This includes the process of validating survey questions and their reliability and testing the model via structural equation modeling. In addition, it would be reasonable to analyze moderating variables

like demographics and digital literacy. Overall, the paper contributes to the literature on cybersecurity awareness, behavioral science and public policy, both theoretically and practically.

Acknowledgement

This research is fully supported by UC TATI Short Term Grant (STG), 9001-2405, which help in completing the research in viable and efficient.

Data Available Statement

Data Availability Statement: No new data were generated or analysed in this study, as this paper is conceptual in nature. All information used in developing the conceptual framework is derived from the published literature cited in the article. For further information regarding the study, readers may contact the corresponding author.

Conflict of Interest

There is no conflict of interests regarding the publication of the paper.

Author Contribution

The authors are responsible for the study conception, research design, data collection, data analysis, result interpretation and manuscript drafting.

References

[1] S. Azmi *et al.*, "A Qualitative Approach of KAP Model Against Online Scam in Malaysia," *Int. J. Acad. Res. Bus. Soc. Sci.*, vol. 15, Feb. 2025, doi: 10.6007/IJARBSS/v15-i2/24701.

[2] M. Bada, A. M. Sasse, and J. R. C. Nurse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?" no. April 2019.

[3] N. N. Ghazali, S. Hassan, and R. Ahmad, "Fortifying Against Cyber Fraud: Instrument Development with the Protection Motivation Theory," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 10, pp. 519–526, 2023, doi: 10.14569/IJACSA.2023.0141055.

[4] S. Hassan, R. Ahmad, N. Katuk, N. N. Ghazali, J. A. Aripin, and F. Ali, "Staying One Step Ahead: Exploring Protection Motivation Theory to Combat Cyber-fraud Among E-services Users.," *Procedia Comput. Sci.*, vol. 234, no. 2023, pp. 1364–1371, 2024, doi: 10.1016/j.procs.2024.04.011.

[5] 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.

[6] R. W. Rogers, "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation," in *social psychophysiology. A sourcebook*, 1983.

[7] D. L. Floyd, S. Prentice-Dunn, 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.

[8] Huigang Liang and Yajiong Xue, "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective.," *J. Assoc. Inf. Syst.*, 2010.

[9] 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.*, 2016, doi: 10.1016/j.cose.2016.02.009.

[10] T. for G. Institute, "Building resilience against scams and fraud: Spotlight on Malaysia," 2024. https://techforgoodinstitute.org/blog/event-highlights/building-resilience-against-scams-and-fraud-spotlight-on-malaysia/.

[11] M. Business, "Banks collectively launch refreshed #JanganKenaScam awareness campaign," *Malaysian Business*, 2023. https://www.malaysian-business.com/index.php/wordpress/item/8390-banks-collectively-launch-refreshed-jangankenascam-awareness-campaign.

[12] Businesstoday, "Banks' scam awareness campaign proves effective – survey," *Businesstoday*, 2023. https://www.businesstoday.com.my/2023/11/09/banks-scam-awareness-campaign-proves-effective-survey/.

[13] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," *J. Psychol.*, 1975.

[14] 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," 2016, doi: 10.1016/j.cose.2016.02.009.

[15] 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 Adv. Inf. Syst.*, 2021, doi: 10.1145/3462766.3462770.

[16] L. A. Tawalbeh and F. Muheidat, "Factors that Motivate Defense Against Social Engineering Attacks Across Organizations," 2023, doi: 10.1016/j.procs.2023.09.013.

[17] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Comput. Secur.*, vol. 31, no. 1, pp. 83–95, Feb. 2012, doi: 10.1016/J.COSE.2011.10.007.

[18] M. Warkentin, A. Johnston, J. Shropshire, and W. Barnett, "Continuance of Protective Security Behavior: A Longitudinal Study," *Decis. Support Syst.*, vol. 92, Sep. 2016, doi: 10.1016/j.dss.2016.09.013.

[19] 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. Manag. Inf. Syst.*, 2015, doi: 10.25300/MISQ/2015/39.4.5.

[20] A. C. Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Q.*, vol. 34, no. 3, pp. 549–566, Aug. 2010, doi: 10.2307/25750691.

[21] T. Herath and R. Rao, "Protection motivation and deterrence: A framework for security policy compliance in organisations," *EJIS*, vol. 18, pp. 106–125, Apr. 2009, doi: 10.1057/ejis.2009.6.

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

[23] Michael D Slater, "Operationalizing and Analyzing Exposure: The Foundation of Media Effects Research," *Journal. Mass Commun. Q.*, vol. 81, no. 1, pp. 168–183, Mar. 2004, doi: 10.1177/107769900408100112.

[24] Y. Feng, W. Gu, F. Dong, D. Dong, and Q. Zhihong, "Overexposure to COVID-19 information amplifies emotional distress: a latent moderated mediation model," *Transl. Psychiatry*, vol. 12, p. 287, Jul. 2022, doi: 10.1038/s41398-022-02048-z.

[25] R. E. Rice and C. K. Atkin, "Public Communication Campaigns." SAGE Publications, Inc., 55 City Road, London, 2013, doi: 10.4135/9781544308449.

[26] R. C. Plotnikoff and L. Trinh, "Protection motivation theory: Is this a worthwhile theory for physical activity promotion?," *Exerc. Sport Sci. Rev.*, 2010, doi: 10.1097/JES.0b013e3181d49612.

[27] C. I. Hovland and W. Weiss, "The Influence of Source Credibility on Communication Effectiveness*," *Public Opin. Q.*, vol. 15, no. 4, pp. 635–650, Jan. 1951, doi: 10.1086/266350.

[28] Alyssa Appelman and S. Shyam Sundar, "Measuring Message Credibility: Construction and Validation of an Exclusive Scale," *Journal. Mass Commun. Q.*, vol. 93, no. 1, pp. 59–79, Oct. 2015, doi: 10.1177/1077699015606057.

[29] K. P. Hocevar, M. Metzger, and A. J. Flanagin, "Source Credibility, Expertise, and Trust in Health and Risk Messaging," in *Oxford Research Encyclopedia of Communication*, 2017.