

**JOURNAL OF INFORMATION
SYSTEM AND TECHNOLOGY
MANAGEMENT
(JISTM)**www.gaexcellence.com/jistm**DEVELOPING A CYBERCRIME SELF-PROTECTION
INSTRUMENT FOR TEACHERS: INTEGRATING THEORY
OF PLANNED BEHAVIOR AND SELF-EFFICACY)**Nurul Hidayah Mohd Yusof¹, Ahmad Zainal Abidin Abd Razak^{2*}¹Faculty of Management and Economics, Universiti Pendidikan Sultan Idris, Malaysia p20192001332@siswa.upsi.edu.my <https://orcid.org/0009-0001-7160-5483>²Faculty of Management and Economics, Universiti Pendidikan Sultan Idris, Malaysia ahmad.zainal@fpe.upsi.edu.my <https://orcid.org/0000-0001-8333-8020>

*Corresponding Author

Article Info:**Article history:**

Received date: 30.07.2026

Revised date: 24.08.2026

Accepted date: 24.09.2026

Published date: 28.09.2026

To cite this document:

Yusof, N. H. M., & Razak, A. Z. A. A. (2026). Developing A Cybercrime Self-Protection Instrument for Teachers: Integrating Theory of Planned Behavior and Self-Efficacy). *Journal of Information System and Technology Management*, 11 (44), 676-693.

Abstract:

The increasing number of internet users in Malaysia has led to increased exposure to cybercrime risk. Among the various forms of cybercrime, telecommunication fraud like the Macau scam has become a major concern. This type of scam deceives individuals through phone calls and messages. Although various awareness campaigns have been conducted, the cases still occur. This shows that existing preventive efforts are insufficient to encourage sustained self-protective behaviour. Teachers are among the targeted groups by the scammers. However, only a few instruments have been developed specifically to examine the factors influencing teachers' intention and self-protective behaviour. Therefore, this study aims to develop a structured questionnaire to investigate the factors influencing teachers' intention to adopt self-protective behaviours against cybercrime. Intention serves as a mediating variable leading to self-protective behaviour in the Malaysian context. The instrument was developed by combining the Theory of Planned Behavior (TPB) and Self-Efficacy Theory. Its consisting of attitude, subjective norms, perceived behavioural control, self-efficacy, and intention to self-protect. 7-point Likert scale was used to measure the items. The questions were adapted from previous studies on cybercrime. A quantitative approach was used, and the questionnaire was pilot tested with teachers from a selected public school to assess the clarity of the items and the reliability and factor structure of the instrument. The pilot data were analysed using SPSS. Internal consistency of the items was assessed by using Cronbach's alpha while Exploratory Factor Analysis (EFA) was used to examine the factor structure of the instrument. The preliminary results confirmed high internal consistency across all scales, with Cronbach's alpha

coefficients exceeding the 0.70 threshold. Ultimately, this study provided a validated, context-specific questionnaire that reliably measures teachers' behavior to mitigate cyber risks, serving as a practical tool for future empirical research and policymaking.

DOI: 10.35631/JISTM.1144041 **Keyword:**

Cybercrime, Cybersecurity Behaviour, Macau Scam, Self-Efficacy, Theory of Planned Behavior



© The authors (2026). This is an Open Access article distributed under the terms of the Creative Commons Attribution (CC BY NC) (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited. For commercial re-use, please contact jistm@gaexcellence.com.

Introduction

The internet is now a vital part of everyday life. Following the COVID-19 pandemic, Malaysia experienced a sharp rise in digital use; as such, in 2021, the percentage of individuals who used the internet was 96.8% (DOSM, 2022). Although the digital transformation offers more convenience, it also exposes the general population to more cybersecurity risks. One of the main risks that is currently being addressed is the Macau scam. Today, scammers use voice over IP (VoIP), caller identification spoofing, and social engineering to trick unsuspecting people (Rosley et al., 2023).

Despite continuous efforts by government authorities and cybersecurity agencies, Macau Scam cases continue to arise. According to the Royal Malaysia Police, 7,734 scam cases were reported in 2023, resulting in financial losses exceeding RM321.1 million (PDRM, 2023). Scammers have become more sophisticated and now utilise artificial intelligence (AI)-generated voice cloning and spoofed caller identification to manipulate victims. As a result, these scams affect individuals across different socioeconomic backgrounds, including retirees, corporate professionals, and educators (Bernama, 2023).

Although various regulatory measures and public awareness campaigns have been introduced, these initiatives remain insufficient to effectively reduce the growing incidence of cyber scams (MKN, 2024). One of the main challenges is human behaviour. Many individuals underestimate their vulnerability to cyber threats, have limited awareness of evolving scam techniques, and are unable to recognise fraudulent attempts. Existing studies have largely focused on technological solutions, while the behavioural and cognitive factors influencing cybersecurity remain relatively underexplored. Factors such as attitude, perceived behavioral control, social influence, and self-efficacy play important roles in shaping individuals'

intentions to adopt self-protective behaviours (Chatterjee et al., 2019; Nurul Nadiyah et al., 2019).

Furthermore, research on teachers' self-protective behavior against cybercrime remains scarce, even though teachers are among the demographics frequently targeted by online scams in Malaysia (Bernama, 2023). Examining teachers' cybersecurity behavior is essential because they act as key agents in nurturing digital literacy among future generations. Cultivating a cyber-savvy society requires teachers to possess adequate knowledge and actively demonstrate safe online practices themselves (Jelani et al., 2021). Consequently, questions arise regarding teachers' actual preparedness and capability to mitigate cyber risks. This is critical because, without mastering and adopting these protective behaviors, teachers cannot effectively impart cybersecurity knowledge to their students, leaving the aspiration of a cyber-secure society dashed.

In order to fill these research gaps, the present study seeks to develop and validate a structured survey tool for measuring teachers' self-protective intentions and behaviours in relation to cyber threats. Based on the Theory of Planned Behavior (TPB) and Self-Efficacy Theory, the instrument included the main constructs of attitude, subjective norms, perceived behavioral control, self-efficacy, and self-protection intention. By offering a measurement tool that is rooted in theory and proven to be reliable, the study enhances our understanding of the cognitive factors that influence self-protective behaviour. The instrument is expected to help support future research and to assist policymakers, educational institutions, and cybersecurity agencies in formulating targeted behaviour-based intervention strategies in order to improve cybersecurity awareness and promote a more cyber-savvy society in the future.

Literature Review

Theory of Planned Behavior (TPB)

The conceptual framework of this study is based on the Theory of Planned Behavior (TPB) proposed by Ajzen (1991). TPB is an extension of the Theory of Reasoned Action (TRA). It has been widely used to understand how individuals' intentions can lead to specific behaviors (Ajzen, 2001). The empirical validity of TPB has been demonstrated across a range of contexts, including retail cybercrime (Aloysius et al., 2019), educational program enrollment (Li et al., 2009), and ethical decision-making (Reni & Anggraini, 2016). Under TPB, actual behavior is largely influenced by behavioral intention. TPB was determined by three key construct which is attitude, subjective norms, and perceived behavioral control (PBC) (Aertsens et al., 2011). Attitude refers to an individual's positive or negative evaluation of a particular behavior (Pavlou & Fygenson, 2006), while subjective norms represent the perceived social influence of important people or groups (Ajzen, 1991; Valliere, 2017). PBC reflects an individual's perception of how easy or difficult it is to perform the behavior (Ajzen, 1991; Bandura, 1997). When these determinants align positively, the likelihood of an individual engaging in the target behavior increases significantly. In the context of cybercrime mitigation, TPB provides a useful framework for understanding how individuals adopt self-protective behaviors, particularly when engaging in high-risk online activities (Daud et al., 2020). The framework developed helps to explain how attitudes, social expectations, and individuals perceived control over their actions work together to influence their decision to take active measures to protect themselves from emerging digital threats.

Self-efficacy Theory

In addition to the TPB, Self-efficacy Theory by Bandura (1997) was also frequently employed by researchers to explain human behavior. Self-efficacy refers to an individual's belief in their ability to organize and execute the actions necessary to achieve a specific goal (Bandura, 1986, 1991). This cognitive characteristic is important because confidence in one's own abilities helps individuals manage complex challenges, particularly in uncertain situations involving risks such as cybercrime (Bellò et al., 2018). As a result, individuals with higher self-efficacy tend to demonstrate greater motivation and commitment to apply protective behaviors (Hassan et al., 2020; Bortne et al., 2025).

Although self-efficacy and perceived behavioral control (PBC) look similar, they remain distinct constructs within the behavioral literature. Self-efficacy primarily reflects an individual's internal belief in their personal competence, which is often strengthened through direct experience (Parkinson et al., 2017). In contrast, PBC extends beyond internal confidence by incorporating external factors, including the availability of resources and situational opportunities that facilitate behavior (Ajzen, 1991). The availability and use of security tools can enhance PBC by making protective actions appear more manageable within a given context (Son et al., 2013). In essence, self-efficacy reflects the internal conviction that "I believe I can do it," whereas PBC represents the broader perception that "I have the control and resources to do it."

In keeping with this distinction, research carried out in Malaysia showed that internet self-efficacy among students and teachers is still relatively low, which hinders the uptake of effective privacy and cybersecurity practices (Lee, Tan, & Siah, 2017; Zainal et al., 2023). These results show how important it is to boost people's confidence in carrying out protective actions by means of specific interventions, for example through awareness campaigns, digital literacy programmes, and the development of practical cybersecurity skills. Furthermore, an increased awareness of how often and how severely cyber threats occur will result when appropriate educational programmes are introduced. This in turn can enhance people's motivation to carry out self-protective behaviours (Drew, 2020). To sum up, self-efficacy is about individuals' belief in their own ability, while perceived behavioural control (PBC) takes into account both personal capability and the availability of the resources needed to carry out a behaviour.

Behavior To Self-Protect

Attitude, subjective norms, and perceived behavioral control are widely recognised as key determinants of human behaviour under the Theory of Planned Behavior (TPB) (Ajzen, 1991, 2002). Extensive empirical evidence demonstrates that these constructs significantly influence behavioural intention, with perceived behavioural control consistently identified as one of the strongest predictors of actual behaviour (Choi & Suh, 2022; Yoon, 2011). Within the context of cybercrime prevention, behavioural factors are particularly important because effective mitigation relies largely on individuals' willingness to adopt appropriate self-protective practices (Hadlington & Chivers, 2018; Warner et al., 2014).

The adoption of self-protective behaviour is influenced not only by behavioural beliefs but also by individuals' confidence in their ability to protect themselves. According to Bandura (1986), effective self-protection depends on individuals' capability to make informed decisions and

create a secure environment rather than relying solely on external interventions. Consequently, proactive self-protection is regarded as a shared responsibility, complementing governmental initiatives and legal enforcement in reducing cybercrime risks (Afida et al., 2014; Boush et al., 2015). Individuals are generally more likely to adopt protective measures when the perceived benefits exceed the associated costs, whereas protective behaviour declines when the perceived effort or inconvenience outweighs the expected consequences of victimisation (McCarthy & Chaudhary, 2014; Skogan, 1981; Vakhitova et al., 2020). Despite these findings, limited research has examined how individual characteristics influence the adoption of self-protective behaviours (Fissel & Lee, 2024).

Self-efficacy has also been widely recognised as an important predictor of behavioural intention and actual behaviour. Previous experiences shape individuals' confidence in performing protective actions, thereby strengthening their intention to engage in cybersecurity practices (Parkinson et al., 2015; Van Stralen et al., 2009). Accordingly, self-protective behaviour has become increasingly important during online activities such as e-commerce, online banking, and social networking, which expose users to various cyber threats (Daud et al., 2020). This perspective is consistent with the National Consumer Policy, which promotes knowledgeable, proactive, and responsible digital citizens capable of practising continuous online self-protection (Afida et al., 2014; National Consumer Policy, 2010).

People's individual attitudes and personal traits also affect how they respond to cyber risks. Generally, a sense of insecurity causes people to be more careful, while too great a sense of confidence often causes individuals to underestimate cyber threats and fail to take necessary security measures (Abassi et al., 2016; Lea et al., 2009). These differences in behaviour are in turn influenced by demographic and psychological factors such as personality, gender, education, nationality, and previous life experiences (Messick, 1999). The same kind of pattern can be seen in Malaysia, since internet users there show different levels of perceived online safety, indicating variations in their cyber risk perception (MCMC, 2020).

There is a high usage of the internet in areas of working, learning, purchasing goods and communicating, which opens up new possibilities for cybercriminal behavior (Olofinbiyi & Singh, 2020). Cybercriminals have adjusted their tactics to exploit the changes in the behavioral pattern (Felson & Clarke, 1998), which means the necessity of developing adequate self-protection measures. People who feel more in control of their resources usually are in a better position to practice the necessary behaviors and decrease their vulnerability to cyber risks (Dawson et al., 2021). Previous victimization has led to behavioral changes aimed at avoiding repeated victimization (Cohen & Felson, 1980; Turanovic & Pratt, 2014); however, findings from studies conducted to date are inconclusive. Drew (2020) found no significant difference in the behavior of previous victims and non-victims.

Recent evidence further indicates that many internet users remain unaware that routine online activities, including social networking, online shopping, browsing digital content, and seeking online relationships, may inadvertently expose sensitive personal information to cybercriminals (Ernawati et al., 2023; Khadijah et al., 2020; Lee et al., 2022). Cybercriminals increasingly exploit these behaviours through highly targeted attack strategies (Fidlizan Muhammad et al., 2024). Moreover, individuals who are unable to distinguish legitimate websites from fraudulent platforms are particularly vulnerable to financial fraud and identity theft (Hamsi et al., 2015; Zahari et al., 2019). This highlights the importance of strengthening

cybersecurity awareness, digital literacy, and secure online practices (Dunham, 2022; Puram et al., 2011; Wilson et al., 2023).

In addition, psychological characteristic such as low awareness, high neuroticism, limited internet experience, and poor digital literacy has been consistently associated with greater cybercrime susceptibility (Fidlizan Muhammad et al., 2024; Ge et al., 2021). Beyond individual capability, support from family members and close friends also contributes to cybercrime prevention by encouraging information sharing, validating suspicious online activities, and facilitating informed decision-making (Fidlizan Muhammad et al., 2024).

Methodology

Research Design

This study using a quantitative, cross-sectional research design to examine teachers' self-protective behaviours against cybercrime. Pilot test data were analysed using IBM SPSS Statistics Version 29. IBM SPSS Statistics is a widely recognised statistical software package that facilitates data management, interpretation, and quantitative analysis across various social science disciplines (Wagner-Huang, 2020).

Sampling Strategy

The target population for this pilot study comprised Malaysian public secondary school teachers (*Sekolah Menengah Kebangsaan*, SMK). This demographic was selected because public servants, particularly teachers, are heavily targeted by online scammers, with police statistics indicating an average of three teacher victims daily (Bernama, 2023; Majlis Keselamatan Negara, 2023).

SMK schools were specifically chosen over specialized institutions-such as Science Schools, Religious Schools, or National-Type Schools (*Sekolah Jenis Kebangsaan*, SJK) due to the greater demographic and professional diversity of their teaching staff. In SMKs, there are many academic streams, and their educators are composed of many genders, races, ages, and educational levels. It is important that this be reflected in the pilot phase of testing to avoid biases in sampling and ensure that the measurement instrument is generally applicable to all kinds of teachers.

Also, it is important to validate this scale among teachers because of their double responsibility for cyber risk management. Beyond their vulnerability as potential targets, educators play a pivotal role in promoting online safety. Enhancing their digital resilience not only improves their self-protective behaviors but also fosters cybersecurity awareness among students (Pitchan et al., 2019; Zulkifli et al., 2020; Ahmed et al., 2021; Pitchan et al., 2025).

A cluster sampling approach was adopted, with individual schools serving as sampling clusters to facilitate preliminary data collection. Each selected school formed a heterogeneous cluster spanning various genders, age brackets (23-60 years), ethnicities, religions, and qualifications. Including both male and female teachers at this pilot stage helped identify and mitigate potential gender-related response bias before finalizing the survey scale (Jusoh & Nizar, 2022).

Pilot Testing

A total of fifty teachers from one selected school participated in the pilot study to assess the reliability and validity of the research instrument. Data were collected using an online questionnaire administered through Google Forms. The data collection process was conducted in one-month period, from April until May 2026.

Content Validation

Two subject matter experts from the management field were referred for the validation of the questionnaire. The evaluation centred on the format and structure, language used, and the presence of ambiguous or redundant items. The information that was received after the validation process was then used to enhance the quality of the questionnaire.

Ethical Consideration

In the initial section of the questionnaire, a declaration of informed consent was included in order to inform about the aims of the research, the rights of the respondents, the confidentiality policy, the usage of collected data, and consent. This has been done to protect the personal details of the respondents and to maintain ethics in research.

Questionnaire Structure

The questionnaire comprised seven sections, with the measurement items adapted from established sources in the literature. Section A gathered respondents' demographic information, including gender, age, race, nationality, highest educational qualification, individual gross income, experience of scam victimization and frequency of receiving suspicious calls. Sections B to G consisted of 7 items measured using a seven-point Likert scale. A seven-point Likert scale was used, as it is one of the most commonly adopted response formats in research (Cox, 1980). The use of an odd number of response options allows respondents to select a neutral response when appropriate (Preston & Colman, 2000). Compared with a five-point scale, a seven-point Likert scale provides greater response discrimination and more accurately captures respondents' opinions (Chang, 1994; Cox, 1980). Previous research has also suggested that using more than seven response categories may reduce response accuracy, as respondents may find it difficult to distinguish between the available options (Miller, 1956).

Measurement Items

The questionnaire consisted of six constructs: attitude, subjective norms, perceived behavioral control, self-efficacy, intention to self-protect, and behavior to perform self-protect. All measurement items were adapted from previously validated instruments and assessed using a seven-point Likert scale ranging from 1 (strongly disagree) to 7 (strongly agree).

The Attitude (ATT) scale used was composed of seven items, which were drawn from Van Steen and Deeleman (2021) and Glanz et al. (2015). The items focused on measuring how important, useful, and beneficial were the respondents' perceptions about practicing cybersecurity behaviors. More specifically, the items evaluated whether the respondents perceive compliance with cybersecurity policies, maintaining devices and software updated, usage of scam detection apps, and practicing cybersecurity behaviors to improve online

security and minimize chances of being scammed. Subjective norms (SBN) scale used consisted of seven items drawn from Glanz et al. (2015) and Van Steen and Deeleman (2021). The items examined the extent to which the respondents are socially influenced by significant others regarding their cybersecurity behaviors and how these others encourage and support them to practice cybersecurity behaviors.

Perceived Behavioral Control (PBC) was measured using seven items adapted from Van Steen and Deeleman (2021) and Armitage et al. (1999). The items evaluated respondents' perceived control and ability to perform recommended cybersecurity behaviours, including complying with cybersecurity policies, avoiding phishing emails, scanning devices, detecting scam calls, updating devices, and exercising personal control in protecting themselves against cyber scams. Self-efficacy (SEF) was measured using seven items adapted from Cho and Lee (2015) and Pratama et al. (2025). These items assessed respondents' confidence in their ability to protect themselves from cyber scams, perform precautionary measures despite potential challenges, recognise scam attempts, and manage their actions to minimise the risk of cybercrime victimisation.

Intention to Self-protect (INT) was measured using seven items adapted from Cho and Lee (2015) and Pratama et al. (2025). The items assessed respondents' intentions to adopt self-protective behaviours against cybercrime, including avoiding cyber risks, being more cautious when dealing with suspicious situations, changing passwords regularly, updating antivirus software, monitoring unusual device activities, responding promptly to scam alerts, and creating strong passwords.

Behavior to Perform Self-protect (BEH) was measured using seven items adapted from Huang et al. (2020). These items evaluated respondents' actual self-protective cybersecurity practices, including checking network and website security before accessing online services, managing browsing history, updating antivirus software, using different passwords across online platforms, responding immediately to scam alerts, and using applications that identify or block unknown callers.

Data Analysis

The pilot test data was analyzed by using IBM SPSS Statistics Version 29 to validate the measurement model. Descriptive analysis, factor analysis, reliability measures and Exploratory Factor Analysis (EFA) analysis were conducted. Results from the analyses were used by the researcher to evaluate the real feedback from the respondents and this helped a lot in making a conclusion and recommendations.

Findings

Descriptive Analysis

A total of 47 out of 50 distributed questionnaires were returned, representing a high response rate of 94%. Table 1 presents the detailed profile of the respondents.

Table 1: Descriptive Analysis of Respondent Profile

Description		Percentage (%)
Gender	Male	19.1
	Female	80.9
Age Group	21-30	34
	31-40	27.7
	41-50	14.9
	51-60	23.4
Race	Malay	95.7
	Chinese	2.1
	Indian	2.1
Nationality	Malaysian	100
Education Level	Diploma	25.5
	Degree	63.8
	Masters	8.5
	PhD	2.1
Income Level (Gross)	RM2001-RM3000	19.1
	RM3001-RM4000	23.4
	RM4001-RM5000	10.6
	RM5001-RM6000	2.1
	RM6001-RM7000	10.6
	RM7001-RM8000	6.4
	RM8001-RM9000	14.9
	RM9001-RM10000	12.8
Victimization Experience	Yes	40.4
	No	59.6
Frequency of Receiving Suspicious Call or Scam Attempt Per Month	Never	8.5
	1-2 times	44.7
	3-4 times	21.3
	5-6 times	14.9
	7-8 times	4.3
	> 8 times	6.4

Table 1 has shown that 80.9% of the respondents were female, while remaining balance of 19.1%. were male. Majority aged between 21 and 30 years old (34.0%), followed by those aged 31 to 40 years old (27.7%), 51 to 60 years old (23.4%), and 41 to 50 years old (14.9%). Most of the respondents were Malays (95.7%) with Chinese and Indian teachers comprising 2.1% each. All participating teachers were Malaysian citizens (100.0%). Regarding educational background, the teachers were highly qualified, with a majority holding a Bachelor's degree (63.8%), followed by Diploma holders (25.5%), Master's degree holders (8.5%), and PhD holders (2.1%). For monthly gross income, the distribution among the teachers was diverse. Majority of the respondent earned gross income between RM3,001 and RM4,000 (23.4%), followed by RM2,001 to RM3,000 (19.1%) and RM8,001 to RM9,000 (14.9%).

From the findings, it has shown that 40.4% of the respondents reported having experienced prior victimization. Whereas 59.6% had never been victimized. Furthermore, concerning the frequency of receiving suspicious calls or scam attempts per month, only 8.5% of the teachers had never encountered any attempts. The majority of participating teachers (44.7%) reported receiving suspicious calls 1 to 2 times per month, followed by 3 to 4 times (21.3%), 5 to 6 times (14.9%), 7 to 8 times (4.3%), and more than 8 times per month (6.4%). Overall, the diverse background and active scam exposure among the teachers provided an appropriate context for validating the survey instrument.

Exploratory Factor Analysis

Table 2 shows the results of Exploratory Factor Analysis loadings, KMO statistics, and Cronbach's alpha reliability values for all constructs.

Table 2: Summary of Exploratory Factor Analysis (EFA) and Reliability Analysis by Construct

Construct	Initial Loading	Final Loading	KMO	Construct	Initial Loading	Final Loading	KMO
Individual Attitude			0.831	Self-efficacy			0.914
ATT1	0.756	0.756		SEF1	0.898	0.898	
ATT2	0.867	0.867		SEF2	0.912	0.912	
ATT3	0.671	0.671		SEF3	0.918	0.918	
ATT4	0.956	0.956		SEF4	0.895	0.895	
ATT5	0.878	0.878		SEF5	0.924	0.924	
ATT6	0.706	0.706		SEF6	0.831	0.831	
ATT7	0.829	0.829		SEF7	0.859	0.859	
Subjective Norms			0.794 (0.789) *	Intention to Self-protect			0.803
SBN1	0.692	0.625*		INT1	0.754	0.754	
SBN2	0.808	0.650*		INT2	0.780	0.780	
SBN3	0.588 & 0.680	-		INT3	0.741	0.741	
SBN4	0.634	0.664*		INT4	0.780	0.780	
SBN5	0.817	0.856*		INT5	0.770	0.770	
SBN6	0.867	0.908*		INT6	0.695	0.695	
SBN7	0.854	0.904*		INT7	0.659	0.659	
Perceived Behavioral Control			0.897	Behavior to Perform Self-protect			0.890
PBC1	0.896	0.896		BEH1	0.778	0.778	
PBC2	0.829	0.829		BEH2	0.842	0.842	
PBC3	0.909	0.909		BEH3	0.904	0.904	

PBC4	0.877	0.877	BEH4	0.932	0.932
PBC5	0.906	0.906	BEH5	0.870	0.870
PBC6	0.838	0.838	BEH6	0.810	0.810
PBC7	0.829	0.829	BEH7	0.792	0.792

Sphericity significant value : $p < 0.001$

Note: Values marked with () indicate refined EFA results after dropping item SBN3. Initial KMO was 0.794.

All the constructs had high sampling adequacy since the KMO values varied between 0.794 and 0.914, with Bartlett's test of sphericity attaining statistical significance at $p < 0.001$. All but one item had high loadings (higher than 0.60) on their corresponding constructs. SBN3 was excluded from the Subjective Norms construct owing to cross-loading problems with an item loading value of less than 0.20 (loadings were 0.588 and 0.680). After excluding SBN3, all other constructs had clear unidimensional factors structures.

Reliability Test

Reliability through internal consistency of the measuring tool was calculated by employing the Cronbach's alpha coefficients. The purpose of this calculation is to ensure the statistical validity of the questionnaire scales. The Cronbach's alpha values of all constructs are presented in Table 3.

Table 3: Summary of Reliability Test

Construct	No. of Items measured	Cronbach's Alpha Value
ATT	7	0.926
SBN	6	0.896
PBC	7	0.955
SEF	7	0.964
INT	7	0.894
BEH	7	0.943

As displayed in Table 2, all constructs exhibited high internal consistency reliability, with Cronbach's alpha values ranging from 0.894 to 0.964, well above the standard acceptable threshold of 0.70 (Hair et al., 2019). Specifically, high reliability was observed for Subjective Norms (alpha = 0.896, 6 items) and Intention to Self-Protect (alpha = 0.894, 7 items). Furthermore, Individual Attitude (alpha = 0.926), Behavior to Perform Self-Protect (alpha = 0.943), Perceived Behavioral Control (alpha = 0.955), and Self-Efficacy (alpha = 0.964) demonstrated excellent internal reliability.

In general, these results indicate that the revised survey tool is highly reliable and consistent and is therefore prepared to be used for data collection.

Discussion

The main purpose of conducting this pilot study was to perfect the measurement items that were developed for assessing the self-protective behaviors exhibited by teachers against online fraudsters. Unlike evaluating the structural relationships, this assessment was carried out with the objective of ensuring the items are clear, well-structured and construct reliable.

Overall, the psychometric assessments confirm that the adapted items are well-suited for measuring the intended constructs. During content validation, feedback from subject matter experts led to essential linguistic and structural refinements, ensuring the items were clear, contextually relevant, and free of ambiguity. Subsequent statistical testing using Exploratory Factor Analysis (EFA) confirmed strong sampling adequacy across all scales ($KMO > 0.78$; Bartlett's Test $p < 0.001$), supporting the factorability of the item set.

Regarding acceptability and retention of the items, almost all of them showed high acceptability, showing high factor loadings on a single dimension (> 0.60). However, item SBN3 from the Subjective Norms had problems with cross loading having an interval of less than 0.20. To keep the construct pure and to avoid overlapping of concepts, item SBN3 had to be excluded from the construct. In that case, the rest of 6 items in Subjective Norms, along with 7 items each in Individual Attitude, Perceived Behavioral Control, Self-Efficacy, Intention to Self-protect, and Actual Behavior, showed clear factors.

Furthermore, internal consistency reliability testing yielded Cronbach's alpha values between 0.894 and 0.964, far exceeding the standard 0.70 threshold (Hair et al., 2019). These high values demonstrate that the items within each scale measure their respective theoretical constructs with high consistency and minimal error. Ultimately, the successful development and refinement of these items provide a dependable, standardized instrument capable of accurately capturing human behavioral drivers in cybercrime prevention.

Conclusion

This pilot study effectively designed, improved, and validated a structured survey tool specifically suited for measuring self-protection against cyber scams amongst educators. After undergoing the processes of expert content validation and statistical analysis, the questionnaire was successfully transformed into an effective and well-rounded 41-items scale which consists of six fundamental theoretical concepts namely Individual Attitude, Subjective Norms, Perceived Behavioral Control, Self-Efficacy, Intention to Self-Protect, and Behavior to Perform Self-Protect.

Empirical findings reveal that the resulting items have high levels of unidimensionality, separation of factors, and reliability. It has been systematically identified and eliminated problematic items to ensure minimal error and ambiguity in measurements. Thus, the resulting questionnaire becomes a reliable methodology for future research projects on digital resilience and cyber safety behaviors amongst educators.

-
- Acknowledgements:** We would like to express our deepest gratitude to the Ministry of Education Malaysia and the respective State Education Departments for granting permission to conduct this study. Heartfelt thanks are also extended to all the school administrators and teachers who generously gave their time to participate as respondents in this research.
- Funding Statement:** No financial support for the research and/or authorship of this article.
- Conflict of Interest Statement:** It was declared that there is no conflict of interest regarding the publication of this paper. All authors have contributed to this work and approved the final version of the manuscript for submission to the Journal of Information System and Technology Management (JISTM)
- Ethics Statement:** This study was conducted in accordance with ethical research standards. All procedures involving human participants were reviewed and approved by the Human Research Ethics Committee, Universiti Pendidikan Sultan Idris, approval number UPSI/PPPI/PYK/ETIKA(M) /Jld.24(88). Consent was obtained from all participants prior to data collection. Participation was voluntary, and respondents were assured of confidentiality and anonymity. The data collected were used solely for academic purposes.
- Author Contribution Statement:** All authors contributed significantly to this work. N.H. Mohd Yusof carried out the research design, data collection, statistical analysis, and drafted the manuscript. A. Z. A. Abd Razak acted as the primary supervisor, contributing to the conceptual framing, providing critical feedback, and revising the manuscript. All authors read and approved the final manuscript.
-

References

- Abassi, A., Zahedi, F. M., & Chen, Y. (2016). Phishing susceptibility: The good, the bad, and the ugly. 2016 IEEE Conference on Intelligence and Security Informatics, 169-174, Tucson: IEEE.
- Aertsens, J., Mondelaers, K., Verbeke, W., & Buysse, J. (2011). The influence of subjective and objective knowledge on attitude, motivations and consumption of organic food. *British Food Journal*, 113, 1353–1378. <https://doi.org/10.1108/00070701111179988>
- Afida Mastura, M. A., Elistina, A. B., & Syuhaily, O. (2014). Perlindungan pengguna ke arah memperkasakan pengguna di Malaysia. *Persatuan Ekonomi Pengguna dan Keluarga Malaysia*.
- Ahmed, O. S., Nasef, S. A., Zuhir, A., Rawashdeh, A., & Elmagzoub, M. (2021). Teacher's awareness to develop student cyber security : A Case Study Teacher's awareness to develop student cyber security: A Case Study. *Turkish Journal of Computer and Mathematics Education*, 12(May), 5148-5156.
- Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50, 179-211.
- Ajzen, I. (2001), "Attitudes", *Annual Review of Psychology*, Vol. 52, pp. 27-58.
- Aloysius, J. A., Arora, A., & Venkatesh, V. (2019). Shoplifting in mobile checkout settings: cybercrime in retail stores. *Information Technology and People*, 32(5), 1234–1261. <https://doi.org/10.1108/ITP-06-2018-0292>
- Armitage, C. J., Conner, M., Loach, J., & Willetts, D. (1999). Different perceptions of control: Applying an extended theory of planned behavior to legal and illegal drug use. *Basic and Applied Social Psychology*, 21(4), 301–316. https://doi.org/10.1207/S15324834BASP2104_4
- Bandura, A. (1986). The explanatory and predictive scope of self-efficacy theory. *Journal of Social and Clinical Psychology*, 4, 359–373.
- Bandura, A. (1997), *Social Learning Theory*, Prentice Hall, Englewood Cliffs, NJ
- Bandura, A. (1991), "Social cognitive theory of self-regulation", *Organizational Behavior and Human Decision Processes*, Vol. 50 No. 2, pp. 248-287.
- Bellò, B., Mattana, V., and Loi, M. (2018). The power of peers: a new look at the impact of creativity, social context and self-efficacy on entrepreneurial intentions. *Int. J. Entrepreneurial Behav. Res.* 24, 214–233. doi: 10.1108/IJEBR-07-2016-0205
- Bernama, October, 3 (2023). Guru paling ramai dalam kalangan penjawat awam jadi mangsa scammer di Johor - Polis retrieved from Guru paling ramai dalam kalangan penjawat awam jadi mangsa scammer di Johor - Polis, Astro Awani on 20 December 2024.
- Bortne, Ø., Bjørnstad, J., Arnestad, M. N., Tjora, T., & Brønnick, K. K. (2025). Self-efficacy or perceived behavioral control: which influences bank-switching intention? *Journal of Marketing Analytics*. <https://doi.org/10.1057/s41270-025-00408-4>
- Boush, D. M., Friestad, M., & Wright, P. (2015). *Deception in The Marketplace*
- Chang, L. (1994). A psychometric evaluation of four-point and six-point Likert-type scales in relation to reliability and validity. *Applied Psychological Measurement*, 18, 205±215.
- Chatterjee, S., Kar, A. K., Dwivedi, Y. K., & Kizgin, H. (2019). Prevention of cybercrimes in smart cities of India: from a citizen's perspective. *Information Technology and People*, 32(5), 1153–1183. <https://doi.org/10.1108/ITP-05-2018-0251>
- Cho, H., & Lee, J. S. (2015). The influence of self-efficacy, subjective norms, and risk perception on behavioural intentions related to the h1n1 flu pandemic: A comparison between Korea and the US. *Asian Journal of Social Psychology*, 18(4), 311–324. Retrieved from <https://doi.org/10.1111/ajsp.12104>

- Choi, Y., & Suh, K. H. (2022). Verifying the usefulness of the theory of planned behavior model for predicting illegal use of online content: the role of outcome expectancies and social loafing. *BMC Psychology*, 10(1). <https://doi.org/10.1186/s40359-022-00978-3>
- Cohen, L. E., & Felson, M. (1979). Social change and crime rates trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608
- Cox, E. P. (1980). The optimal number of response alternatives for a scale: a review. *Journal of Marketing Research*, 17, 407±422.
- Daud, N. A., Arif, A. M. M., Bakar, E. A., & Osman, S. (2020). Determinants of self-protection practices in online shopping among the students of higher education institutions, Malaysia. *Malaysian Journal of Consumer and Family Economics*, 25(S1), 91–110.
- Dawson K, Gyurcsik N, Culos-Reed N, Brawley L (2001). Perceived control: a construct that bridges theories of motivated behavior. In: Roberts G (ed) *Advances in motivation in sport and exercise*. Human Kinetics, Champaign, IL, pp 321–357
- Department of Statistics Malaysia, April, 28, 2022. Retrieved on November, 7, 2023 from <https://www.dosm.gov.my/portal-main/release-content/ict-use-and-access-by-individuals-and-households-survey-report-malaysia-2021>
- Drew, J. M. (2020). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*, 6(1), 17–33. <https://doi.org/10.1108/JCRPP-12-2019-0070>
- Dunham, D. (2022). Why men are more likely to fall for scams. *The Consumer Lawyer*. <https://theconsumerlawyer.blog/2022/08/26/why-men-are-more-likely-to-fall-for-onlinescams/>. 26 August.
- Ernawati Abdul Wahab, Muhammad Adnan Pitchan & Ali Salman (2023). Pengetahuan, Sikap dan Amalan Masyarakat di Kuala Lumpur Terhadap Kempen Pencegahan Jenayah Penipuan Dalam Talian. *Jurnal Komunikasi: Malaysian Journal of Communication* 39(1): 240-258.
- Felson, M. & Clarke, R. (1998), “Opportunity makes the thief: practical theory for crime prevention”, *Police Research Series Paper 98*, Home Office, London.
- Fidlizan Muhammad, Salwa Amirah Awang, Ahmad Zakirullah Mohamer Shaarani, Mohd Yahya Mohd Hussin, & Nurhanie Mahjom. (2024). Pengaruh Pengetahuan Tip Pencegahan Terhadap Keyakinan Remaja di Pantai Timur bagi Melindungi Diri daripada Jenayah Scam. *Akademika*, 94(2), 179–196. <https://doi.org/10.17576/akad-2024-9402-10>
- Fissel, E. R., & Lee, J. R. (2024). Block? Delete? All of the above? The self-protective behaviors of young adult cyberstalking victims. *Journal of Aggression, Conflict and Peace Research*, 16(4), 301–315. <https://doi.org/10.1108/JACPR-03-2024-0891>
- Ge, Y., Lu, L., Cui, X., Chen, Z., & Qu, W. (2021). How personal characteristics impact phishing susceptibility: The mediating role of mail processing. *Applied Ergonomics* 97: 103526
- Glanz, K., Rimer, B. K., Orleans, C. T., & Viswanath, K. (2015). *Health behavior and health education theory, research, and practice* (4th ed.). USA: Jossey-Bass.
- Hadlington, L. and Chivers, S. (2018), “Segmentation analysis of susceptibility to cybercrime: exploring individual differences in information security awareness and personality factors”, *Policing: A Journal of Policy and Practice*, pp. 1-14, available at: <https://doi.org/10.1093/policing/pay027>
- Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, 31(1), 2–24. <https://doi.org/10.1108/EBR-11-2018-0203>

- Hamsi, A. S., Tobi, S. N., & Masrom, M. 2015. Cybercrime over Internet Love Scams in Malaysia: A Discussion on the Theoretical Perspectives, Connecting Factors and Keys to the Problem”, *Journal of Management Research* 7(2): 169-181.
- Hassan, A., Saleem, I., Anwar, I., and Hussain, S. A. (2020). Entrepreneurial intention of Indian university students: the role of opportunity recognition and entrepreneurship education. *Educ. Train.* 62, 843–861. doi: 10.1108/ET-02-2020-0033
- Huang, H.-Y., Demetriou, S., Banerjee, R., Tuncay, G. S., Gunter, C. A., & Bashir, M. (2020). Smartphone Security Behavioral Scale: A New Psychometric Measurement for Smartphone Security. arXiv Preprint arXiv:2007.01721.
- Jelani, N. S., Salim, S. S., & Zaremohzzabieh, Z. (2021). *Teachers Shape Secondary School Students' Behaviours through the Use of Learning Theories: The Case of Malaysia*. <https://doi.org/10.35631/IJEPC.64200>
- Jusoh, W., & Nizar, W. N. (2022). Online Scams Awareness among Muslim University Studts in Malaysia. *Journal of Islamic, Social, Economics and Development*, 7(43), 50–58. <https://doi.org/10.55573/JISED.074305>
- Khadijah Alavi, Maizatul Haizan Mahbob, & Mohammad Syahrul Azha Soood (2020) Strategi Komunikasi Penjenayah Cinta Siber Terhadap Wanita Profesional. *Jurnal Komunikasi: Malaysian Journal of Communication* 36(3): 296-311.
- Lea, S.E.G. Fischer, P. & Evans, K.M. (2009), “The psychology of scams: provoking and committing errors of judgement, report for the office of fair trading”, available at: www.oft.gov.uk/shared_oftr/reports/consumer_protection/oft1070.pdf
- Lee, W. Y., Tan, C.-S., & Siah, P. C. (2017). *The role of online privacy concern as a mediator between internet self-efficacy and online technical protection privacy behavior*. *Sains Humanika*, 9(3-2), 37–43. <https://doi.org/10.11113/sh.v9n3-2.1271>
- Lee, Y.Y., Gan, C.L. & Liew, T.W. (2022). Phishing victimization among Malaysian young adults: cyber routine activities theory and attitude in information sharing online. *The Journal of Adult Protection* 24(3/4):179-194
- Li, J., Mizerski, D., Lee, A., & Liu, F. (2009). The relationship between attitude and behavior: an empirical study in China. *Asia Pacific Journal of Marketing and Logistics*, 21(2), 232–242. <https://doi.org/10.1108/13555850910950059>
- Majlis Keselamatan Negara, March, 28, 2023. 1065 guru menjadi mangsa scammer. Retrieved from <https://www.mkn.gov.my/web/ms/2023/03/28/1065-guru-jadi-mangsa-scammer/>
- Majlis Keselamatan Negara, March, 6, 2024. Penipuan Melalui Caller Id Spoofing Dalam Macau Scam: Satu Ancaman Digital Terkini retrieved from gov.my/wpcontent/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf
- Malaysian Communications And Multimedia Commission (MCMC) (2020). *Internet User Survey, 2020*. Retrieved 3 Jan 2022 from <https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/IUS-2020-Report.pdf>. ISSN 1823-2523
- McCarthy, B. and Chaudhary, A. (2014), “Rational choice theory”, in Bruinsma, G. and Weisburd, D. (Eds), *Encyclopedia of Criminology and Criminal Justice*, Springer, New York, NY, pp. 4307–4315.
- Messick, D. M. (1999). Alternative logics for decision-making in social settings. *Journal of Economic Behavior and Organisation*, 39(1), 11–28.
- Miller, G. A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review*, 63(2), 81–97. <https://doi.org/10.1037/h0043158>

- Nurul Nadiah, S.T. Elistina, A.B., Afida Mastura, M.A., Saodah, A. & Zuroni, J. (2019). The intensity of consumer education and consumer empowerment among Malaysian consumers. *Malaysian Journal of Consumer and Family Economics*, 22(2), 20-42.
- Olofinbiyi, S. A., & Singh, S. B. (2020). The role and place of covid-19: An opportunistic avenue for exponential world's upsurge in cyber crime. *International Journal of Criminology and Sociology*, 9(January), 221–230. <https://doi.org/10.6000/1929-4409.2020.09.20>
- Parkinson, J., David, P., & Rundle-Thiele, S. (2017). Self-efficacy or perceived behavioural control: Which influences consumers' physical activity and healthful eating behaviour maintenance? *Journal of Consumer Behaviour*, 16(5), 413–423. <https://doi.org/10.1002/cb.1641>
- Pavlou, P.A. & Fygenson, M. (2006). "Understanding and predicting electronic commerce adoption: an extension of the theory of planned behavior", *MIS Quarterly*, Vol. 30 No. 1, pp. 115-143.
- PDRM (Polis Diraja Malaysia). (2023). *Commercial Crime Investigation Department (CCID) – Semak Mule Portal*. <https://ccid.rmp.gov.my>
- Preston, C. C., & Colman, A. M. (2000). Optimal number of response categories in rating scales: reliability, validity, discriminating power, and respondent preferences. *Acta Psychologica*, 104(1), 1–15. [https://doi.org/10.1016/S0001-6918\(00\)00018-6](https://doi.org/10.1016/S0001-6918(00)00018-6)
- Puram, P.K., Kaparathi, M., & Rayaprolu, A.K.H. (2011). Online scams: taking the fun out of the internet. *Indian Journal of Computer Science and Engineering* 2(4): 559-565.
- Pitchan, M. A., Omar, S. Z., & Ghazali, A. H. A. (2019). Cyber security practice among internet users towards cyberbullying, pornography, phishing email and online shopping. *Jurnal Komunikasi: Malaysian Journal of Communication*, 35(3), 212-227. <https://doi.org/10.17576/JKMJC-2019-3503-1>
- Pitchan, M. A., Salman, A., & Arib, N. M. (2025). A Systematic Literature Review on Online Scams: Insights into Digital Literacy, Technological Innovations, and Victimology. *Jurnal Komunikasi: Malaysian Journal of Communication*, 41(1), 107–124. <https://doi.org/10.17576/JKMJC-2025-4101-07>
- Pratama, O., Aladin, R. A., Budiarto, L., & Sundjaja, A. M. (2025). Determinants of security behavior intention in state-owned enterprises: Applying Protection Motivation Theory to phishing emails. *International Journal of Safety and Security Engineering*, 15(3), 443–453. <https://doi.org/10.18280/ijssse.150304>
- Reni, F., & Anggraini, R. (2016). The Role of Perceived Behavioral Control and Subjective Norms to Internal Auditors' Intention in Conveying Unethical Behavior : A Case Study in Indonesia. *Rev. Integr. Bus. Econ. Res.*, 5(2), 141–150.
- Rosley, N. A., Hashim, H., Chow, N. Z., & Chiang, J.-T. ' (2023). *Combating The Macau Scam In Malaysia: Strategies For Mitigation And Resolution From Civil Law And Shari'Ah Perspectives*. 2(2), 30–44. <http://lpssjournal.com>
- Skogan, W.G. (1981), *On Attitudes and Behaviours*, Sage Publications, Beverly Hills.
- Son, J., Jin, B., & George, B. (2013). Consumers' purchase intention toward foreign brand goods. *Management Decision*, 51(2), 434–450. <https://doi.org/10.1108/00251741311301902>
- Turanovic, J.J. & Pratt, T.C. (2014), "Can't stop, won't stop: self-control, risky lifestyles, and repeat victimization", *Journal of Quantitative Criminology*, Vol. 30 No. 1, pp. 29-56.
- Van Steen, T., & Deeleman, J. R. A. (2021). Successful Gamification of Cybersecurity Training. *Cyberpsychology, Behavior, and Social Networking*, 24(9), 593–598. <https://doi.org/10.1089/cyber.2020.0526>

- Van Stralen, M. M., De Vries, H., Mudde, A. N., Bolman, C., & Lechner, L. (2009). Determinants of initiation and maintenance of physical activity among older adults: A literature review. *Health Psychology Review*, 3, 147–207. doi:10.1080/17437190903229462
- Wagner-Huang, W. E. (2020). *Using IBM SPSS Statistics for research methods and social science statistics* (7th ed.). SAGE Publications.
- Warner, L. M., Schütz, B., Wolff, J. K., Parschau, L., Wurm, S., & Schwarzer, R. (2014). Sources of self-efficacy for physical activity. *Health Psychology*, 33(11), 1298
- Wilson, S., Hassan, N.A., Khor, K.K., Sinnappan, S., Abu Bakar, A.R. and Tan, S.A. (2023). A holistic qualitative exploration on the perception of scams, scam techniques and effectiveness of anti-scam campaigns in Malaysia. *Journal of Financial Crime* (in print). <https://doi.org/10.1108/JFC-06-2023-0151>.
- Yoon, C. (2011). Theory of Planned Behavior and Ethics Theory in Digital Piracy: An Integrated Model. *Journal of Business Ethics*, 100(3): 405-417.
- Zahari, A. I., Bilu, R. & Said, J. (2019). The Role of Familiarity, Trust and Awareness Towards Online Fraud, *Journal of Research and Opinion* 6(9): 2470–2480, <https://doi.org/10.15520/jro.v6i9.23>.
- Zainal, N. C., Puad, M. H. M., & Sani, N. F. M. (2023). Moderating effect of self-efficacy in the relationship between knowledge, attitude and environmental behavior of cybersecurity awareness. *Asian Social Science*, 18(1), 55–65. <https://doi.org/10.5539/ass.v18n1p55>
- Zulkifli, Z., Molok, N. N. A., Abd Rahim, N. H., & Talib, S. (2020). Cyber Security Awareness Among Secondary School Students in Malaysia. *Journal of Information Systems and Digital Technologies*, 2(2), 28-41. Retrieved from <https://journals.iium.edu.my/kict/index.php/jisdt/article/view/151>