JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGY
https://e-journal.uum.edu.my/index.php/jict

How to cite this article:
Mat Aji, Z., Wan Yaacob, W. M. Y., & Zakaria, N. H. (2026). Cybercognition as emerging determinant in Protection Motivation Theory: Toward explaining secure intention behaviour in online gaming among adolescents. *Journal of Information and Communication Technology*, *25*(2), 122-140. https://doi.org/10.32890/jict2026.25.2.6

Cybercognition as Emerging Determinant in Protection Motivation Theory: Toward Explaining Secure Intention Behaviour in Online Gaming among Adolescents

[1]Zahurin Mat Aji, [2]Wan Mohd Yusoff Wan Yaacob & [3]Nur Haryani Zakaria
[1&3]School of Computing, Universiti Utara Malaysia, Malaysia
[2]Department of IT and Communication, Politeknik Tuanku Syed Sirajuddin, Malaysia

[*1]zahurin@uum.edu.my
[2]wanmohdyusoff@ptss.edu.my
[3]haryani@uum.edu.my
*Corresponding author

Received: 5/5/2025 Revised: 26/6/2025 Accepted: 5/7/2025 Published: 30/4/2026

ABSTRACT

The increasing prevalence of online gaming among adolescents has heightened the need to understand the psychological factors that influence secure online behaviour. Protection Motivation Theory (PMT) is limited in its ability to explain technology-related behaviours because it primarily focuses on conscious, rational decision-making driven by threat and coping appraisals. While PMT is widely used to explain individuals' protective intentions, emerging cognitive constructs such as cybercognition, which refers to the skills, heuristics, and cognitive dispositions that shape online decision-making, remain underexplored within this framework. This study investigates cybercognition as a potential determinant of the secure intention behaviour model, which refers to self-instructions to perform actions to attain secure behaviour in an online gaming environment. Using a simple random survey of adolescent gamers, the research examines how cybercognitive abilities interact with PMT components, including perceived severity, vulnerability, self-efficacy and response efficacy, to predict intentions to engage in secure online practices. Structural equation modelling reveals that cybercognition significantly enhances the explanatory power of PMT by influencing both threat appraisal and coping appraisal pathways. Findings suggest that adolescents with higher cybercognitive awareness are more likely to adopt protective behaviours while gaming. The study contributes to theoretical advancements in PMT by integrating cybercognition and offers practical implications for designing targeted digital safety interventions and educational programs for the youth.

Keywords: Behavioural addiction, cyber threat, online game addiction, Protection Motivation Theory, secure intention behaviour.

INTRODUCTION

The COVID-19 pandemic, which began in late 2019 and persisted for several years, brought significant transformations to everyday life. Its far-reaching disruptions compelled individuals to reassess their approaches to work, social interaction and leisure activities. Among the most notable changes was the heightened reliance on digital technologies, particularly mobile applications and online games, as people adapted to new living patterns under prolonged restrictions (Nawaz et al., 2024; Gregersen et al., 2023; Norman et al., 2023). With the enforcement of lockdowns and physical distancing measures, smartphones became the primary medium for conducting work, accessing education, maintaining social connections, and engaging in entertainment (Nawaz et al., 2024; Newman, 2022). Consequently, people became increasingly reliant on their mobile devices, blurring the boundaries between virtual and real-life experiences. Mobile apps and games offer both connections and escape from the challenges of the pandemic. Furthermore, online gaming has become a popular outlet for stress relief during and after the pandemic. Games such as PUBG, Fortnite and Mobile Legends allow individuals to immerse themselves in captivating virtual worlds and foster social bonds with friends and strangers (Purwaningsih & Nurmala, 2021; Tomicic et al., 2019).

However, this increased engagement with online games also raised concerns about behavioural patterns. As gaming became embedded in daily routines, some individuals began to exhibit signs of online game addiction (OGA), a problematic, excessive and compulsive use of games that impairs functioning across multiple areas of life (Norman et al., 2023; Xu et al., 2012). These behavioural changes can have stronger psychological effects, with users becoming more introverted, violent or losing interest in their surroundings. Moreover, their academic and occupational performance may also be affected if they cannot tolerate their gaming habits (Purwaningsih & Nurmala, 2021; Shamsudin et al., 2019). Eventually, these gamers began spending more time playing online due to the free time they had while staying at home during lockdowns, until it became an irresistible distraction (Wibowo & Fransco, 2021). This addiction can have far-reaching consequences on the individual and societal levels. In the context of the post-pandemic effects, it could worsen the already stressful situation. Even though they believed they would escape the problematic impacts, the gamers found only temporary relief, without solving the main issues (Newman, 2022; Purwaningsih & Nurmala, 2021; Julisia & Nursalim, 2025).

Since the early 2000s, scholarly interest in the multifaceted issues surrounding online game addiction has expanded substantially. Most of this research focuses on areas related to psychological and physical well-being, as well as employee and general user performance (Shamsudin et al., 2019; Türker & Çakmak, 2019; Goncalves et al., 2018). Recently, the focus has been on examining the cybersecurity implications of OGA (Conner & Norman, 2022; Pollini et al., 2022; Jenkins et al., 2021; Yadav, 2021; Durak, 2019; Aivazpour & Rao, 2018; Hadlington, 2017b). Hadlington (2017b) deals specifically with adolescents whose impulsive behaviour, driven by an obsession that leads to careless actions and increased vulnerability to cyber threats. Conner and Norman (2022) and Jenkins et al. (2021) suggested that intention is the most influential factor in shaping one's behaviour and attitude towards cybersecurity. To address this emerging issue, it is essential to develop a model grounded in a theoretical lens that explains the behavioural factors shaping security behavioural intention and influencing individuals' reactions and decision-making.

Several researchers have adopted the Protection Motivation Theory (PMT) in security behaviour studies by eliciting fear to deter behaviour in response to cyber threats that pose danger or harm (Jansen & Schaik, 2018). However, the inefficiency of PMT's fear appeal construct may reduce fear incautiously due to its influence on addictive behaviour (Simpson, 2017). Consequently, fear appeal contributes to individuals' inability to engage in self-protection in decision-making and is therefore not suitable for implementation solely in studies on addictive behaviour (Simpson, 2017; Lowry, 2023; Kiran et al., 2025).

Accordingly, this study advances a revised application of PMT by incorporating cybercognition to more effectively explain secure behavioural intentions among adolescents exhibiting online gaming addiction (OGA). In line with this perspective, the study introduces the Secure Intention Behaviour (SIB) model, specifically designed to account for the unique cognitive and behavioural characteristics of adolescents with OGA. The study's objectives are threefold: (i) to identify the key factors influencing SIB in this population, (ii) to develop a conceptual SIB model that integrates these determinants, and (iii) to validate the model through hypothesis testing and expert evaluation. The paper begins with a review of relevant literature, followed by a detailed description of the conceptual framework and the research methodology, and subsequently presents the findings derived from the analysis. It is followed by a discussion of the theoretical and practical implications, with the paper concluding by summarising the contributions and outlining directions for future research.

RELATED STUDIES

OGA among Adolescents

OGA has emerged as a significant issue due to the unique characteristics and widespread availability of online gaming platforms. OGA refers to problematic, excessive and compulsive usage of online gaming that causes a substantial impairment to function in multiple life domains over a long duration (Purwaningsih & Nurmala, 2021; Xu et al., 2012). The online gaming environment is designed to be highly engaging and rewarding, often featuring in-game achievements and social interactions. This combination of immediate gratification and continuous reinforcement can make games habit-forming, leading to excessive play. Following the COVID-19 pandemic, a surge in gaming activity contributed to accelerated digital growth, particularly in mobile phone and Internet usage. Meltwater Global Digital Growth Report 2023 mentioned that the digital user population increased by approximately 67 million (0.8%) between January and December. Among this population, mobile phone users accounted for 168 million (3.2%), active social media users for 137 million (3.0%), and internet users for 98 million (1.9%). Of the 346 million Internet users, approximately 76% engage in online gaming on various platforms, including computers and mobile devices.

The surge in digital engagement has paralleled a growing incidence of OGA among adolescents, a demographic particularly susceptible to the immersive, highly reinforcing nature of online games (Bekir & Çelik, 2019). Adolescents, defined by the World Health Organisation (WHO) as individuals aged 10 to 19, are more likely to develop compulsive gaming habits due to limited digital literacy and still-developing cognitive skills. Spano (2004) categorises adolescence into early (10–14 years), middle (15–16 years) and late (17–19 years) stages, each with distinct developmental characteristics. Adolescents are at risk of becoming victims of cyber threats as they are still developing their digital literacy and critical thinking skills. Their limited experience in the online world can make it challenging to recognise

and respond to cyber threats effectively (Novrialdy & Atyarizal, 2019; Xu et al., 2012). They also often experience peer pressure and a desire to fit in with their social groups. This drive can lead them to engage in insecure behaviours, such as sharing personal information, participating in online challenges, or accepting requests from strangers.

The prominent characteristics of late adolescents involve the transition to adulthood, including becoming independent, forming identity, and acquiring other essential life skills. Thus, this study focuses on late adolescents, who are most susceptible to the influences of their digital environment, including online gaming (Bekir & Çelik, 2019). Studies related to the biopsychosocial framework identified several main components of addiction that include mood modification, salience, tolerance, conflict, relapse, withdrawal and problems (Lemmens et al., 2009; Griffiths, 2005). These elements reinforced compulsive behaviour, making it difficult for individuals to moderate gaming without targeted intervention. Fear-appeal-based strategies, once effective at discouraging risky online behaviour, have gradually lost their effectiveness in addressing security concerns (Stubbendorff & Stevenson, 2020). The relationship between intentional behaviour and OGA is also multifaceted, encompassing an individual's planned actions or strategies to engage in specific activities, guided by prior knowledge (Jenkins et al., 2021; Pratama et al., 2025).

SIB within Online Gaming Setting

Ajzen (1985) described intention as a person's internal willingness or commitment to plan and engage in behaviours that may eventually become habitual. Pahnila et al. (2013) further emphasised that intention is a key determinant of behaviour change, while Shropshire et al. (2015) defined intention as a mental state representing a commitment to practising secure behaviour and performing related actions. Similarly, SIB refers to self-instructions and deliberate actions aimed at achieving safe conduct in an online environment (Sheeran & Webb, 2016). SIB is characterised by purposeful, goal-directed actions that align with ethical standards and safety measures, ensuring responsible decision-making. SIB emphasises the actual behaviour required to maintain digital well-being, including setting boundaries, managing time, and prioritising real-life responsibilities over online gaming. However, when intention behaviour was compromised by addictive behaviour, individuals may fail to regulate their gaming habits, leading to excessive gameplay and potential OGA (Conner & Norman, 2022). As addiction intensified, the ability to follow through on secure intentions weakened.

In the context of cybersecurity and online gaming, SIB plays a critical role in protecting individuals from potential threats, such as phishing attacks, in which malicious actors attempt to deceive users into revealing sensitive information. Adolescents exhibiting strong SIB are more likely to recognise such threats, exercise caution, and engage in protective behaviours—such as avoiding suspicious links, verifying sources, and practising secure account management. Conversely, a lack of SIB can increase vulnerability to OGA and exposure to cybersecurity risks, including falling victim to phishing, which may result in compromised personal information or unsafe gaming practices.

Hence, it becomes essential to enhance the PMT by incorporating cognitive capabilities, such as cybercognition, to strengthen intention-behaviour links and support informed decision-making in digital environments (Hadlington, 2017a). Moreover, as fear appeal was found ineffective in mitigating cyber threats, cybercognition is deemed necessary for developing SIB in the context of OGA among adolescents.

OGA and SIB among Adolescents

Alrobai et al. (2014) developed persuasive methods to combat this addiction by implementing an online peer-group approach. This solution was verified by Kesici and Tunç (2018) through their study related to the OGA severity among university students, while Baturay and Toker's (2019) and Lemmens and Hendriks' (2016) concluded that it was highly likely that online games with strong interactive relationships, emphasising various genres, would exhibit addictive characteristics. These findings indicated that the dynamic game design contributed to the addictive behaviour among those adolescents struggling with academic and social transitions. Bekir and Çelik (2019) demonstrated that these adolescents had the highest propensity for risk-taking and reward-seeking, contributing to OGA. Their results were extracted using the combination of three validated scales: sensation seeking, OGA and basic psychological needs. Schneider et al. (2017) added that late adolescents are also prone to OGA because they are no longer closely monitored by their parents, as they have been living separately from their parents' houses due to academic institutions' requirements and other reasons. Collectively, these findings show that developmental, psychological and social factors intersect to heighten the risk of OGA among late adolescents, especially in higher education environments where autonomy and stress levels are elevated.

Intentional behaviour examines the likelihood of translating intentions into actions, encompassing both the level of behaviour and the degree of commitment. While many behaviours are habitual and triggered automatically by situational cues, forming intentions is crucial for achieving long-term cybersecurity goals, as noted by Jenkins et al. (2021). Intention behaviour examines the likelihood of translating intentions into actions, encompassing both the level of behaviour and the degree of commitment. While many behaviours are habitual and triggered automatically by situational cues, forming intentions is crucial for achieving long-term cybersecurity goals, as noted by Jenkins et al. (2021). Yoon and Kim (2013) noted that such variability complicated efforts to generalise findings across contexts. In light of this, Yadav (2021) argued for a more rigorous examination of the relationship between intention and secure behaviour in digital settings.

There is a significant gap in understanding the reciprocal relationship between OGA and behavioural intentions. Examining this dynamic can help establish a more robust theoretical foundation for cybersecurity research focused on adolescents. This study addresses these gaps by investigating how late adolescents' developmental needs and gaming habits influence their capacity for SIB. In doing so, it advances the theoretical understanding of cybersecurity behaviour and informs strategies to promote digital well-being among adolescents in increasingly connected online environments.

Cybercognition

Cybercognition refers to the mental processes involved in acquiring knowledge and performing cognitive activities in cyberspace (e.g., the Internet), which can influence impulsive decision-making and intentional behaviour (Hadlington, 2017a). It encompasses how individuals perceive, think, learn and make decisions in online environments, as well as how they interact with digital devices and systems. This field addresses areas such as digital literacy, online decision-making and the effects of technology on attention, memory and problem-solving skills. Additionally, cybercognition considers the psychological and social consequences of digital engagement, including phenomena such as cyberbullying, digital addiction and the influence of social media. In the context of this study, cybercognition serves as a lens for exploring cognitive processes in online environments and their psychological dimensions. It offers novel insights into the relationship between cognitive function and OGA, supporting Yadav (2021), who noted that gamers who are unable to stop playing often exhibit withdrawal symptoms that impair awareness and hinder secure decision-making.

Additionally, this study highlights attention and concentration deficits among online gamers who experience conflict due to their gaming activities. Blackwell et al. (2017) linked cybercognition to personality traits such as extraversion, neuroticism and fear of missing out (FOMO), showing how these traits influence users' reactions during online game interactions. Similarly, McNeese et al. (2012) examined cognition in cybersecurity, identifying additional components, such as visuospatial processing, the episodic buffer (segmentation), and the phonological loop (language), as key cognitive dimensions. Personality traits, including conscientiousness, impulsivity, introversion and openness to experience, can further shape security behaviour and perceptions of vulnerability, thereby affecting cybercognition. For example, adolescents with high openness to experience may be more attentive to privacy concerns, such as phishing attacks, yet simultaneously more susceptible to cyber threats due to addictive behaviours (Halevi et al., 2016). Accordingly, cybercognition has been incorporated into PMT to enhance the SIB model, integrating cognitive factors to better support cautious, adaptive behaviour in the face of cybersecurity threats (Hadlington, 2017a, 2018b; Nadry et al., 2025).

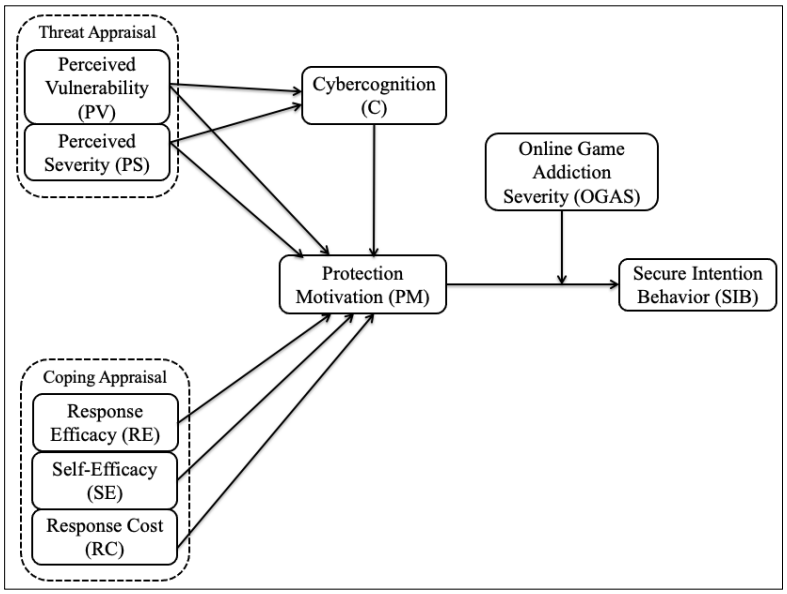
Based on the argument stated, it is evident that cybercognition provides a critical lens for understanding how adolescents acquire knowledge, process information, and make decisions in online environments, particularly in the context of online gaming. Cognitive processes, personality traits, and addictive behaviours collectively shape attention, decision-making, and security-related intentions. Integrating cybercognition into PMT offers a promising approach to explain variations in secure behavioural intentions among adolescents with OGA. By accounting for cognitive vulnerabilities, attentional deficits, and motivational factors, this perspective supports the development of the SIB model, which aims to enhance protective and cautious behaviours in the face of cyber threats.

CONCEPTUAL FRAMEWORK

This study develops a conceptual model based on the updated PMT (Jansen & Schaik, 2018). Figure 1 illustrates the conceptual model of the study.The model consists of nine interrelated constructs, theorising on threat appraisal (i.e., perceived vulnerability (PV) and perceived severity (PS)) and coping appraisal (i.e., response efficacy (RE), self-efficacy (SE) and response cost (RC).

Figure 1

The Conceptual Model of the Study



These components, together with protection motivation (PM) and SIB, form the theoretical backbone of the model. Furthermore, the model is enhanced by including cybercognition to replace the fear appeal construct in the original PMT. Cybercognition plays a crucial role in shaping impulsive decision-making and intentional behaviours. To bridge PM and SIB, this model incorporates OGA severity (OGAS) as a moderating factor, acknowledging its influence on adolescents' cybersecurity-related intentions. The model provides a structured foundation for analysing behavioural responses to cybersecurity challenges among adolescent online gamers.

Hypotheses Development

Hypothesis testing highlights the nature of the underlying relationships among various factors to understand the research problem (Sekaran, 2003). Guided by the proposed conceptual model, ten hypotheses were formulated and tested to examine the relationships between exogenous variables (independent predictors) and the endogenous variable (secure behaviour intention). The results of these tests are presented in Table 1, followed by a detailed discussion of the findings in the subsequent sections. These hypotheses are visually represented in the SIB model, with mapped hypotheses shown in Figure 2. This figure serves as a blueprint for the empirical testing process. By mapping each hypothesis onto this conceptual model, researchers can trace the influence of individual and contextual factors on secure behaviour intentions, thereby providing a structured framework for interpreting the data.

Table 1

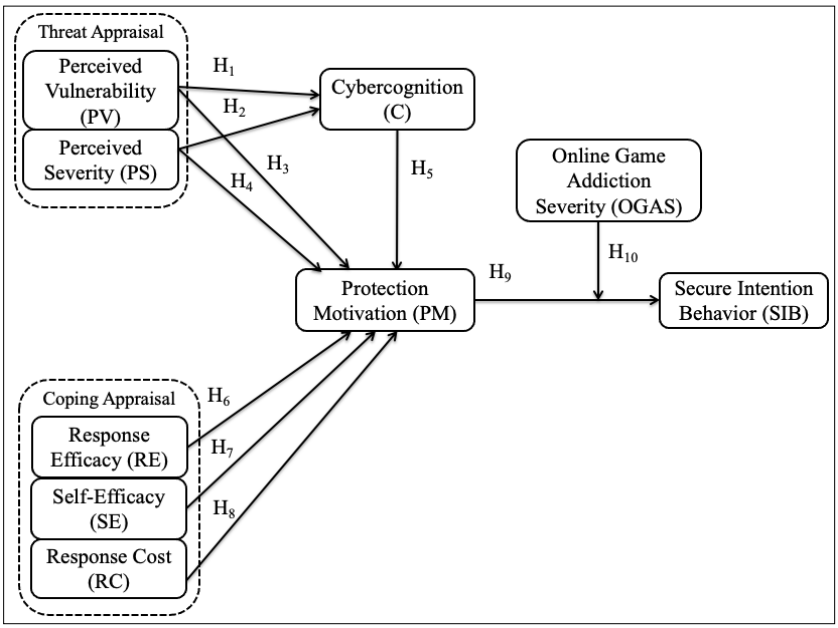
List of Main Hypotheses

	Description	Exogenous Variables	Endogeneous Variables
H_1	Perceived vulnerability has a positive influence on cybercognition among adolescents in Malaysian HLIs.	PV	C
H_2	Perceived severity has a positive influence on cybercognition among adolescents in Malaysian HLIs.	PS	C
H_3	Perceived vulnerability has a positive influence on protection motivation among adolescents in Malaysian HLIs.	PV	PM
H_4	Perceived severity has a positive influence on protection motivation among adolescents in Malaysian HLIs.	PS	PM
H_5	Cybercognition has a positive influence on protection motivation among adolescents in Malaysian HLIs.	C	PM
H_6	Response efficacy has a positive influence on protection motivation among adolescents in Malaysian HLIs.	RE	PM
H_7	Self-efficacy has a positive influence on protection motivation among adolescents in Malaysian HLIs.	SE	PM
H_8	Response cost has a negative influence on protection motivation among adolescents in Malaysian HLIs.	RC	PM
H_9	Protection motivation has a positive influence on SIB among adolescents in Malaysian HLIs.	PM	SIB
H_{10}	OGA severity moderates the relationship between protection motivation and SIB among adolescents in Malaysian HLIs.	PM	SIB

Notes. PV = Perceived Vulnerability, PS = Perceived Severity, C = Cybercognition, RE = Response Efficacy, SE = Self-Efficacy, RC = Response Cost, PM = Protection Motivation, SIB = Secure Intention Behaviour, HLIs = Higher Learning Institutions.

Figure 2

SIB Model with Mapped Hypotheses



METHODOLOGY

This study employed a quantitative research design to provide systematic and empirically grounded answers to the proposed research questions. A survey approach was adopted to examine the relationships among PMT constructs, cybercognition, and SIB among adolescents engaged in online gaming activities. The quantitative approach was deemed appropriate as it enables theory testing, model evaluation, and statistical assessment of predictive relationships within a defined population.

Literature Review and Model Development

The development of the research model was supported by a systematic review of the literature addressing SIB, online gaming activities, and cybersecurity-related decision-making among adolescents. A systematic literature review (SLR) was conducted to establish a comprehensive and unbiased understanding of existing knowledge and to identify key determinants relevant to SIB in the OGA context. Reputable sources, including peer-reviewed journal articles, conference proceedings, books, and prior empirical studies, were examined, with particular emphasis on cybersecurity and behavioural perspectives. The review followed established guidelines proposed by Kitchenham et al. (2010) and Bettany-Saltikov and McSherry (2012), ensuring methodological rigor and transparency.

Drawing on the findings of the SLR, a conceptual research model was developed within the PMT. The model conceptualises SIB within the OGA context by identifying relevant PMT constructs and integrating cybercognition as an emerging determinant. Hypothesised relationships among the constructs were formulated based on theoretical reasoning and empirical evidence, resulting in a coherent framework for subsequent empirical testing.

Instrument Validation

Data were collected using a structured questionnaire developed by adapting established measurement instruments to ensure content validity and reliability, primarily from the Online Cognition Scale (OCS) (Błachnio et al., 2015) and the OGA Scale (Lemmens et al., 2009) to measure cybercognition. Constructs related to PMT and SIB were adapted from previous research in cybersecurity and behavioural studies. All items were measured using a Likert-type scale.

Before large-scale data collection, the instrument underwent an expert review process to assess clarity, relevance, and consistency of the measurement items. A review kit containing the questionnaire and supporting materials was provided to subject-matter experts, and their feedback was incorporated to refine the instrument. The revised questionnaire was subsequently used in a pilot test to confirm its suitability for the target population.

The instrument comprised three sections (A, B and C). Section A collected demographic information and included a screening item to assess respondents' prior experience with online gaming; adolescents without such experience were excluded from the study. Eligible respondents then completed Sections B and C, which assessed self-protection motivation and online gaming-related tendencies influencing SIB in the context of OGA. Table 2 summarises the questions included in the instrument.

Table 2

List of the Questions in the Instrument

Construct	Item	Questions
Perceived Vulnerability	A1	I would click the link to fill in my personal information (username and password) in order to continue using the service.
	A2	I know there is a risk of becoming a phishing victim if I click the link.
	A3	I could become a phishing victim if I share the requested personal information.
Perceived Severity	B1	If I were a victim of phishing attacks, there would be no effect on me.
	B2	If I were a victim of phishing attacks, the consequences would be mild (e.g., effects on an individual).
	B3	If I were a victim of phishing attacks, the consequences would be moderate (e.g., effects on an organisation).
	B4	If I were a victim of phishing attacks, the consequences would be severe (e.g., global-level effects).
Response Efficacy	C1	Not sharing personal information in online games helps to prevent phishing attacks.
	C2	I believe that not sharing personal information in online games is an effective way to prevent phishing attacks.
	C3	If I do not share my personal information in online games, the likelihood of becoming a phishing victim will decrease.
Self-Efficacy	D1	I am able to take steps to prevent myself from sharing personal information in online games to avoid phishing attacks.
	D2	Not sharing personal information in online games is easy to do as a preventive measure against phishing attacks.
	D3	Using the recommended measure of not sharing personal information in online games is convenient.

(continued)

Construct	Item	Questions
Response Cost	E1	Despite the possibility of becoming a phishing victim, not sharing personal information in online games is inconvenient.
	E2	Despite the possibility of becoming a phishing victim, being cautious about whether to share personal information in online games is time-consuming.
	E3	Despite the possibility of becoming a phishing victim, not sharing personal information in online games requires a lot of mental effort.
	E4	Despite the possibility of becoming a phishing victim, not sharing personal information in online games requires starting a new habit that is difficult to implement.
Diminished Impulse Control (Cybercognition)	F1	I make decisions quickly when playing online games.
	F2	When playing online games, I do not think about the possibility of becoming a phishing victim.
	F3	I often think about the possibility of becoming a phishing victim after playing online games.
	F4	The thought of becoming a phishing victim scares me.
	F5	I feel worried when thinking about the possibility of becoming a phishing victim.
	F6	Despite the possibility of becoming a phishing victim, I find the offline world less exciting than what I can do online.
	F7	Despite the possibility of becoming a phishing victim, I cannot stop thinking about online games all the time.
	F8	Despite the possibility of becoming a phishing victim, I cannot reduce my online gaming frequency even though I am capable of doing so.
Protection Motivation	G1	I am likely to avoid sharing personal information in online games to protect myself from phishing attacks.
	G2	I would follow the practice of not sharing personal information in online games to protect myself from phishing attacks.
	G3	I am certain that I will not share personal information in online games to protect myself from phishing attacks.
	G4	I intend not to share personal information in online games as an effort to protect myself from phishing attacks.
Secure Intention Behaviour	H1	I will not click on any pop-up messages that appear on my screen while playing online games.
	H2	I will verify messages or emails that ask me to enter financial or personal information in online games.
	H3	I will not respond to messages from unknown parties requesting me to update my username or password.
	H4	When prompted to update an online game, I will check the update carefully.

The constructs were measured using a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). This scale was selected for its balanced response format, which helps reduce central tendency bias and facilitates robust statistical analysis (Comrey, 1988; Dwivedi et al., 2010). To ensure clarity, relevance, and theoretical consistency, the instrument was reviewed by experts in information systems and cybersecurity and aligned with the extended PMT.

Sampling and Data Collection

A probability sampling approach was adopted, using a three-stage simple random sampling technique. Due to the absence of a comprehensive list of adolescent students, the sampling frame was based on a list of higher learning institutions (HLIs) obtained from the Malaysian Ministry of Higher Education

(MoHE). In the first stage, 85 HLIs across Peninsular Malaysia were selected to ensure coverage of the Northern, Southern, Eastern, and Central regions. In the second stage, 10 students were randomly selected from each institution, yielding a total sample of 850 respondents. This multi-stage random sampling procedure was utilised to minimise selection bias, ensure adequate representation across institutions, enhance the external validity and support the generalisability of the study's findings.

Data collection was conducted through both online and face-to-face surveys to enhance accessibility and participation. For online respondents, the questionnaire was distributed via email through Google Forms, while face-to-face data collection was conducted in a supervised setting. To ensure respondents had an adequate contextual understanding of cybersecurity threats, a brief video on phishing was shown prior to completing the questionnaire. Participation was voluntary, and ethical considerations, including informed consent and respondent anonymity, were strictly observed. The data collection process resulted in a dataset suitable for quantitative analysis.

Data Analysis

Data analysis was conducted using Partial Least Squares Structural Equation Modelling (PLS-SEM), chosen for its suitability in modelling complex relationships and handling non-normal data distributions. PLS-SEM is not only appropriate for exploratory studies with predictive aims but also allows for the simultaneous estimation of measurement and structural models. Before performing the analysis, the data were assessed to ensure compliance with key PLS-SEM assumptions, including indicator reliability, internal consistency, convergent validity and discriminant validity. The data analysis in this study was unfolded in two phases. Initially, IBM SPSS Statistics (SPSS) was used for data entry, screening, and preparation for the second phase. Subsequently, in the second phase, PLS-SEM was employed to test hypotheses. At this stage, Confirmatory Factor Analysis (CFA) was employed to validate the factors derived earlier through Exploratory Factor Analysis (EFA).

Model Evaluation and Validation

To further validate the robustness of the proposed model and analytical procedures, an expert evaluation was conducted following data analysis. Four experts from the domains of cybersecurity, psychology, information systems, and information technology participated in this evaluation. Each expert had more than ten years of professional and academic experience and was affiliated with reputable academic institutions. Using a structured evaluation kit, the experts assessed the appropriateness of the analytical methods, hypothesis-testing procedures, and the interpretation of results. This evaluation provided additional support for the validity of the research findings and confirmed the adequacy of the proposed model.

RESULT AND FINDINGS

Demographic Profiles of Respondent

The data collection involved distributing 850 questionnaires through online and face-to-face methods to selected HLIs. A total of 713 questionnaires were returned, yielding a response rate of approximately 82.0%, which is considered notably high. Of these, 87.0% were completed online, while 13.0% were submitted in paper-based format. All responses were screened for completeness and accuracy, with checks for missing data and outliers. After validation, 660 responses (75.6% of those distributed) were deemed valid and suitable for analysis. Among the 660 valid respondents, 355 (53.8%) were male, and 305 (46.2%) were female, aged 17-19 years, with an average age of 19. This gender distribution aligns

with existing data indicating that online gaming engagement is typically higher among male adolescents (Statista, 2018). Geographically, respondents were drawn from urban (60.6%) and rural (39.4%) regions. In terms of academic level, the majority were diploma students (68.2%), followed by bachelor's degree (16.2%) and certificate students (15.6%).

Almost all respondents (97.0%) reported prior experience with online gaming, highlighting the pervasiveness of this activity among HLI adolescents. However, the duration varied, with the largest proportion (33.0%) playing for 1–2 hours daily. This was followed by those who played for 2–3 hours (24.0%), less than 1 hour (23.0%), 3–4 hours (10.0%), 4–5 hours (5.0%), and more than 5 hours daily (5.0%). Mobile phones were the most frequently used gaming platform, preferred by 74.0% of respondents, indicating a strong inclination toward mobile-based gaming. Other platforms included computers (21.0%), consoles (2.0%), tablets (2.0%) and arcade machines (1.0%). In terms of game genres, strategy games were most popular (35.6%), followed by massively multiplayer online (MMO) games (30.0%), adventure (10.0%), sports (10.0%), simulation (7.4%) and racing games (7.0%). These usage patterns offer valuable insights into the gaming habits of HLI adolescents and provide a behavioural context crucial for understanding their susceptibility to OGA and related security risks.

Assessment of Structural Model

This study also delves into the primary factors in structural analysis related to collinearity. Although the multicollinearity test was conducted during data preparation, the issue was revisited in the structural model analysis. Variance Inflation Factor (VIF) values were computed using the PLS algorithm to assess multicollinearity. The findings affirm the earlier assessment, with all VIF values falling below 10 (minimum: 1.381; maximum: 4.726), indicating that the model is not adversely affected by multicollinearity. This study employed a standard bootstrapping procedure involving 5,000 samples and 660 cases (Hair et al., 2014) to evaluate the significance of the path coefficient (*ß*). Figure 3 presents the assessment of the structural model, and Table 3 summarises the hypothesis-testing results for the SIB model structure.

Figure 3

Assessment of Structural Model using PLS-SEM

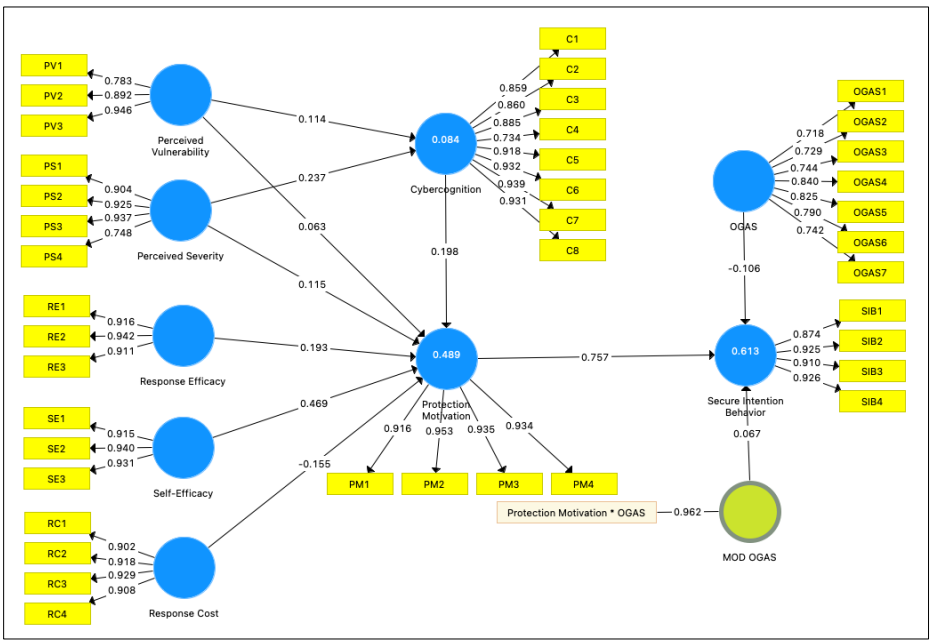


Table 3

Assessment of Hypotheses in the SIB Structural Model

Hypothesis		ß	T Values	p Values	95% CI	Result
H1	PV -> C	0.114	2.923	0.00***	0.034, 0.186	Supported
H2	PS -> C	0.237	5.062	0.00***	0.148, 0.331	Supported
H3	PV -> PM	0.063	1.650	0.100NS	0.004, 0.142	*Returned*
H4	PS -> PM	0.115	3.457	0.00***	0.053, 0.180	Supported
H5	C -> PM	0.198	6.278	0.00***	0.139, 0.261	Supported
H6	RE -> PM	0.193	4.097	0.00***	0.085, 0.279	Supported
H7	SE -> PM	0.469	9.164	0.00***	0.367, 0.565	Supported
H8	RC -> PM	-0.155	4.411	0.00***	0.218, 0.088	Supported
H9	PM -> SIB	0.757	31.683	0.00***	0.709, 0.800	Supported
H10	PM -> SIB	0.106	4.149	0.00***	0.059, 0.160	Supported

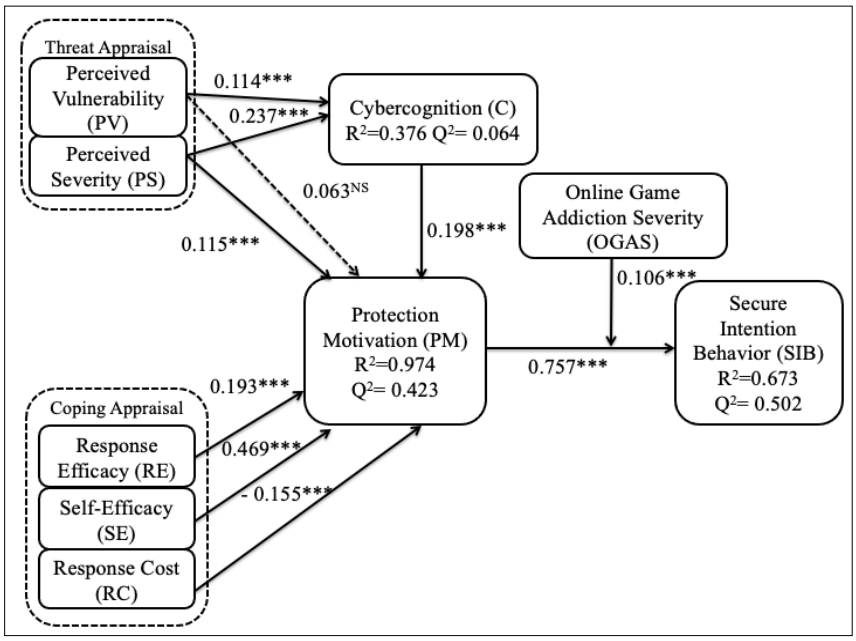
Notes. **p < 0.05, ***p< 0.01, NS = Not Significant, PV = Perceived Vulnerability, PS = Perceived Severity, C = Cybercognition, RE = Response Efficacy, SE = Self-Efficacy, RC = Response Cost, PM = Protection Motivation, SIB = Secure Intention Behaviour.

Hypothesis H_1 proposed that PV positively influences C among adolescents in online gaming environments. The analysis supported H_1 with a significant relationship ($\beta = 0.114$, t = 2.923, p < 0.01). Similarly, H_2, which posited that PS has a positive effect on C, was confirmed ($\beta = 0.237$, t = 5.062, p < 0.01). However, H_3, suggesting a positive influence of PV on PM, was not statistically supported ($\beta = 0.063$, t = 1.650, p > 0.01). H_4 proposed a positive correlation between PS and PM, which was upheld ($\beta = 0.115$, t = 3.457, p < 0.01). Additionally, a significant correlation was found between C and PM ($\beta = 0.198$, t = 6.278, p < 0.01), supporting H_5. H_6, predicting a positive relationship between Response Efficacy (RE) and PM, was supported ($\beta = 0.193$, t = 4.097, p < 0.01). Likewise, H_7 (SE → PM) and H_8 (RC → PM) were both supported, with $\beta = 0.469$, t = 9.164 and $\beta = 0.155$, t = 4.411, respectively (p < 0.01).

The main hypothesis H_9 suggested that PM positively influences SIB. PLS path analysis confirmed a significant relationship between PM and SIB ($\beta = 0.757$, t = 31.683, p < 0.01). Additionally, Hypothesis H_{10} examined the moderating role of OGAS on the relationship between PM and SIB. The interaction term (PM*OGAS) was statistically significant ($\beta = 0.106$, t = 4.149, p < 0.05), indicating that OGAS moderates the effect of PM on SIB. Thus, players with higher OGAS are more likely to translate protective motivation into actual security behaviours in gaming environments. At the end of the analysis phase, the proposed model was finalised to represent SIB in the context of online gaming awareness comprehensively. Figure 4 visualises the proposed model, illustrating both supported and unsupported hypotheses. Solid lines represent significant relationships, while dotted lines denote those that are not statistically supported. This proposed model provides valuable insights into the behavioural mechanisms underlying gamers' responses to phishing threats.

Figure 4

The proposed SIB Model



Notes. **p < 0.05, ***p< 0.01, NS = Not Significant. PV = Perceived Vulnerability, PS = Perceived Severity, C = Cybercognition, RE = Response Efficacy, SE = Self-Efficacy, RC = Response Cost, PM = Protection Motivation, SIB = Secure Intention Behaviour, OGAS = OGA Severity.

DISCUSSION

This study conducted a comprehensive evaluation of prior studies and models of security behaviour to address the research questions. This study has also successfully adapted the PMT model, incorporating cybercognition and OGAS as moderators. The following provides the answers to the three main research questions, together with a comprehensive summary of research achievements. The first objective of this study is to identify the factors contributing to SIB among OGA adolescents. This objective was addressed through a systematic literature review that informed the study's fundamental ideas. The structural analysis of the model has uncovered seven factors and one insignificant factor. PM was found to be the most dominant predictor (β = 0.757), followed by SE (β = 0.469), PS (β = 0.237), C (β = 0.198), RE (β = 0.193), RC (β = 0.155), and PV (β = 0.114). These findings were in line with previous research that has indicated a positive correlation between the factors (Briggs et al., 2017; Hadlington, 2017a; Jansen & Schaik, 2018). The results show that these factors are related to adolescents' intention toward security behaviour, thereby justifying their selection as contributing factors in the SIB model in the context of OGA among late adolescents in Malaysian HLIs.

The second objective of this study was to develop an SIB model that incorporates the identified factors. This was achieved by constructing a conceptual model grounded in PMT and integrating Cybercognition and OGAS to address the behavioural addiction context, which has often been overlooked in previous cybersecurity-focused PMT studies. Relevant hypotheses were formulated to examine the relationships between the model's constructs. Cybercognition refers to the mental processes involved in acquiring knowledge, evaluating information, and making decisions in digital environments. As an emerging determinant in cybersecurity research, it plays a critical role in shaping

adolescents' SIB particularly in the context of OGA. This model contributes to the body of knowledge by extending the results of previous studies on the relationships among the factors (Hadlington, 2017a; Jansen, 2015) in the context of OGA among adolescents. Unlike the traditional PMT factors, cybercognition influences how individuals perceive threats, process digital information, and convert motivational cues into protective actions. In this study, cybercognition serves as a moderating variable, influencing the strength of the relationships between PMT constructs and SIB. Adolescents with higher cybercognitive skills are more likely to accurately assess cyber threats and adopt protective measures, whereas those with lower skills may be more vulnerable, highlighting the importance of integrating cognitive capacity into models of digital security behaviour.

The third objective was achieved by evaluating the constructs of the proposed model through expert and practitioner validation. This study provides a comprehensive evaluation of the SIB model in the context of OGA among adolescents in Malaysian higher education institutions. The evaluation involves objectively examining various aspects to determine the contribution to knowledge. Model evaluation becomes the most important step in model development. Theoretically, it integrates cybercognition as a key determinant, demonstrating how cognitive processes shape SIB and introduces OGAS as a moderating factor, offering a novel perspective that extends PMT. While PMT traditionally emphasises fear appeals to motivate protective behaviour, this study highlights the importance of cognitive mechanisms in translating threat appraisal and coping processes into secure behavioural intentions. Overall, the findings advance both theory and practice, confirming that cybercognition and OGAS jointly provide a more accurate explanation of adolescents' security intentions in digital environments affected by gaming addiction.

CONCLUSION AND FUTURE RESEARCH

This study introduces a model grounded in PMT to explore how various psychological factors influence adolescents' SIB in online gaming environments. It examines the relationship between threat and coping appraisals, offering a structured framework for understanding cybersecurity behaviours. Key elements, such as perceived severity, perceived vulnerability, response efficacy, self-efficacy, response cost, and cybercognition, were validated as critical for assessing SIB among adolescents in Malaysian HLIs. The model also enables the development of effective measurement tools, ensuring adaptability to emerging cyber threats and supporting improved cybersecurity decision-making. It lays a foundation for scalable solutions that can evolve alongside digital threats in the online gaming context. Additionally, the study provides strong empirical evidence that cybercognition significantly predicts protection motivation among adolescents, underscoring its importance in designing effective cybersecurity interventions. The findings also confirm that the OGAS plays a crucial moderating role in the relationship between protection motivation and SIB, especially concerning susceptibility to phishing attacks. These insights offer valuable guidance to the MoHE in crafting targeted cybersecurity strategies. By prioritising cybercognition and leveraging the validated SIB model, the MoHE can implement responsive, sustainable measures to address adolescent vulnerabilities within HLIs.

ACKNOWLEDGMENT

This research was supported by the Ministry of Higher Education (MoHE) through the Fundamental Research Grant Scheme (Ref: FRGS/1/2020/ICT03/UUM/02/1). The content of this article is solely the responsibility of the authors and does not necessarily represent the official views of MoHE, Malaysia.

REFERENCES

Aivazpour, Z., & Srinivasan Rao, V. (2018). *Impulsivity and risky cybersecurity behaviors: A replication*. Americas Conference on Information Systems 2018: Digital Disruption, AMCIS 2018, 2017, 1–9. https://www.academia.edu/download/70929456/impulsivity_replication.pdf

Ajzen, I. (1985). *From intentions to actions: A theory of planned behavior.* Action Control, 11–39. https://doi.org/10.1007/978-3-642-69746-3_2

Alrobai, A., Phalp, K., & Ali, R. (2014). *Digital addiction: A requirements engineering perspective*. In International Working Conference on Requirements Engineering: Foundation for Software Quality (pp. 112-118). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-05843-6_9

Baturay, M. H., & Toker, S. (2019). Internet addiction among college students: Some causes and effects. *Education and Information Technologies*, *24*(5), 2863–2885. https://doi.org/10.1007/s10639-019-09894-3

Bekir, S., & Çelik, E. (2019). Examining the factors contributing to adolescents' online game addiction. *Anales de Psicologia*, *35*(3), 444–452. https://doi.org/10.6018/analesps.35.3.323681

Bettany-Saltikov, J., & McSherry, R. (2012). *How to do a systematic literature review in nursing: A Step-by-Step Guide*. McGraw Hill

Błachnio, A., Przepiórka, A., & Hawi, N. S. (2015). Exploring the online cognition scale in a Polish sample. *Computers in Human Behavior*, *51*(PA), 470–475. https://doi.org/10.1016/j.chb.2015.05.028

Blackwell, D., Leaman, C., Tramposch, R., Osborne, C., & Liss, M. (2017). Extraversion, neuroticism, attachment style and fear of missing out as predictors of social media use and addiction. *Personality and Individual Differences*, *116*, 69–72. https://doi.org/10.1016/j.paid.2017.04.039

Comrey, A. L. (1988). Factor-analytic methods of scale development in personality and clinical psychology. *Journal of Consulting and Clinical Psychology*, *56*(5), 754–761. https://doi.org/10.1037/0022-006X.56.5.754

Conner, M., & Norman, P. (2022). Understanding the intention-behavior gap: The role of intention strength. *Frontiers in psychology*, *13*, 923464. https://doi.org/10.3389/fpsyg.2022.923464

Creswell, J. W. (2013). *Research design qualitative, quantitative, and mixed method approaches* (p. 273). SAGE.

Durak, H. (2019a). Human factors and cybersecurity in online game addiction: An analysis of the relationship between high school students' online game addiction and the state of providing personal cybersecurity and representing cyber human values in online games. *Social Science Quarterly*, *100*(6), 1984–1998. https://doi.org/10.1111/ssqu.12693

Dwivedi, Y. K., Papazafeiropoulou, A., Brinkman, W. P., & Lal, B. (2010). Examining the influence of service quality and secondary influence on the behavioural intention to change Internet service provider. *Information Systems Frontiers*, *12*(2), 207–217. https://doi.org/10.1007/s10796-008-9074-7

Goncalves et al. (2018). Scale to assess leaders' perceptions about their workers' digital addiction. *Addiction & Health*, *10*(4), 223–230. https://doi.org/10.22122/ahj.v10i4.637

Gregersen, E. M., Astrupgaard, S. L., Jespersen, M. H., Gårdhus, T. P., & Albris, K. (2023). Digital dependence: Online fatigue and coping strategies during the COVID-19 lockdown. *Media, Culture and Society*, *45*(5), 967–984. https://doi.org/10.1177/01634437231154781

Griffiths, M. (2005). A 'components' model of addiction within a biopsychosocial framework. *Journal of Substance Use*, *10*(4), 191–197. https://doi.org/10.1080/14659890500114359

Hadlington, L. (2017a). *Cybercognition: Brain, behavior and the digital world*. SAGE.

Hadlington, L. (2017b). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hadlington, L. (2018). Lee Hadlington, cybercognition: Brain, behaviour, and the digital world. *Psychology Learning & Teaching*, *17*(3), 323–325. https://doi.org/10.1177/1475725718787921

Hadlington, L. (2018a). Employees attitude towards cyber security and risky online behaviors: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology, 12*(1), 269–281. https://doi.org/10.5281/zenodo.1467909

Hadlington, L. (2018b). The 'human factor' in cybersecurity. In *Psychological and Behavioral Examinations in Cyber Security, 3*, 46–63. https://doi.org/10.4018/978-1-5225-4053-3.ch003

Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial Least Squares Structural Equation Modeling (PLS-SEM): An emerging tool in business research. In *European Business Review* (Vol. 26, Issue 2, pp. 106–121). Emerald Group Publishing Ltd. https://doi.org/10.1108/EBR-10-2013-0128

Halevi et al. (2016). *Cultural and psychological factors in cybersecurity.* ACM International Conference Proceeding Series, November 2017, 318–324. https://doi.org/10.1145/3011141.3011165

Jansen, J., & van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behavior against phishing. *International Journal of Human Computer Studies, 123*(January 2018), 40–55. https://doi.org/10.1016/j.ijhcs.2018.10.004

Jenkins, J. L., Durcikova, A., & Nunamaker, J. F. (2021a). Mitigating the security intention-behavior gap: The moderating role of required effort on the intention-behavior relationship. *Journal of the Association for Information Systems, 22*(1), 246–272. https://doi.org/10.17705/1jais.00660

Julisia, N., & Nursalim, M. (2025). The relationship between learning motivation and self-regulated learning with online game addiction of junior high school students. *QUANTA Journal: Kajian Bimbingan Dan Konseling Dalam Pendidikan*, *9*(1), 40–48. https://doi.org/10.22460/quanta.v9i1.5551

Kesici, A., & Fidan Tunç, N. (2018). The development of the digital addiction scale for university students: Reliability and validity study. *Universal Journal of Educational Research*, *6*(1), 91–98. https://doi.org/10.13189/ujer.2018.060108

Kiran, U., Khan, N. F., Murtaza, H., Farooq, A., & Pirkkalainen, H. (2025). Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory. *Computers and Security*, *149*. https://doi.org/10.1016/j.cose.2024.104204

Kitchenham et al. (2010). Systematic literature reviews in software engineering-A tertiary study. *Information and Software Technology*, *52*(8), 792–805. https://doi.org/10.1016/j.infsof.2010.03.006

Lemmens, J. S., & Hendriks, S. J. F. (2016). Addictive online games: Examining the relationship between game genres and internet gaming disorder. *Cyberpsychology, Behavior, and Social Networking, 19*(4), 270–276. https://doi.org/10.1089/cyber.2015.0415

Lemmens, J. S., Valkenburg, P. M., & Peter, J. (2009). Development and validation of a game addiction scale for adolescents. *Media Psychology*, *12*(1), 77–95. https://doi.org/10.1080/15213260802669458

Lowry, P. B., Moody, G. D., Parameswaran, S., & Brown, N. J. (2023). Examining the differential effectiveness of fear appeals in information security management using two-stage meta-analysis. *Journal of Management Information Systems*, *40*(4), 1099-1138. https://doi.org/10.1080/07421222.2023.2267318

McNeese et al. (2012). *Perspectives on the role of cognition in cyber security.* Proceedings of the Human Factors and Ergonomics Society, 268–271. https://doi.org/10.1177/1071181312561063

Meltwater. (2023). *Digital Global Growth 2023*. https://www.meltwater.com/en/2023-global-digital-trends

Nadry, Z., Hakimi, M., Sirat, A. W., & Popal, Z. (2025). Strengthening cybersecurity awareness through Education: The expanding role of cyber law in academic institutions. *Jurnal Analisis Hukum*, *8*(2), 193–209. https://doi.org/10.38043/jah.v8i2.7086

Nawaz, S., Bhowmik, J., Linden, T., & Mitchell, M. (2024). Adapting to the new normal: Understanding the impact of COVID-19 on technology usage and human behavior. *Entertainment Computing*, *51*, 100726. https://doi.org/10.1016/j.entcom.2024.100726

Newman, E. (2022). COVID-19: A human security analysis. *Global Society*, *36*(4), 431–454. https://doi.org/10.1080/13600826.2021.2010034

Norman et al. (2023). Technology dependency and impact during COVID-19: A systematic literature review and open challenges. *IEEE Access, 11*, 40741-40760. https://doi.org/10.1109/ACCESS.2023.3250770

Novrialdy, E., & Atyarizal, R. (2019). Online game addiction in adolescents: What should school counselors do? *Jurnal Konseling Dan Pendidikan, 7*(3), 97. https://doi.org/10.29210/132700

Pahnila, S., Karjalainen, M., & Siponen, M. (2013). *Information security behavior: Towards multi-stage models.* PACIS 2013 Proceedings, 102. http://aisel.aisnet.org/pacis2013/102

Pollini et al. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology and Work, 24*(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Pratama, O., Aladin, R. A., Lim, B., & 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/ijsse.150304

Purwaningsih, E., & Nurmala, I. (2021). The impact of online game addiction on adolescent mental health: A systematic review and meta-analysis. *Open Access Macedonian Journal of Medical Sciences (OAMJMS)*, *9*(F), 260-274. http://repository.unair.ac.id/id/eprint/123624

Schneider, L. A., King, D. L., & Delfabbro, P. H. (2017). Family factors in adolescent problematic internet gaming: A systematic review. *Journal of Behavioral Addictions, 6*(3), 321–333. https://doi.org/10.1556/2006.6.2017.035

Sekaran, U. (2003). Research methods for business: A skill-building approach, fourth edition. *Journal of Chemical Information and Modeling*, *53*(9). https://doi.org/10.1017/CBO9781107415324.004

Shamsudin, N. N. A., Yatin, S. F. M., Nazim, N. F. M., Talib, A. W., Sopiee, M. A. M., & Shaari, F. N. (2019). Information security behaviors among employees. *International Journal of Academic Research in Business and Social Sciences, 9*(6), 560–571. https://doi.org/10.6007/ijarbss/v9-i6/5972

Sheeran, P., & Webb, T. L. (2016). The intention–behavior gap. *Social and Personality Psychology Compass, 10*(9), 503–518. https://doi.org/10.1111/spc3.12265

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers and Security, 49*(March 2015), 177–191. https://doi.org/10.1016/j.cose.2015.01.002

Simpson, J. K. (2017). Appeal to fear in health care: Appropriate or inappropriate? *Chiropractic and Manual Therapies, 25*(1). https://doi.org/10.1186/s12998-017-0157-8

Spano, S. (2004). Stages of Adolescent Development. *Youth Upstate Center of Excellence*, *1*(1), 1–4.

Statista. (2018). Online Games - worldwide | Statista Market Forecast. https://www.statista.com/outlook/212/100/online-games/worldwide#market-revenue

Stubbendorff, C., & Stevenson, C. W. (2020). Dopamine regulation of contextual fear and associated neural circuit function. *European Journal of Neuroscience, December 2019,* 1–15. https://doi.org/10.1111/ejn.14772

Tomicic, I., Grd, P., & Schatten, M. (2019). *Reverse engineering of the MMORPG client protocol.* In Proceedings of 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2019, 1099–1104. https://doi.org/10.23919/MIPRO.2019.8756873

Türker, P., & Çakmak, E. (2019). An investigation of cyber wellness awareness: Turkey secondary school students, teachers, and parents. *Computers in the Schools*, *36*(4), 293–318. https://doi.org/10.1080/07380569.2019.1677433

Wibowo, T., & Fransco, N. (2021). *Pengaruh kecanduan mobile game terhadap gangguan sosial pada era COVID-19.* In CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences, 1(1) 687-694). https://www.academia.edu/download/95306762/4496-206-5145-1-10-20210330.pdf

Xu, Z., Turel, O., & Yuan, Y. (2012). Online game addiction among adolescents: Motivation and prevention factors. *European Journal of Information Systems, 21*(3), 321–340. https://doi.org/10.1057/ejis.2011.56

Yadav, N. (2021). Relationship between cognitive functions and online game addiction. *International Journal of Indian Psychology*, *9*(4). https://doi.org/10.25215/0904.112

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. *Information Technology and People, 26*(4), 401–419. https://doi.org/10.1108/ITP-12-2012-0147