Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

BEYOND AWARENESS : A CONCEPTUAL FRAMEWORK OF CYBERCRIME SELF-PROTECTION BASED ON TPB AND SELF-EFFICACY THEORY

Nurul Hidayah Mohd Yusof [1*]
Ahmad Zainal Abidin Abd Razak [2]

[1] Universiti Pendidikan Sultan Idris, Perak, Malaysia
(E-mail: p20192001332@siswa.upsi.edu.my)
[2] Universiti Pendidikan Sultan Idris, Perak, Malaysia
(E-mail: ahmad.zainal@fpe.upsi.edu.my)
*Corresponding author: ahmad.zainal@fpe.upsi.edu.my

Article history
Received date : 15-2-2026
Revised date : 16-2-2026
Accepted date : 17-3-2026
Published date : 20-4-2026

To cite this document:
Mohd Yusof, N. H., & Abd Razak, A. Z. A. (2026). Beyond awareness: A conceptual framework of cybercrime self-protection based on TPB and self-efficacy theory. *Journal of Islamic, Social, Economics and Development (JISED),* 11 (82), 27 – 44

Abstract: *The rapid increase in internet penetration in Malaysia has heightened exposure to cybercrime, particularly the Macau Scam, despite ongoing government efforts in legal enforcement and awareness campaigns. While past research has largely emphasised technical and regulatory responses, it has given limited attention to the psychological and behavioural determinants of self-protection. Addressing this gap, this conceptual paper develops a framework that integrates the Theory of Planned Behaviour (TPB) with Self-Efficacy Theory to explain Malaysians' intention to adopt self-protective measures against cybercrime. The proposed framework examines how attitude, subjective norms, and perceived behavioural control interact with self-efficacy to shape individual confidence and willingness to engage in protective behaviours. The integration of self-efficacy offers an important extension to TPB, providing deeper insights into how personal belief and perceived capability influence cybersecurity actions. This combination is particularly relevant in the Malaysian collectivist context, where social influence and perceived competence strongly affect behavioural outcomes. Theoretically, this study extends TPB with self-efficacy, thereby enhancing its explanatory power in cybersecurity behaviour research. In practice, the framework informs policymakers, educators, and law enforcement in designing user-centred strategies that move beyond technical safeguards towards cultivating proactive, self-reliant citizens. By emphasising behavioural empowerment, this study highlights pathways to strengthen Malaysia's national cyber resilience.*

Keywords: *Cybercrime, Macau Scam, Theory of Planned Behavior, Self-Efficacy, Cybersecurity Behavior*

Copyright © Academic Inspired Network - All rights reserved

This work is licensed under CC BY 4.0

Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

Introduction

In today's digital age, internet usage has become essential for communication, financial transactions, and daily activities. In Malaysia, internet usage surged to 96.8% in 2021, especially after the COVID-19 pandemic (DOSM, 2022). However, this heavy reliance on technology has increased exposure to cyber threats, particularly the Macau Scam, which uses fake phone calls, VoIP, and social engineering to deceive victims (Rosley et al., 2023).

Despite strong efforts by the government and cybersecurity agencies, Macau Scam cases continue to rise. In 2023, there were 7,734 reported cases with losses exceeding RM321.1 million (PDRM, 2023). Scammers now employ advanced tactics, including fake caller IDs and AI-generated voices, to deceive victims. This crime affects people from various backgrounds, including retirees, teachers, and professionals (Bernama, 2023).

Current measures, such as cybersecurity laws and awareness campaigns, are insufficient to prevent these scams (MKN, 2024). Many victims underestimate their risk, lack awareness of scams, and fail to detect fraud. Previous studies focused more on technical solutions, but little attention is given to how personal factors like attitude, perceived control, social influence, and self-efficacy affect one's intention to protect themselves (Nurul Nadiah et al., 2019; Chatterjee et al., 2019).

This study aims to explore how these behavioral factors influence Malaysians' citizen intention to adopt self-protective measures against the Macau Scam. It combines the Theory of Planned Behavior (TPB) and Self-Efficacy Theory to create a comprehensive framework in understanding self-protective behaviour among Malaysian's. The research offers practical insights for policymakers, law enforcement, and educators in improving cybersecurity strategies. The paper covers the background, literature review, and conceptual framework, and concludes with key implications and future recommendations.

Literature Review

Issues of Cybercrime in Malaysia

Cybercrime has become a major concern in Malaysia, especially since the COVID-19 pandemic, which accelerated the shift towards online activities and led to a surge in cybercrime cases such as Macau scams, phishing, malware attacks, and identity theft (Aziz et al., 2020; Ismail et al., 2022). A total of RM3.18 billion has been lost to online scams, impacting more than 95,800 victims from 2021 to April 2024 in the country (MyCert2025).

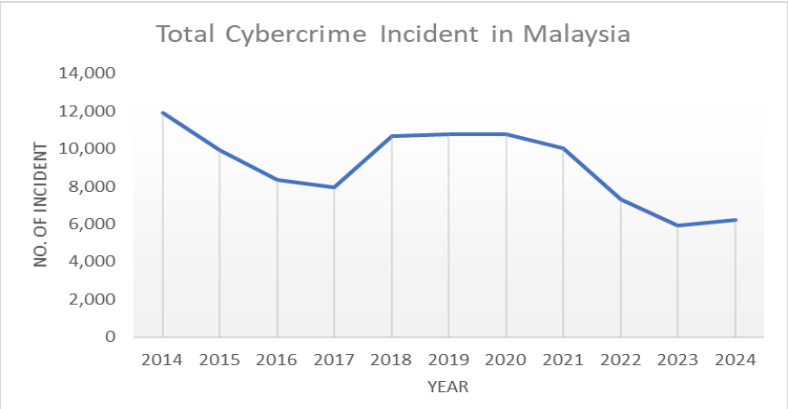

Figure 1: Total Cybercrime Incident in Malaysia

Source: https://www.mycert.org.my/portal/statistics

Copyright © Academic Inspired Network - All rights reserved

This work is licensed under CC BY 4.0

Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

The Malaysian government, through various bodies and agencies, has taken proactive steps to combat cybercrime. This includes implementing legal frameworks, public awareness campaigns, and strengthening enforcement agencies. In Budget 2025, RM10 million was allocated to NACSA to recruit 100 personnel, reflecting the government's serious stance against cyber threats like the Macau Scam (MKN, 2024). Key legislations such as the Consumer Protection Act 1999 (CPA), Personal Data Protection Act 2010 (PDPA), and Electronic Commerce Act 2006 were imposed to reduce consumer vulnerability (Nurul Atikaf et al., 2020), in line with the National Consumer Policy, which promotes self-protection among consumers (Yi & Arif, 2021).

The Malaysia Cyber Security Strategy 2020-2024, with RM1.8 billion funding, further strengthens cyber resilience (MOSTI, 2020). Cybersecurity Malaysia (CSM) supports this via MyCERT, digital forensics, and public education through the CyberSAFE Programme (CyberSecurity Malaysia, 2024). Meanwhile, PDRM, via CCID, operates the Semak Mule Portal and conducts Ops Penipuan (PDRM, 2023). The MCMC enforces content control and campaigns like *"Stop. Think. Connect."* (MCMC, 2023). Malaysia also collaborates internationally with bodies like Interpol, ASEAN, and FIRST (National Security Council Malaysia, 2022). Despite all efforts, cybercrime remains a growing challenge.

Cybercrime continues to present a complex and evolving challenge (Bailey, Kaplan, & Rezek, 2014). Reliance solely on system security measures and governmental interventions has proven insufficient in addressing the growing threat. Individuals must therefore adopt proactive strategies to protect themselves in the digital environment. The need for self-protection is further amplified by contributing factors such as high internet penetration, limited digital literacy, and excessive engagement with social media platforms like Facebook, which collectively heighten the risk of cyber victimization (Hamzah, 2021; Singh et al., 2021).

Understanding cybercrime and its impact

Cybercrime refers to illegal activities conducted using computers, networks, or digital platforms (Hill & Marion, 2016; McGuire et al., 2013). Common forms include phishing, malware, hacking, DDoS, social engineering, and identity theft (Jain & Gupta, 2020). According to the Fraud Triangle Theory (Cressy, 1953), cybercrime arises from three factors: pressure, opportunity, and rationalization, with opportunity being the strongest driver.

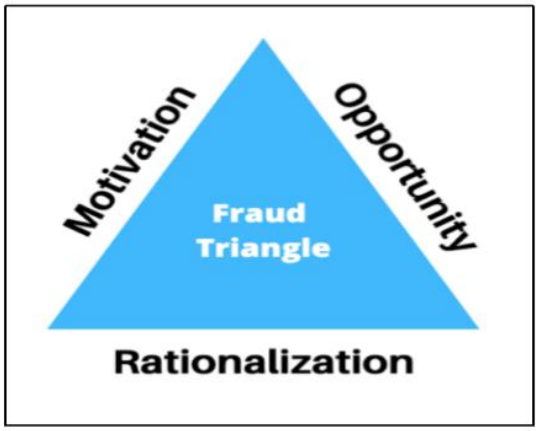

Figure 2: Fraud Triangle

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

Opportunities for cybercrime victimization increase when individuals underestimate their vulnerability to fraud and fail to recognize deceptive communications (Williams et al., 2017; Norris & Brookes, 2021). In Malaysia, studies show that self-protection against cyber risks remains at a moderate level, exposing individuals to greater threats (Nurul Nadiah et al., 2019; Laily Paim et al., 2017). This situation becomes even more challenging in the era of Artificial Intelligence (AI), where scams are more sophisticated and harder to detect.

Money is the main motivation behind cybercrime, driving various illegal activities like ransomware, identity theft, online fraud, and stealing financial data such as credit card or bank account information (Hizam, 2024). For many offenders, cybercrime has become a lucrative source of income, attracting both individuals and organized groups. It offers a quick and easy way to make money without traditional work or investment, often through methods like bank data theft, credit card scams, and digital extortion (Ulo et al., 2024).

The belief of some cyber offenders, perceiving their actions as a way to resist exploitative corporations, unjust financial systems, or corrupt institutions, enables them to rationalize financial theft, data breaches, and digital sabotage as efforts to correct economic injustices. This thaught rationalized the wrong deeds by the fraudster. In some instances, hackers portray themselves as digital vigilantes, claiming to expose unethical practices or redistribute wealth. This narrative of economic retribution is reinforced by global economic inequalities, where individuals from marginalized or disadvantaged regions view cybercrime as a means to address personal or collective grievances (Faisal & Mustafa, 2025).

The presence of these three contributing factors increases the likelihood of cybercrime. This issue should be taken seriously, as cybercrime not only causes financial and emotional harm but also supports wider criminal activities such as money laundering and human trafficking (Roškot et al., 2020). While legal frameworks and cybersecurity systems are already in place, personal factors such as attitudes, self-efficacy, and online behaviour play an important role in determining one's vulnerability to cyber threats.

Role of Human Behavior in Cybercrime Protection

Human behaviour is a critical determinant in mitigating cybercrime victimisation. According to the Theory of Planned Behavior (TPB), an individual's intention to engage in protective behaviour is shaped by three key factors: attitude, subjective norms, and perceived behavioral control (Ajzen, 1991).In parallel, self-efficacy, an individual's belief in their ability to execute specific tasks, significantly influences the adoption of protective online practices (Bandura, 1986). Individuals who possess higher levels of awareness, digital literacy, and confidence are more inclined to engage in self-protective behaviours, while those with limited cybersecurity knowledge or who exhibit overconfidence are more susceptible to cyber threats (Abassi et al., 2016; Lea et al., 2009).

In the Malaysian context, research indicates that many users perceive themselves as safe online but remain unaware of underlying cyber risks, including scams and fraudulent websites (MCMC, 2020; Fidlizan et al., 2024). This behavioural gap is further supported by findings from the 2021 Financial Capability and Inclusion Demand Side (FCI) Survey, which revealed a concerning lack of digital financial literacy among Malaysians. Approximately one in three respondents indicated a willingness to share their bank account passwords or PINs with close friends, reflecting poor awareness of cybersecurity risks. Furthermore, nearly two-thirds of

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

individuals admitted they did not verify website security features before conducting online transactions, such as ensuring the legitimacy of payment pages (Bernama, 2022).

The tendency to create easy-to-remember passwords based on personal information, driven by convenience, increases vulnerability to hacking and account exploitation, particularly those linked to banking institutions, while the disclosure of personal details on social media further facilitates fraudulent activities (Bernama, 2022). Such tendencies significantly increase exposure to financial fraud. Consequently, reliance solely on system-based security and governmental intervention is insufficient. Individuals must take active and responsible steps to protect themselves from cyber threats (Susskind, 2014).

Intention to Self-Protect

Intention to self-protect refers to an individual's readiness and determination to engage in behaviours that prevent cybercrime (Ajzen, 1991). Undoubtedly, technological advancement plays a significant role in mitigating cybercrime risk (Zhao et al., 2012). Adopting protective tools can disrupt unsafe digital environments and reduce fraudulent activity (Drew, 2020). However, the effectiveness of such technology depends mainly on individual intention to utilise them. Without this intention, the benefits of technological progress may remain unrealised, particularly when human negligence persists. In such cases, even the most sophisticated systems can fail to prevent cybercrime (Ye & Potter, 2011).

Based on the Theory of Planned Behaviour (TPB), intention serves as a key predictor of behaviour, shaped by three core components: attitude, subjective norms, and perceived behavioural control (PBC) (Ajzen, 1991). Individuals' intentions and attitudes toward protective tools are often influenced by perceived effectiveness, switching costs, and psychological factors (Ye & Potter, 2011). When individuals perceive risks such as financial loss, identity theft, or fraud, their intention to adopt protective measures tends to increase particularly when accompanied by strong self-efficacy and supportive social norms (Cho & Lee, 2015; Daud et al., 2020). This positive attitude leads to actual protective behaviours (Linan et al., 2011; Holst & Iversen, 2011).

In general, Malaysians demonstrate only a moderate level of self-protection ability when facing online threats (Nurul Nadiah et al., 2019). This pattern can be attributed to cultural values. As a nation rooted in Asian traditions, Malaysia is often characterised by a collectivist culture, where individual behaviours and decisions are shaped by social contexts and interpersonal relationships (Ishii, 2013). In such societies, people tend to conform to the behaviours of their social groups (Yusof & Razak, 2018).

The impact of self-efficacy on behavioural intention tends to be weaker than that observed in more individualistic Western societies (Chen et al., 2006). A collectivist orientation encourages individuals to rely on shared responsibility, collective judgement, and external cues when making behavioural decisions (Earley, 1994; Gibson, 1999). Therefore, in the Malaysian setting, subjective norms play a critical role alongside individual intentions and technological competence. Additionally, social support has been shown to enhance behavioural intention (Gunasegaran et al., 2024). These social influences act as strong drivers of behavioural change, especially in promoting online self-protection.

Beyond the core components of the Theory of Planned Behavior (TPB), this study includes self-efficacy as a key factor in understanding individuals' intentions to protect themselves

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

against cybercrime. Higher levels of self-efficacy are linked to a stronger willingness to face cybersecurity challenges and to take proactive measures to address them (Hassan et al., 2020). Individuals with elevated self-efficacy generally exhibit greater motivation, persistence, and goal-directed behaviour, thereby strengthening the connection between belief in one's capabilities and the intention to act in self-protective ways (Bortne et al., 2025).

Therefore, self-protection against cyber threats is influenced by individual intention which is supported by self-efficacy, social influence and perceived behavioural control in encouraging proactive cybersecurity behaviour. Although technological tools are available their effectiveness ultimately depends on the human factor which is our willingness to adopt and utilise them.

Role of Attitude

Attitude refers to an individual's positive or negative evaluation of a behaviour or situation, and it influences how a person thinks, feels, and acts (Fishbein & Ajzen, 1975; Ajzen, 2011; Bagozzi, 1994a, 1994b). A positive attitude encourages the intention to act, whereas a negative attitude tends to discourage it (Alanazi et al., 2022). According to the Tripartite Model, attitude consists of three components: conative (intention to act), affective (feelings), and cognitive (knowledge and beliefs) (Schiffman & Kanuk, 2004).

In the context of cybercrime, attitude plays a key role in shaping one's intention to protect themselves online. A positive attitude towards cybersecurity encourages protective actions, while a careless or negative attitude may lead to greater risk (Drew, 2020). Individuals who downplay the seriousness of cyber threats are more likely to face security incidents (Constantin et al., 2020). Although having technical knowledge and experience can improve one's attitude and response to cyber risks (Son et al., 2013), overconfidence may increase vulnerability (Martens et al., 2019). People who are familiar with computers and technology are generally better at handling phishing attempts (Pattinson et al., 2012). However, the extent to which IT skills can truly protect against phishing attacks remains uncertain (Broadhurst et al., 2020).

According to Cohen and Felson (1980), individuals who have previously experienced victimisation are more likely to modify their behaviour and adopt more cautious actions in the future. This is because the perception that cybercrime is becoming increasingly common often leads to heightened insecurity (Martens et al., 2019). This sense of vulnerability is especially pronounced among those with limited technological experience, who tend to be more concerned about security and privacy issues (Karim et al., 2020). When individuals perceive greater risk, they tend to adopt more careful, vigilant behaviour (Abassi et al., 2016), leading them to adopt self-protective strategies to reduce their exposure to cybercrime (Leukfeldt, 2014). Ultimately, such behavioural adjustments are made to prevent future victimisation (Turanovic & Pratt, 2014).

However, research has shown that individuals with some knowledge of scams may develop an inflated sense of confidence in their ability to detect fraud and may underestimate their own vulnerability to deception (Martens et al., 2019). This overconfidence, coupled with an indifferent attitude, can lead to risky behavior and an increased likelihood of fraud victimization. Consequently, prior victimization or awareness of cyber threats does not necessarily translate into more effective self-protection. Victims may still fail to take meaningful action to prevent future incidents (Drew, 2020).

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

Drew (2020) also suggests that further investigation is needed to understand why some victims do not change their behavior or show motivation to adopt protective measures. A lack of awareness regarding self-protective strategies, or other influencing factors, may explain this inaction. Therefore, research into self-protective behavior is essential for addressing cybercrime, as risky attitudes may create greater opportunities for fraudulent activities to occur. The goal is not only to protect individuals who have never been victimized, but also to prevent re-victimization among those previously affected. In this study, the researcher aims to examine the relationship between attitude and an individual's intention and behavior to self-protect in the context of cybercrime.

Perceived Behavioral Control (PBC)

Perceived Behavioral Control (PBC) refers to an individual's belief in their ability to perform specific actions, taking into account both internal capabilities and external constraints (Ajzen, 1985). It reflects the general belief that an individual's own actions, rather than external influences such as authority figures or situational opportunities, determine outcomes (Ajzen, 2005).

Unlike self-efficacy, which focuses solely on internal belief, PBC encompasses additional factors such as time, financial means, skills, and social support (Dawson et al., 2021). The availability of resources and information shapes an individual's perception of control over a particular behaviour (Ajzen, 1991; Glanz et al., 2015). These resources, such as self-confidence, comfort, decisiveness, financial capability, and knowledge, can either facilitate or hinder one's intention to engage in a particular behaviour (Glanz et al., 2015; Macovei, 2015).

Individuals with a high level of PBC over these resources are more likely to form the intention to perform the behaviour. However, when the necessary effort or resources are limited or difficult to access, the strength of these intentions may diminish (Ajzen & Fishbein, 2005). This reduction in control perception can negatively impact individuals' motivation and willingness to adopt preventive behaviours, especially when such measures are perceived as challenging to implement (Sommestad et al., 2019).

Limited access to required resources or the perception that cybersecurity practices are complex can reduce individuals' intention, motivation, and willingness to engage in them particularly among those who find tools like password managers or firewall software unfamiliar and more complicated than they truly are (Ajzen & Fishbein, 2005; Sommestad et al., 2019). Although specific actions such as updating antivirus software or backing up data have become routine (Alanazi et al., 2022), various challenges in the digital environment, including low technical literacy, unclear cybersecurity information, and weak self-regulation, can further reduce perceived behavioural control, thereby increasing individuals' vulnerability to online scams (Cross, 2016).

PBC is a significant predictor of online safety practices (Burns & Robert, 2013). Supporting this, Alanazi et al. (2022) found that PBC significantly influences young adults' intentions to engage in cybersecurity practices. A higher level of PBC increases the likelihood of engaging in self-protective behaviors, while lower PBC can serve as a barrier (Parkinson et al., 2017).

Self-Efficacy and Its Influence on Behaviour

Self-efficacy refers to an individual's belief in their ability to perform specific tasks, including self-protection against cybercrime (Bandura, 1994). Although cybersecurity systems and legal

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

frameworks are in place, these mechanisms alone are insufficient to entirely prevent cyberattacks, thereby making personal responsibility a critical element in cyber defence (Afida Mastura et al., 2014). Individuals with high self-efficacy tend to exhibit greater confidence and perseverance in adopting protective behaviours, whereas those with low self-efficacy are more likely to attribute their vulnerability to external factors (Ahmad & Safaria, 2013).

In Malaysia context, studies suggest that the level of self-efficacy in online protection remains moderate, partly influenced by collectivist cultural norms that place greater emphasis on social influence than individual confidence (Ishii, 2013). Lee, Tan, and Siah (2017) found that internet self-efficacy among Malaysian undergraduate students is relatively low, which significantly hinders their engagement in technical privacy protection behaviours. Similarly, Zainal et al. (2023) reported that self-efficacy related to cybersecurity awareness is also low among Malaysian educators and students, further limiting the adoption of self-protective practices.

Nevertheless, previous studies indicate that self-efficacy can be enhanced through targeted interventions such as increasing knowledge, building practical experience, and shifting societal perceptions (Balapour et al., 2019). Moreover, the frequency and severity of cyber threats, when combined with appropriate education and awareness campaigns, have been shown to influence individuals' motivation to adopt protective behaviours (Drew, 2020). Therefore, this study seeks to explore the extent to which self-efficacy influences Malaysians' intentions and behaviours regarding the application of self-protective measures against cyber threats.

.

Theoretical Model

The conceptual framework for this study is based on the Theory of Planned Behavior (TPB), developed by Ajzen (1991), which was expanded from the earlier Theory of Reasoned Action (TRA) model. TPB explains that human behaviour is driven by intention, influenced by three factors: Attitude (personal evaluation of the behaviour), Subjective Norms (social pressure or influence from others), and PBC (perceived ease or difficulty in performing the behaviour). TPB has been widely used in studies related to cybercrime, auditing, and consumer behaviour.

Researchers widely use the Theory of Planned Behaviour (TPB) to understand human intention and behaviour (Ajzen, 2001). Studies such as Aloysius et al. (2019) on cybercrime in retail, Li et al. (2009) on attitude and behaviour regarding enrolment intention in an educational program, and Reni & Anggraini (2016) on auditors' ethical decisions demonstrate TPB's reliability in explaining behaviour. According to TPB, intention is the key predictor of human behavior, influenced by three main factors: attitude**,** subjective norms**,** and perceived behavioral control (PBC) (Aertsens et al., 2011). Attitude reflects a person's positive or negative evaluation of performing a behavior (Pavlou & Fygenson, 2006). Subjective norms refer to the perceived social pressure from important people, such as family and friends, which can shape intention (Ajzen, 1991; Valliere, 2017). PBC is about one's belief in their ability to perform a behaviour if they feel capable; their intention increases (Ajzen, 1991; Bandura, 1997). When these three factors align positively, the likelihood of the behavior happening is higher.

Another theory widely used by previous researchers to understand human behaviour is Bandura's (1997) Self-efficacy Theory. Self-efficacy refers to an individual's belief in their ability to organize and execute actions to achieve a specific goal (Bandura, 1986, 1991). It is crucial because confidence in one's ability helps individuals handle challenges, especially in uncertain situations like cybercrime risks (Bellò et al., 2018). High self-efficacy increases motivation and commitment to take protective actions (Hassan et al., 2020; Bortne et al., 2025).

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

While self-efficacy and PBC may seem similar, they are different. Self-efficacy focuses on internal beliefs in one's ability, often strengthened by experience (Parkinson et al., 2016), whereas PBC concerns external control**,** based on available resources and opportunities (Ajzen, 1991). For example, using security tools boosts PBC by making protective behavior feel more doable (Son et al., 2013). Simply put, self-efficacy is "I believe I can do it"**,** while PBC is "I think I can control the situation to do it." The key difference is the addition of PBC in TPB, which reflects how much control a person feels they have over a behaviour.

Proposed Model

This study extends the Theory of Planned Behavior (TPB) by incorporating the construct of self-efficacy to provide a more comprehensive explanation of individuals' intentions and behaviours in adopting self-protective measures against cybercrime. Prior research has demonstrated that self-efficacy significantly influences technology adoption, particularly in contexts such as e-government, e-commerce, mobile applications, and digital health platforms (Balapour et al., 2019; Fox & Connolly, 2018; Shaw & Sergueeva, 2019). As cybercrime is closely linked to the use of digital technologies, the role of self-efficacy becomes increasingly important in understanding individuals' motivation and capacity to engage in protective behaviours.

Relying solely on the original TPB model may not be sufficient, as individuals with adequate knowledge and awareness may still refrain from taking action due to a lack of confidence in their ability to use security tools effectively (Balapour et al., 2019). In such cases, the availability of technical solutions is rendered ineffective if users do not believe they are capable of utilising them. Within this framework, self-efficacy refers to an individual's internal belief in their competence, while perceived behavioural control (PBC) captures external factors such as resources, support, or obstacles (Parkinson et al., 2017).

Integrating both constructs is expected to offer a more robust understanding of how individuals form intentions and translate them into actual cybersecurity practices. This perspective is further supported by Zainal et al. (2023), who found that self-efficacy plays a moderating role in the relationship between cybersecurity awareness, knowledge, attitudes, and behavior among Malaysian participants. Their findings underscore the value of including self-efficacy in behavioural models, as it enhances the explanatory power of TPB in predicting cybersecurity-related actions. Therefore, this model is proposed for the purposes of this study.

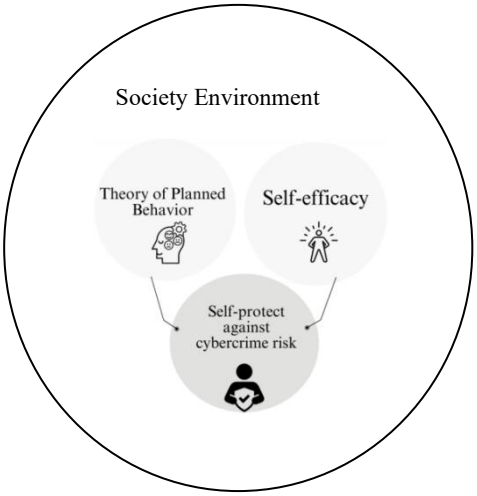

Figure 3: Proposed Model

Copyright © Academic Inspired Network - All rights reserved

This work is licensed under CC BY 4.0

Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

Importance of the Study

This study seeks to provide valuable insights for governments, businesses, financial institutions, and policymakers by examining public attitudes and technology literacy related to self-protective behaviour in reducing cybercrime. Such insights are crucial for identifying the factors that heighten individual vulnerability, thereby enabling more strategic actions to minimise risks and foster a safer digital environment. Although the Theory of Planned Behavior (TPB) has been widely applied across multiple domains (Aloysius et al., 2019; Li et al., 2009), and self-efficacy has been independently shown to predict protective behaviors (Balapour et al., 2019; Fox & Connolly, 2018), their explicit integration remains uncommon. Recent systematic reviews of cybersecurity behaviour research confirm that while TPB and Protection Motivation Theory (PMT) are frequently employed, studies that explicitly integrate TPB with self-efficacy are very limited (Alsharida et al., 2023). Furthermore, findings from the Study of Cybersecurity Self-Efficacy reveal methodological inconsistencies and fragmentation in this field, reinforcing the rarity of models that explicitly combine TPB and self-efficacy (Borgert et al., 2021).

In Malaysia, although TPB and entrepreneurial self-efficacy have been applied in the study of cyber-entrepreneurial intentions (Vafaei-Zadeh et al., 2022), and other works have examined self-efficacy, awareness, or subjective norms in cyber contexts, very limited research has comprehensively tested a framework that fully integrates TPB and self-efficacy to explain self-protective behaviour against cybercrime or scam victimisation among the general public. This gap is even more evident in the Malaysian cybersecurity context, where direct applications of TPB with self-efficacy remain scarce (Zainal et al., 2023).

The uniqueness of this study lies in proposing a conceptual framework that combines TPB and self-efficacy, which is believed to provide a more comprehensive explanation of Malaysians' intentions and behaviours to adopt self-protective measures, particularly in reducing Macau Scam victimization. The findings of this research offer valuable insights for the government in assessing Malaysians' proficiency in managing cybercrime risks.

Understanding the public's level of cybersecurity awareness is essential to designing effective, proactive strategies to address these threats. To cultivate a cyber-savvy culture, it is recommended that cybersecurity knowledge and skills be nurtured from the school level. Pencheva (2020) emphasises the importance of introducing cybersecurity education at the secondary level, while Ahmed et al. (2021) advocate for its integration into the formal school curriculum. Nonetheless, Rahim (2019) identifies several implementation challenges, such as a shortage of expertise, limited funding, and inadequate resources. Therefore, a well-structured strategic plan is necessary to create a safer digital environment for the future.

Conclusion

The growing threat of cybercrime in Malaysia, especially scams such as the Macau Scam, shows the urgent need to understand the behavioural factors that influence individuals' efforts to protect themselves online. While government actions and technological tools are important for addressing these threats, they are not enough without active user involvement.

This study combines the Theory of Planned Behaviour (TPB) with Self-Efficacy Theory to better understand how personal beliefs, attitudes, social influences, and perceived control affect cybersecurity behaviour. Including self-efficacy in the model is especially helpful, as it focuses on an individual's confidence to take effective protective actions. By examining these

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

psychological elements, this study provides policymakers, educators, and cybersecurity professionals with useful insights for designing more targeted awareness programs that better meet the needs of Malaysian users. Encouraging a stronger sense of ability and responsibility among users is essential to building resilience against online threats.

For future research, studies may explore additional psychological or contextual factors such as digital literacy, emotional regulation, or cultural influences that may shape cybersecurity behaviours. Longitudinal studies could also be conducted to observe how these behaviours change over time, especially as technology and cybercrime tactics continue to evolve. Furthermore, expanding the research to include different age groups or professional sectors can offer more specific recommendations for tailored cybersecurity interventions.

Acknowledgements
We would like to thank Universiti Pendidikan Sultan Idris for their helpful feedback and support.

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0

Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

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. https://doi.org/10.1109/isi.2016.7745462

Ahmad, A. & Safaria, T. (2013). Effect of self-efficacy on students' academic perform. *Journal of Educational, Health and Community Psychology*, 2(1), 22-29.

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. https://doi.org/10.17762/turcomat.v12i10.5297

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*.

Ajzen, I. (1985). From intentions to actions: a theory of planned behaviour, in Kuhl, J. et al. (Ed.), Action-Control: From Cognition to Behaviour, Springer, Heidelberg, pp. 11-39. https://doi.org/10.1007/978-3-642-69746-3_2

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50*, 179-211. https://doi.org/10.1016/0749-5978(91)90020-t

Ajzen, I. (2005). *Attitudes, personality, and behavior (2nd).* Maidenhead, UK: Open University Press.

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & Health*, *26*, 1113-1127. https://doi.org/10.1080/08870446.2011.613995

Ajzen, I. (2001). Nature and operation of attitudes. *Annual review of psychology*, *52*(1), 27-58. https://doi.org/10.1146/annurev.psych.52.1.27

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, *136*. https://doi.org/10.1016/j.chb.2022.107376

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

Alsharida, R. A., Al-Rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society, 73*, Article 102258. https://doi.org/10.1016/j.techsoc.2023.102258

Aziz, N. A.; Othman, Jamal; Lugova Halyna & Suleiman, A. (2020). Malaysia's approach in handling COVID-19 onslaught: Report on the Movement Control Order (MCO) and targeted screening to reduce community infection rate and impact on public health and economy. *Journal of Infection and Public Health*, *14(4)*, 337–339. https://doi.org/10.1016/j.jiph.2020.08.007

Bagozzi, R.P. (Ed.) (1994a), *Principles of Marketing Research*, Blackwell Business, Oxford.

Bagozzi, R.P. (Ed.) (1994b), *Advanced Methods of Marketing Research*, Blackwell Business, Oxford.

Balapour, A., Reychav, I., Sabherwal, R., & Azuri, J. (2019). Mobile technology identity and self-efficacy: Implications for the adoption of clinically supported mobile health apps. *International Journal of Information Management*, *49*(October 2018), 58–68. https://doi.org/10.1016/j.ijinfomgt.2019.03.005

Copyright © Academic Inspired Network - All rights reserved

This work is licensed under CC BY 4.0

Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, 84(2), 191-215. https://doi.org/10.1037/0033-295x.84.2.191

Bandura, A. (1986). The Explanatory And Predictive Scope Of Self-Efficacy Theory. *Journal of Social and Clinical Psychology*, 4, 359– 373. https://doi.org/10.1521/jscp.1986.4.3.359

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. https://doi.org/10.1108/ijebr-07-2016-0205

Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2020). Phishing risks in a university student community. *Trends and Issues in Crime and Criminal Justice*, *2*(587), 4–23. https://doi.org/10.52922/ti04251

Bernama. (2022, October 4). Sharing of bank account password, PIN number will lead to fraud cases, mule accounts - BNM. https://international.astroawani.com/malaysia-news/sharing-bank-account-password-pin-number-will-lead-fraud-cases-mule-accounts-bnm-384061

Bernama. (2022, Disember 27). Smartphone: one wrong click could wipe out your savings *Bernama.com.https://www. Bernama.com/en/news.php?id=2151325&utm_source=chatgpt.com*

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., Bjornestad, 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

Borgert, N., Jansen, L., Böse, I., Friedauer, J., Sasse, M. A., & Elson, M. (2024). Self-Efficacy and Security Behavior: Results from a Systematic Review of Research Methods. In *Proceedings of the CHI Conference on Human Factors in Computing Systems 2024* (pp. 1-32). ACM. https://doi.org/10.1145/3613904.3642432

Burns, S., & Roberts, L. (2013). Applying the Theory of Planned Behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety*, *15*(1), 48–64. https://doi.org/10.1057/cpcs.2012.13

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

Chen, S. X., Chan, W., Bond, M. H. & Stewart, S. M. (2006). The effects of self-efficacy and relationship harmony on depression across cultures. *Journal of Cross-Cultural Psychology*, 37, 643–658. https://doi.org/10.1177/0022022106292075

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

Cohen, L. E., & Felson, M. (1979). Social change and crime rates trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608. https://doi.org/10.2307/2094589

Constantin, M., Borţea, A. N., & Costovici, D. A. (2020). Risks and Vulnerabilities in Digital Public Services. Threat of Cyberterrorism Vs Romania's Cybersecurity Strategy. HOLISTICA *Journal of Business and Public Administration*, 11(2), 74-84. https://doi.org/10.2478/hjbpa-2020-0020

Cressey, D. R., (1953). *Other people's money; a study of the social psychology of embezzlement.* Free Press. https://doi.org/10.2307/2087778

Copyright © Academic Inspired Network - All rights reserved

This work is licensed under CC BY 4.0

Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

Cross, C. (2016). Using financial intelligence to target online fraud victimization: Applying a tertiary prevention perspective. *Criminal Justice Studies*, 29(2), 124–145. https://doi.org/10.1080/1478601x.2016.1170278

CyberSecurity Malaysia. (2024). *Cyber999 – Report Cyber Incidents*. https://www.cybersecurity.my

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.

Department of Statistics Malaysia (DOSM). (2023). *Crime Statistics Malaysia 2023*. Retrieved from https://www.dosm.gov.my

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

Earley, P. C. (1994). Self or group? Cultural effects of training on self-efficacy and performance. *Administrative Science Quarterly*, 39, 89–117. https://doi.org/10.2307/2393495

Faisal, D., & Mustafa, K. (2025, March). *Neutralization Techniques and Economic Retribution: The Justification of Cybercrime*. https://doi.org/10.13140/RG.2.2.20385.52326

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

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley. https://doi.org/10.2307/2065853

Fox, G., & Connolly, R. (2018). Mobile health technology adoption across generations: Narrowing the digital divide. *Information Systems Journal*, 28(6), 995–1019. https://doi.org/10.1111/isj.12179

Gibson, C. B. (1999). Do they do what they believe they can? Group efficacy and group effectiveness across tasks and cultures. *Academy of Management Journal*, 42, 138–152. https://doi.org/10.2307/257089

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. https://doi.org/10.1177/109019819101800409

Gunasegaran, H., Islam, G. M. N., Yusof, N. H. M., & Bakar, K. A. (2024). Extended Theory of Planned Behavior with Push-Pull Factors: A Conceptual Framework on Housewives Entrepreneurial Intention. International Journal of Academic Research in Business and Social Sciences. https://doi.org/10.6007/ijarbss/v14-i10/22419

Hamzah, I. S. (2021). Personal security on facebook: Threats and solutions. *Jurnal Komunikasi: Malaysian Journal of Communication*, *37*(1), 379–395. https://doi.org/10.17576/JKMJC-2021-3701-22

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. https://doi.org/10.1108/ET-02-2020-0033.

Hill, J. B., & Marion, N. E. (2016). *Introduction to cybercrime: computer crimes, laws, and policing in the 21st century*. Bloomsbury Publishing USA.

Copyright © Academic Inspired Network - All rights reserved

This work is licensed under CC BY 4.0

Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

Hizam, A. (2024). Types of cybercrimes and digital forensic investigation tools: A review. Al-Andalus Journal, 19(11), 7–24.

Holst, A., & Iversen, J. M. (2011). An application of a revised theory of planned behavior: Predicting the intention to use personal care products without endocrine disrupting chemicals. *Copenhagen Business School*.

Ishii, K. (2013). Culture and the mode of thought: A review. *Asian Journal of Social Psychology*, 16, 123–132. https://doi.org/10.1111/ajsp.12011

Ismail, N., Ramlee, Z., & Abas, A. (2022). THE LEGAL PROOF OF MACAU SCAM IN MALAYSIA. Malaysian *Journal of Syariah and Law* | بماليزيا والقانو الشريعة مجلة |, 10(1), 23–33. www.mjsl.usim.edu.my

Jain, A., & Gupta, N. (2020). Cyber Crime. *National Journal of Cyber Security Law*, 2(2), 152-158.

Kanwal, M., Ul, Q., Zahoor, A., Mussarat, S., Khadam, N., & Zainab, M. (2022). Cybercrime: An emerging global challenge for the states. *Global Partners in Education Journal*, 10(1), 47–60.

Karim, M.W.,Haque, A., Ulfy, M. A., & Anis, Z. (2020). Factors Influencing the Use of E-wallet as a Payment Method among Malaysian Young Adults. *Journal of International Business and Management*, (February). https://doi.org/10.37227/jibm-2020-2-21

Lai, P. C. (2016). Design and security impact on consumers' intention to use single platform e-payment. *Interdisciplinary Information Sciences*, 22(1), 111–122. https://doi.org/10.4036/iis.2016.111

Laily Paim, Shuhaily Osman & Sharifah Azizah Haron. (2017). Pembentukan indeks pendayaupayaan pengguna Malaysia. *Malaysian Journal of Consumer and Family Economics*, 20(2), 81-105.

Leukfeldt, E.R. (2018). Coping with cybercrime victimization: an exploratory study into impact and change, *Journal of Qualitative Criminal Justice & Criminology*, Vol. 2 No. 2, pp. 205-228.

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_oft/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

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

Liñán, F., Urbano, D., & Guerrero, M. (2011). Regional variations in entrepreneurial cognitions: Start-up intentions of university students in Spain. *Entrepreneurship and regional development*, *23*(3-4), 187-215. https://doi.org/10.1080/08985620903233929

Macovei, O. I. (2015). Applying the theory of planned behavior in predicting proenvironmental behaviour: The case of energy conservation. *Acta Universitatis Danubius. Œconomica*, *11*(4), 15-32.

Malaysian Communications and Multimedia Commission (MCMC). (2023). *CyberSAFE Programme*. https://www.cybersafe.my

Majlis Keselamatan Negara, October, 20,2024. Belajawan 2025: Pemerkasaan Agensi Keselamatan Siber Negara (NACSA), MKN. Retrieved from https://www.mkn.gov.my/web/ms/2024/10/20/belanjawan-2025-pemerkasaan-agensi-keselamatan-siber-negara-nacsa-mkn/(Assessed on 21 November 2024).

Copyright © Academic Inspired Network - All rights reserved

This work is licensed under CC BY 4.0

Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

Malaysian Communications and Multimedia Commission (MCMC) (2020*). Internet User Survey, 2020*. Retreived 3 Jan 2022 from https://www.mcmc.gov.my/skmmgov my/media/ General/pdf/IUS-2020-Report.pdf. ISSN 1823-2523

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, *92*, 139-150. ttps://doi.org/10.1016/j.chb.2018.11.002

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, *75*, 1-35.

MKN. (2024, October 20). *Belanjawan 2025: RM10 juta diperuntukkan kepada NACSA*. National Security Council Malaysia.

MOSTI. (2020). *Malaysia Cyber Security Strategy (MCSS) 2020–2024*. National Cyber Security Agency (NACSA). https://www.nacsa.gov.my

New Straits Times. (2023, November 2). Malaysia third in the world for time spent on internet. Retrieved from https://www.nst.com.my

National Security Council Malaysia. (2022). *Malaysia's Role in ASEAN Cybersecurity Cooperation*. https://www.nsc.gov.my

Norris, G., & Brookes, A. (2021). Personality, Emotion And Individual Differences in Response To Online Fraud. *Personality and Individual Differences,* 169(1), 109-847. https://doi.org/10.1016/j.paid.2020.109847

Nurul Atikaf, D., Afida Mastura, M.A., Elistina, A.B., Syuhaily, O. (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.

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.

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

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*, 20(1), 18-28. https://doi.org/10.1108/09685221211219173

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS quarterly*, 115-143. https://doi.org/10.2307/25148720

PDRM (Polis Diraja Malaysia). (2023). *Commercial Crime Investigation Department (CCID) – Semak Mule Portal*. https://ccid.rmp.gov.my

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education.IEEE Security and Privacy. https://doi.org/10.1109/MSEC.2020.2969409

Rahim, N. H. A., Hamid, S., & Kiah, M. L. M. (2019). Enhancement of Cybersecurity Awareness Program on Personal Data. Malaysian Journal of Computer Science, 32(3), 221-245. https://doi.org/10.22452/mjcs.vol32no3.4

Roškot, M., Wanasika, I., & Kreckova Kroupova, Z. (2020). Cybercrime in Europe: surprising results of an expensive lapse. *Journal of Business Strategy*. https://doi.org/10.1108/JBS-12-2019-023

Copyright © Academic Inspired Network - All rights reserved

This work is licensed under CC BY 4.0

Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

Rosley, A., Mohamed, N., Ismail, N. A., & Ibrahim, A. (2023). Strategy for mitigation and resolution of Macau scam in Syariah and civil law. *Malaysian Journal of Syariah and Law*, 11(1), 50–65. https://doi.org/10.33102/mjsl.vol11no1.510

Schiffman, L.G. & Kanuk, L.L. (2004), *Consumer Behaviour*, 8th ed., Pearson Education, Upper Saddle River, NY.

Shaw, N., & Sergueeva, K. (2019). The non-monetary benefits of mobile commerce: Extending UTAUT2 with perceived value. *International Journal of Information Management*, 45,44–55. https://doi.org/10.1016/j.ijinfomgt.2018.10.024

Singh, M. M., Frank, R., & Wan Zainon, W. M. N. (2021). Cyber-criminology defense in pervasive environment: A study of cybercrimes in Malaysia. *Bulletin of Electrical Engineering and Informatics*, *10*(3), 1658–1668. https://doi.org/10.11591/eei.v10i3.3028

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information and Computer Security*, *23*(2), 200–217. https://doi.org/10.1108/ICS-04-2014-0025

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

Susskind, N. G. (2014). Cybersecurity compliance and risk management strategies: What directors, officers, and managers need to know. *NYUJL & Bus.*, *11*, 573.

Turanovic, J. J., & Pratt, T. C. (2014). "Can't stop, won't stop": Self-control, risky lifestyles, and repeat victimization. *Journal of quantitative criminology*, *30*(1), 29-56. https://doi.org/10.1007/s10940-012-9188-4

Ulo, E., Obire, M. O., Akpumuvie, C. E., & Ogbeide, H. E. (2024). Motivational Analysis Behind Cyber Criminal Behaviour in Nigeria. European Journal of Arts, Humanities and Social Sciences, 1(5), 61-71. https://doi.org/10.59324/ejahss.2024.1(5).03

Vafaei-Zadeh, A., Ganesan, V., Hanifah, H., Teoh, A. P., & Ramayah, T. (2022). *Cyber-entrepreneurial intention among students in Public Universities: Evidence from an Emerging Country*. *Education and Information Technologies, 28*(5), 5385-5419. https://doi.org/10.1007/s10639-022-11362-4

Valliere, D. (2017). Belief patterns of entrepreneurship: exploring cross-cultural logics. *International Journal of Entrepreneurial Behaviour and Research*, *23*(2), 245–266. https://doi.org/10.1108/IJEBR-12-2015-0297

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior,* 72(1), 412-421. https://doi.org/10.1016/j.chb.2017.03.002

Ye, C., & Potter, R. (2011). The role of habit in post-adoption switching of personal information technologies: An empirical investigation. *Communications of the Association for Information Systems*, *28*(1), 35. https://doi.org/10.17705/1cais.02835

Yi, T. J. Arif, A. M. M. (2021). The Relationship Between Self-Efficacy, Awareness And Subjective Norms with Online Shopping Self-Protection Practices Among Chinese Consumers in Seremban , Negeri Sembilan norms. *Jurnal Pengguna Malaysia*, *36*, 81–92.

Younies, H., & Al-Tawil, K. (2020). The impact of digital transformation on cybercrime. *International Journal of Computer Science and Network Security*, 20(4), 198–204.

Yusof, N. H. M., Razak, A.Z. A. (2018). Customer Intention to Commit Motor Insurance Fraud: A Literature Review (2018) – International Business Education Journal (IBEJ) volume 11, issue number 1, 2018, 40-48 (ISSN 1985 2126). https://doi.org/:10.37134/ibej.vol11.1.4.2018

Copyright © Academic Inspired Network - All rights reserved

This work is licensed under CC BY 4.0

Volume: 11 Issues: 82 Special Issue [April, 2026] pp. 27 – 44
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: academicinspired.com/jised
DOI: 10.55573/JISED.118203

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

Zhao, F., José Scavarda, A., & Waxin, M. F. (2012). Key issues and challenges in e-government development: An integrative case study of the number one eCity in the Arab world. *Information Technology & People*, *25*(4), 395-422. https://doi.org/10.1108/09593841211278794

Copyright © Academic Inspired Network
- All rights reserved

This work is licensed under
CC BY 4.0