The Journal of Behavioral Science
2024, Vol. 19, Issue 2, 44-58
Copyright © Behavioral Science Research Institute
ISSN: 1906-4675 (Print), 2651-2246 (Online)

The Journal of Behavioral Science (TJBS)

Quantitative Research Article

Determinants of Phishing Risk Awareness among Thai University Academic Staff

Pita Jarupunphol[1], Wichidtra Sudjarid[2], and Wipawan Buathong[1]*

Abstract

Background/problem: Phishing involves deceiving individuals into disclosing sensitive information. It poses a significant threat to academic institutions, impacting their security, financial stability, reputation, and operational efficiency.

Objective/purpose: This research examined phishing risk awareness among academic staff at two Thai universities and investigated the factors influencing phishing threat awareness using the technology acceptance model (TAM).

Design and Methodology: The study's sample comprised 400 participants, evenly distributed with 200 individuals selected from each of two universities, each employing approximately 450 academic staff members. Data were collected using an online questionnaire.

Results: The results demonstrated correlations between perceived ease of use (PEOU) and perceived usefulness (PU) ($\beta = .52$, $p < .001$), PEOU and attitude towards using (ATT) ($\beta = .25$, $p < .001$), PU and ATT ($\beta = .57$, $p < .001$), and ATT and phishing observation behavior (USE) ($\beta = .14$, $p = .01$). The relationship between phishing observation behavior (USE) and phishing risk awareness (PHA) was found insignificant ($\beta = -.09$, $p = .20$). However, the influences of perceived risk (PR) on USE ($\beta = .15$, $p < .001$) and PHA ($\beta = .17$, $p < .001$) were more pronounced.

Conclusion and Implications: This indicates that the awareness of phishing threats is more linked to the individual's risk perception rather than direct observation of phishing incidents. This suggests that enhancing phishing risk awareness should focus on educating individuals about the risks of phishing rather than increasing the visibility of phishing attempts.

Author Affiliation

[1] Department of Digital Technology, Phuket Rajabhat University, Thailand.
[2] Department of Environmental Science, Sakon Nakhon Rajabhat University, Thailand.

*Corresponding author e-mail: w.buathong@pkru.ac.th
https://orcid.org/0000-0003-0926-3432

Article Information

Submitted: 25.11.23
Accepted: 11.05.24
Published: 31.05.24

Keywords

Behavioral science, cyber threats, perceived risk, phishing risk awareness, SEM, TAM

Academic institutions have been affected by various cyber threats (Musuva et al., 2019; Naagas et al., 2018; Ribeiro et al., 2024), such as distributed denial of service attacks (DDoS), the man in the middle (MIM), and different malware (trojans, viruses, worms, and ransomware). Several schools and colleges have been victims of DDoS and ransomware, ceasing their critical information system services (Naagas et al., 2018). The National Cyber Security Agency (NCSA, 2023) annual report for 2022 reveals that Thailand faced a significant number of cyberattacks, totaling 2,517 incidents. These attacks were categorized into various types, including abusive content (47 incidents), availability (12 incidents), fraud (73 incidents), information gathering (23 incidents), information security (19 incidents), intrusion attempts (268 incidents), intrusions (109 incidents), malicious code (1,365 incidents), and vulnerabilities (601 incidents). This data underscores the pressing need for robust cybersecurity measures and awareness in the country. Phishing techniques, which are deceptive attempts to obtain sensitive information, often play a critical role in these cyber threats. Notably, Thailand is third in the Association of Southeast Asian Nations (ASEAN) region in terms of the proportion of phishing attempts related to financial information. The country has a 55.60% rate

of financial-related phishing attempts, just behind the Philippines at 69% and Singapore at 55.70% (Leesa-Nguansuk, 2022). This escalation in cyber threats, particularly those involving phishing, poses a significant risk to academic institutions in Thailand. The tactics used in cyber-attacks on public and commercial entities are relatively like those employed in the academic sector, making educational institutions equally vulnerable to these digital dangers. This situation underscores the importance of heightened cybersecurity measures and awareness within the academic community to protect against such threats.

In the evolving landscape of cybersecurity threats, phishing emerges as a particularly insidious challenge, demanding a multi-faceted approach for effective mitigation. Contemporary cybersecurity research, particularly in phishing, has focused on technological solutions and user education programs (Hillman et al., 2023). However, a significant gap remains in understanding how socioeconomic and psychological factors collectively shape individuals' awareness and responses to phishing threats (Abroshan et al., 2021). As such, cybersecurity issues, particularly phishing threats, can have significant adverse effects on universities. These effects include potential breaches of sensitive data, disruption of academic operations, and damage to the institution's reputation (Diaz et al., 2020). While demography is a statistical study involving a demographic society that may differ over time or place, education, religion, race, and economic status (Abroshan et al., 2021), the socioeconomic status of the population in different research project areas may represent the potential for easy access to digital technologies and their associated threats. The population in areas with inferior economic status may need more perception, learning, and pursuit of knowledge and experience (Orunsolu et al., 2018). Due to these reasons, this research hypothesizes that geographic, economic, and environmental differences influence academic personnel between two universities in Thailand to understand, perceive, and become aware of phishing threats. This research investigates risk perception and awareness of phishing among academic personnel at university A, Phuket, and university B, Sakon Nakhon, with significant differences in income and cost of living.

This research aims to integrate behavioral science with cybersecurity, offering a novel perspective on the influence of these factors on perceived phishing risk and phishing risk awareness, especially in academic settings. While previous studies have explored the technical and educational dimensions (Diaz et al., 2020; Patterson et al., 2023; Tian et al., 2023), there is limited literature on how socioeconomic status and psychological behavior impact phishing awareness. This study extends the application of behavioral science to cybersecurity, explicitly addressing how varied socioeconomic backgrounds and psychological factors such as risk perception and cognitive biases influence the understanding and handling of phishing threats among academic staff. The research contributes to behavioral science by applying its principles to understand the intersection of socioeconomic factors and cybersecurity awareness. The study employs an interdisciplinary approach to dissect how different socioeconomic environments influence the susceptibility of academic staff to phishing. This approach is critical in revealing the complex and multi-layered nature of phishing risk perception, which goes beyond the traditional scope of technology-focused cybersecurity research.

Literature Review

This section begins with examining the theoretical background of risk perception and awareness in a general context before discussing these concepts within the realm of phishing. After that, the structure and components of the technology acceptance model (TAM) are delineated (Davis, 1989; 1993), followed by a review of the findings from existing studies that have applied TAM to technology adoption and cybersecurity contexts. The rationale behind selecting two universities for the experimental research is then articulated. Additionally, the endogenous and exogenous variables incorporated in this study are identified. Finally, this section elaborates on the nine hypotheses central to this research and outlines the research framework, providing a comprehensive overview of the study's theoretical and methodological foundations.

Theoretical Background

Perception, awareness, and risks are psychological conditions of the senses and mental factors. Depending on the ability to interpret, these conditions are associated with an individual's learning and responses. According to the APA dictionary of psychology (Vandebos, 2015), perception is the process or result of becoming aware of objects, relationships, and events through the senses, while awareness refers to the perception or knowledge of something, considered a behavioral index of conscious awareness. In addition, the risk is defined as 1) "the probability or likelihood that a negative event will occur; 2) the probability of experiencing loss or harm associated with an action or behavior". When risk amalgamates with perception, risk perception or perceived risk is an individual's subjective assessment of the risk level associated with a particular threat. Risk perceptions may vary according to demographic factors. In addition, lack of control is associated with perceived risk (Kasperson et al., 2003). For example, drivers often perceive the risk of accidents as low while driving because they believe they have control over their vehicle. This sense of control can lead to an underestimation of the potential hazards on the road. On the other hand, perceived risks of earthquakes and terrorist attacks are high because they are uncontrollable (Slovic, 1987). Besides, individuals are not aware of actual statistical data. Perceived risks are underestimated or exaggerated because they are habitual, which might be more and less valued than unknown risks. As such, perceived risks are related to an individual's knowledge and confidence about risks, determining how they are perceived and understanding the emotional dimension of feelings (Kasperson et al., 2003; Slovic, 1987). Based on the above definitions, perception is how we receive information from our environment through all the physical senses, such as sight, sound, and touch, but awareness is how much we perceive. In terms of risk perception and risk awareness in this research, individuals may perceive cyber threats exist, but how they respond to them is driven by risk awareness.

Nowadays, phishing remains a sophisticated and adaptable cyber threat, often involving social engineering techniques, where attackers meticulously research and understand their target audience to craft more convincing lures. As stated by Tian et al. (2018), phishing messages are frequently made to appear as if they are from trustworthy entities (e.g., banks, credit card companies, shipping firms, or social networking sites). Attackers have become adept at convincingly masquerading various internet elements, such as email addresses, the content of emails, and website URLs (Parsons et al., 2019). Several articles have been dedicated to identifying factors associated with phishing risk awareness. For instance, Gavett et al. (2017) explored how individual and geographic factors relate to phishing threat risk, focusing on variables like age, gender, ethnicity, location, knowledge, awareness, and observational behavior. The research indicated that older participants were more knowledgeable and aware of phishing threats than their younger counterparts and noted that the difference in location, such as being in a lab versus at home, influenced phishing risk awareness. Besides, Parsons et al. (2013) assessed the ability of individuals to differentiate between phishing and genuine emails, involving 117 participants. Half of the participants were informed that their ability to detect phishing emails was being assessed. The findings revealed that those aware of the context of the phishing study were more accurate in identifying phishing emails and took longer to make decisions than those uninformed. Notably, participants with training and knowledge in information systems were more adept at detecting phishing attempts.

Technology Acceptance Model (TAM)

There are several research on technology acceptance, such as TAM (technology acceptance model) and UTAUT (unified theory of acceptance and use of technology), to understand psychological constructs and factors influencing user adoption of innovation (Hong et al., 2021; Rahimi et al., 2018; Venkatesh et al., 2016). Although UTAUT attempts to synthesize psychological constructs from related prominent theories such as TRA (theory of reason action) (Fishbein & Ajzen, 2009), TPB (theory of planned behavior) (Ajzen, 1991), and TAM with several demographic factors, TAM is still a widely used model for predicting user adoption of innovation due to its usability and understandability (Vukovic et al., 2019). Several TAM

versions and extensions have been proposed (Khlaisang et al., 2021; Park & Park, 2020; Tuah et al., 2022). TAM proposes a framework where perceived ease of use (PEOU) is posited to influence perceived usefulness (PU) as well as attitude towards using (ATT). Additionally, PU is theorized to significantly affect ATT, highlighting the interdependence between ease of use and perceived utility in shaping user attitudes. ATT also impacts intention to use (ITU) or behavioral usage (USE).

Besides TAM constructs, several researchers extended various demographic and psychological factors on TAM and summarized that these factors should be considered to predict user adoption of innovation. For example, Lai and Zainal (2015) extended TAM with a condition of perceived risk to identify its relationship with consumers' intention to use the e-payment system. The author claimed that perceived risk should be considered an essential factor as it strongly affects the intention to use compared with other conditions, such as perceived ease of use and perceived usefulness. In Mutahar et al. (2022), a condition of perceived risk is included in TAM to understand the relationship of perceived risk with TAM constructs concerning mobile banking adoption in developing countries. In this work, perceived risk represents its moderate association with PU only, but there are significant relationships between PEOU and PU. Furthermore, these two constructs are also associated with USE. In addition, Riantini and Wandrial (2018) conducted an experiment on e-banking adoption in South Tangerang using TAM and discovered that TAM constructs influenced the actual use of e-banking services.

In cybersecurity, Hanif and Lallie (2021) explored the influence of cybersecurity factors on the willingness of the older generation in the UK to utilize mobile banking applications. They adopted the UTAUT model, adding variables such as perceived cybersecurity risk, trust, and overall cybersecurity. Employing a mixed-methods approach, the study analyzed data from 191 participants using partial least squares structural equation modeling and thematic analysis. The results showed that performance expectancy and perceived cybersecurity risk are the main factors determining the intention to use mobile banking applications among the older population in the UK. In addition, Seuwou et al. (2016) critically reviewed technology acceptance models (TAM) and theories, exploring external variables influencing information security investment.

Phishing Risk Awareness in Academic Institutions

University A and university B serve as the focal academic institutions in this study. University A is in Phuket, a region characterized by a competitive economy and high cost of living, making it one of Thailand's most expensive areas. Phuket is globally recognized as a prime tourist destination, heavily reliant on the tourism industry, which annually attracts more than ten million tourists, 70% of whom are foreign, significantly contributing to Thailand's revenue. The government has also targeted Phuket for several national development strategies, including initiatives to transform it into a smart city and an international seminar center (Meetings, Incentives, Conferencing, and Exhibitions: MICE). This university hosts approximately four hundred fifty academic personnel.

In contrast, university B is situated in Sakon Nakhon, a province surrounded by mountains, forests, swamps, and extensive lakes. Known for its elderly population and high quality of life, Sakon Nakhon boasts a competitive economy with a low cost of living. The region serves as a pilot city for numerous sufficient economy projects. It primarily earns its income from agriculture, with significant crops including rice, cassava, sugar cane, rubber, and various horticulture crops, alongside local livestock raised by small farmers for supplemental income. Sakon Nakhon is also nationally recognized as a center of Buddhist learning, offering guidance on spiritual peace practices. Despite its rich cultural offerings, the province's total tourism income is comparatively low, with less than seven hundred million baht generated annually from national and foreign tourists.

Research Variables

This study aims to understand phishing threat awareness among academic staff in two Thai universities by utilizing TAM to comprehensively understand how various factors influence perceived phishing risk (PR) and phishing risk awareness (PHA). This research seeks to enrich behavioral science literature by introducing a new dimension to phishing awareness studies to dissect the complex interaction between human behavior and technological threats. It aims to inform the development of more effective, contextually tailored cybersecurity education and policies in academic institutions in Thailand. In structural equation modeling (SEM), like in TAM, variables are often categorized into endogenous and exogenous. Exogenous variables are not influenced by any other variable within the model's scope. They are the independent variables from which causal influences originate in the model. In contrast, endogenous variables are the variables within a model that are influenced by other variables. They are the dependent variables in the model, receiving and manifesting effects from the exogenous variables. In the TAM framework of this research, the endogenous variables include 1) PEOU serves as a starting point for influencing other variables such as PU and ATT; 2) PR acts independently to influence PU, ATT, USE, and PHA. On the other hand, there are four endogenous variables: 1) PU is influenced by Perceived Ease of Use (PEOU) and influences ATT; 2) ATT is influenced by PEOU and PU and also influences USE; 3) USE is influenced by ATT and PR and affects PHA; and 4) PHA is influenced by USE and PR.

Research Hypotheses

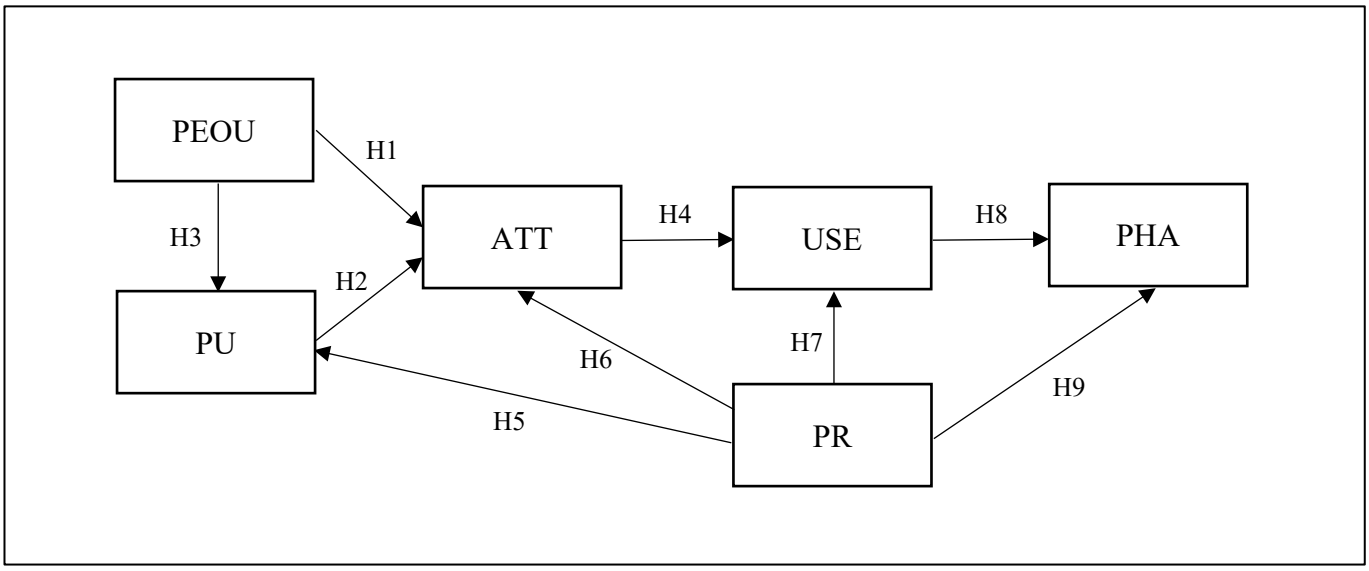
This research posits that TAM can effectively elucidate phishing risk awareness among academic staff, with perceived phishing risk and phishing risk awareness as reliable indicators. The study proposes nine hypotheses: H1) PEOU influences ATT; H2) PU influences ATT; H3) PEOU influences PU; H4) ATT influences USE; H5) PR influences PU; H6) PR influences ATT; H7) PR influences USE; H8) USE influences PHA; and H9) PR influences PHA.

Conceptual Framework

Based on the formulated hypotheses, Figure 1 illustrates the research framework, depicting the relationships among the factors utilized in the study, ranging from H1 to H9.

Figure 1

Research Framework



Note. PEOU (perceived ease of use), PU (perceived usefulness), ATT (attitude towards using), USE (behavioral usage or phishing observation behavior), PR (perceived phishing risk), PHA (phishing risk awareness)

Method

This section outlines the specific methodology employed in conducting this research.

Sample

This study distributed the questionnaire to the academic staff of two universities selected for comparative analysis. The selection of the two universities for this research was strategically aligned with the study's objectives to examine how socioeconomic factors influence phishing threat awareness. University A, situated in Phuket, a southern province of Thailand, offers a setting rich in economic activity and advanced technological exposure, potentially affecting its academic staff's digital literacy and cybersecurity awareness. In contrast, university B is in Sakon Nakhon, a less affluent, predominantly agricultural region in the upper northeast, presenting a starkly different socioeconomic landscape that likely influences the staff's exposure to and understanding of digital threats. This deliberate contrast provides a comprehensive framework to examine the impact of socioeconomic backgrounds on cybersecurity awareness, enabling the study to test the applicability of behavioral theories like the TAM across diverse settings and enhance the generalizability of its findings to other academic institutions within similar socioeconomic contexts. It is essential to highlight that before this research, neither university A nor B had participated in cybersecurity awareness training programs. Each university employs approximately 450 academic staff members. The study's sample comprised 400 participants, with 200 from each university, distributed equally following the Taro Yamane sampling method (Yamane, 1973). Participants were selected from five faculties in proportions reflective of their respective sizes.

Instruments

The research utilized questionnaires to assess the knowledge and experiences of the participants regarding phishing threats. Since the questionnaire must be translated from English to Thai, three university lecturers proficient in both languages validated both versions to ensure that the Thai and English versions were semantically and syntactically consistent before the Thai version was employed for this research. The questionnaire consists of six straightforward yes-or-no questions to provide a basic understanding of the participants' awareness and experiences with phishing. The initial question asked participants if they had heard of the term 'phishing'. Subsequent questions delve into whether they can define phishing and identify its correct meaning. Participants are then asked about their personal experiences with phishing, if these experiences have influenced their online behavior, and whether they feel they possess adequate knowledge to safeguard themselves against phishing threats. Additionally, the questionnaire probes for any observations of online anomalies like unusual messages, links, and content. To gauge perceived phishing risk (PR), the questionnaire includes two questions on a 7-point scale, ranging from 1 (extremely low) to 7 (extremely high), assessing the participants' perceived likelihood and impact of phishing. To assess phishing risk awareness (PHA), participants were presented with 21 questions requiring them to discern between genuine and phishing screens. These phishing screens are designed to closely resemble authentic ones, making distinguishing them challenging. Before deployment, the research instrument undergoes rigorous testing by statistical data collection and cybersecurity experts. This pre-testing phase ensures the reliability of the questionnaire before it is administered to the targeted academic personnel from both universities.

The data were analyzed using R, a programming language widely used for data analysis and visualization (R Core Team, 2022). In addition, Lavaan, another essential R package for structural equation modeling (SEM) analysis (Rosseel, 2012), was mainly used for path coefficient analysis and representation of TAM constructs. A series of question items related to TAM constructs were created based on the rating scale to choose between 1 and 7. PEOU, PU, ATT, and USE question items were designed according to TAM. For example, PEOU means perceived ease of phishing observation instead of innovation. Similarly, PU questions were related to the perceived usefulness of phishing. ATT question items were designed to test attitudes toward phishing observations. Finally, USE question items were based on their frequency of

observing phishing. After that, PR and PHA were tested with TAM to understand the factors underlying phishing risk awareness of academic staff.

Procedure

This research employs two main methods of data analysis: descriptive statistics and structural equation modeling. The descriptive statistics are based on paired sample comparisons between the two universities. This comparison assesses participants' knowledge and experiences concerning phishing threats through a series of questions. Additionally, participants are asked to rate the likelihood and impact of phishing threats on a 7-point scale, ranging from extremely low (1) to extremely high (7). For calculating perceived risk (PR), a risk assessment metric is applied where risk is the product of likelihood and impact (Patterson et al., 2023). The resulting value is then divided by 7 to align with the rating scale, providing a quantifiable PR degree. The number of participants from both universities falling into the three highest degrees of risk perception (extremely high, very high, and high) is then compared to ascertain which university personnel exhibit higher levels of perceived risk. To determine phishing risk awareness (PHA), the study measures the number of participants correctly identifying a screen as phishing. This measurement is based on the principle that anyone, regardless of their vigilance, can fall victim to phishing if they become complacent or less aware of such threats. The total count of correct identifications is then divided into three segments on the 7–point scale, categorizing responses into seven levels of awareness: 1) extremely low (1–3); 2) very low (4–6); 3) low (7–9); 4) medium (10–12); 5) high (13–15); 6) very high (16–18); and 7) extremely high (19–21).

All question items related to TAM constructs were analyzed using the coefficient of confidence by the Cronbach technique (Cronbach, 1951). This process is to ensure that each construct contains consistent question items on an acceptance threshold of a coefficient of confidence of .70 or greater on a basis between $\alpha < .50$ (no reliability) and $\alpha \geq .90$ (high reliability). Apart from the TAM constructs, PHA was positioned after USE to determine the relationship between USE and PHA. In addition, PR was observed if there were relationships between PR and PU, ATT, USE, and PHA, respectively. For factors underlying risk awareness of phishing threats, the data analysis utilizes SEM to analyze the correlation coefficient between factors tested in the hypothesis framework through path analysis. The collected data were analyzed to determine PR and PHA and their correlations with TAM constructs. Furthermore, several model fit indices are analyzed to prove that the tested data is consistent with the relationship of the variables based on the hypotheses (Shi et al., 2019; Shi & Maydeu-Olivares, 2020). For instance, comparative fit index (CFI) measures the relative improvement in the fit of a user-specified model compared to a more restricted baseline model. goodness of fit index (GFI) is similar to the R-squared statistic in regression, measuring the proportion of variance explained by the model. Tucker Lewis index (TLI) compares the chi-square value of the model to the chi-square value of the null model, adjusting for model complexity (i.e., the number of parameters estimated). While root mean square error of approximation (RMSEA) assesses fit per degree of freedom in the model, allowing for the complexity of the model, standardized root mean square residual (SRMR) is the standardized difference between the observed correlation and the predicted correlation. It measures the average magnitude of the standardized residuals between the observed and predicted covariances or correlations (Shi & Maydeu-Olivares, 2020).

Data Representation

The study began by analyzing and comparing the proportions of perceived phishing likelihood, perceived phishing impact, perceived phishing risk (PR), and phishing risk awareness (PHA) between university A and university B to discern differences in perceptions of phishing threats. To evaluate the proposed hypotheses, the analysis was initiated by determining the reliability of the questionnaire items associated with TAM constructs, employing Cronbach's alpha (Cronbach, 1951). Following this, the adequacy of the model was assessed through five previously mentioned fit indices: CFI, GFI, TLI, RMSEA, and SRMR. These indices thoroughly evaluated the model's conformity to the empirical data. After that, PR and PHA were exhibited in a path analysis following the proposed conceptual framework in Figure 1.

These formulated hypotheses from H1 to H9, framed under the TAM constructs, are integral to representing the main hypotheses of our study. This study assesses whether all constructs within TAM retain their validity and whether PR and PHA are effective indicators for understanding perceptions toward phishing threats.

Ethical Considerations

The research tools utilized in this study underwent a comprehensive ethical evaluation. The thorough review process underscores the commitment to upholding ethical standards in research, ensuring the integrity and responsibility of the study methods and practices. The participants were informed about the experiment's objectives and rights within the research context. These rights include the option to decline participation in the research at any stage before submitting their information to the research team. Additionally, they were assured that the questionnaire was designed to avoid collecting referable information, ensuring that no personal data would be gathered. Furthermore, participants were assured of the confidentiality of their information, with guarantees that it would not be disclosed to anyone outside of the research team.

Results

The findings presented in this section commence by examining perceived phishing likelihood, perceived phishing impact, perceived phishing risks, phishing risk awareness, model reliability, and factors influencing phishing risk awareness.

Perceived Phishing Likelihood

Since the risk of a threat could be measured by the multiplication of the threat likelihood and impact, the probability of phishing threats had been one of the critical factors in estimating the risk perception level of both university personnel. From the total sample (n = 400), 13% (52 participants) perceived the likelihood of phishing as extremely high, 9.25% (37 participants) as very high, and 25.75% (103 participants) as high. When these levels were categorized according to the universities, participants from university B had reported higher phishing likelihood levels in terms of extremely high (34 or 17%), very high (20 or 10%), and high (45 or 22.50%) than those from university A. In comparison, 18 (9%), 17 (8.5%), and 58 (29%) participants from university A believed that the phishing likelihood was extremely high, very high, and high, respectively.

Perceived Phishing Impact

Besides the potential of phishing threats, perceptions of phishing impact were categorized as follows: 18% (72 participants) rated the impact as extremely high, another 18% (72 participants) as very high, and 23.50% (94 participants) as high from the entire sample (n = 400). In detail, university A's participants responded that 30, 32, and 52 participants perceived the phishing impact as extremely high, very high, and high, equivalent to 15%, 16%, and 26% of the university's total samples. In contrast, 42 (21%) participants from university B believed that the phishing impact was extremely high. Furthermore, 40 (20%) and 42 (21%) participants from university B perceived the phishing impact as very high and high in the university's total samples, respectively.

Perceived Phishing Risks

Once the likelihood and impact of phishing threats perceived by participants from both universities had been concluded, the perceived phishing risk was calculated based on these two factors, following the methods mentioned earlier. From the total sample (n = 400), the distribution of participants according to their level of perceived phishing risk was as follows: 19.25% (77 participants) reported an extremely high level of awareness, 17.25% (69 participants) a very high level, and 21.50% (86 participants) a high level. When these perceived phishing risk levels were categorized according to the university, participants from university B had higher phishing risk perception levels in terms of extremely high, very high, and high than

those from university A. Among university B's participants, there were 49 (24.50%), 36 (18%), and 51 (25.50%) with extremely high, very high, and high phishing risk perceptions of the university's total samples, respectively. In contrast, participants from university A responded that 28, 33, and 35 participants perceived phishing risks as extremely high, very high, and high, equivalent to 14%, 16.50%, and 17.50% of the university's total samples.

Phishing Risk Awareness

The awareness of phishing threats was assessed through 21 questions, with the results calculated using the previously described methods to maintain consistency with the earlier measurements of perceived phishing risks. From the total sample ($n = 400$), the data indicated that 8.75% (35 participants) demonstrated an extremely high level of phishing awareness, 8.25% (33 participants) a very high level, and 14% (56 participants) a high level. When these levels of phishing awareness were broken down by university affiliation, it was observed that participants from university B demonstrated higher levels of awareness in the categories of extremely high, very high, and high compared to those from university A. Specifically, within university B, 23 participants (11.50% of the university's sample) showed extremely high awareness, 20 participants (10%) showed very high awareness, and 23 participants (11.50%) showed high awareness. On the other hand, at university A, the numbers were lower, with 12 participants (6% of the university's sample) showing extremely high awareness, 13 participants (6.50%) showing very high awareness, and 33 participants (16.50%) showing high awareness. These statistics highlight a notable difference in the level of phishing threat awareness between the two universities.

Reliability of the Model

The overall confidence of all TAM construct question items with Cronbach's alpha was .93, considered an excellent range for data-consistent outcomes. The reliability of all question items could be accepted without removing any questions. Furthermore, question items of each construct represented the mean in the same direction. After this stage, PR and PHA conditions were experimented with these TAM constructs according to the hypothesized model. The results also indicated acceptable fit values [GFI = 1.00; TLI = .93; CFI = .97; SRMR = .05]. Therefore, the hypothesized model was considered an acceptable fit. However, the RMSEA at .094 was slightly higher than the acceptable fit at .08. The path coefficients linking all factors in the model indicated that these factors shared statistically significant relationships. Table 1 shows the fit indices' requirements for good and acceptable fit.

Table 1

Example of SEM Fit Indices

Fit Indices	Good Fit	Acceptable Fit	Research Framework
CFI	$.95 \leq CFI \leq 1.00$	$.90 \leq CFI < 1.00$	0.97
GFI	$.95 \leq GFI \leq 1.00$	$.90 \leq GFI < 1.00$	1.00
TLI	$.95 \leq TLI \leq 1.00$	$.90 \leq TLI < 1.00$	0.93
RMSEA	$0 \leq RMSEA \leq .05$	$.05 \leq RMSEA \leq .08$	0.94
SRMR	$0 \leq SRMR \leq .05$	$.05 \leq SRMR \leq .08$	0.05

Note. comparative fit index (CFI), goodness of fit index (GFI), Tucker Lewis index (TLI), root mean square error of approximation (RMSEA), standardized root mean square residual (SRMR).

Hypothesis Testing Results

The SEM was used to analyze the hypotheses in Table 2. The results yielded the validity of the relationships among TAM constructs. From H1 to H4, all TAM constructs were also positively correlated with each other. For example, PEOU had influenced ATT ($\beta = .25$, $p < .001$), PU was associated with ATT ($\beta = .57$, $p < .001$), PEOU had influenced PU ($\beta = .52$, $p <= .001$), and ATT had influenced USE ($\beta = .14$, $p = .01$). From H5 to H9, however, PR and PHA illustrated some interesting relationships with TAM

constructs. While PHA was positioned after USE, PR would be tested with PU, ATT, USE, and PHA. PR had represented influences on PU, ATT, and USE at (β = .09, p = .004), (β = .07, p < .001), and (β = .15, p < .001), respectively. Although the results did not indicate significant effects, these low correlations should not have been ignored, as perceived usefulness, attitude towards using, and behavioral usage of phishing observations were associated with perceived risks.

Table 2
The Model's Parameter Estimations

Regression	Estimate	Std.Err	Std.lv	Std.all
PHA ~				
USE	-.09	.07	-.09	-.06
PR	.17***	.05	.17	.17
USE ~				
ATT	.14**	.05	.13	.13
PR	.15***	.03	.15	.20
ATT ~				
PU	.57***	.03	.57	.63
PEOU	.25***	.03	.25	.29
PR	.07***	.02	.07	.10
PU ~				
PEOU	.52***	.04	.52	.54
PR	.09**	.03	.09	.12

Note. n = 400, * p < .05, ** p < .01, *** p < .001.

Interestingly, an insignificantly negative influence from USE to PHA (β = -.09, p = .20) implied that academic staff who frequently observed phishing elements were unaware of phishing threats. In contrast, a slightly positive influence from PR to PHA (β = .17, p = .001) indicated that PR was a more robust indicator than USE for understanding risk awareness towards phishing threats. This suggests that an individual's awareness of phishing threats is more closely linked to their perception of risk than their direct observation of phishing incidents. It indicates that enhancing individuals' understanding of the potential risks associated with phishing could be more effective in raising awareness than simply increasing exposure to phishing incidents.

Discussion and Conclusion

The findings of this study revealed the importance of understanding phishing risk awareness in academic settings. For instance, participants from university B, situated in Sakon Nakhon, exhibited greater perceived phishing likelihood, higher assessments of phishing impact, and elevated levels of phishing awareness compared to their counterparts at university A in Phuket. Specifically, individuals at university B reported higher general awareness and assessed the impact of phishing as extremely high more frequently than those at university A. Additionally, the overall awareness of phishing threats was notably greater among participants from university B, reinforcing the distinction in phishing threat perception between the two universities. The results are consistent with Orunsolu et al. (2018), who asserted that factors, such as the economic status and technological exposure of the universities' regions, significantly influence staff awareness and perception of phishing threats (Orunsolu et al., 2018). This aligns with behavioral science theories that suggest environment and socioeconomic conditions shape human behavior and risk perception (Slovic, 1987). By applying these theories to cybersecurity, our research bridges a crucial gap, highlighting how phishing, often viewed merely as a technological threat, is rooted in socioeconomic and psychological factors (Abroshan et al., 2021).

The findings demonstrate the relevance of psychological factors in cybersecurity awareness. The variation in phishing risk awareness among the staff of the two universities can be partly explained through cognitive biases and risk perception theories. For example, staff in a more technologically exposed environment may develop a false sense of security or familiarity bias, impacting their perception of phishing risks (Abroshan et al., 2021; Orunsolu et al., 2018). This finding also aligns with Gavett et al. (2017), who noted that the difference in geographical location can influence awareness levels of phishing threats. Although university A's participants demonstrated a higher level of understanding and experience with phishing threats than those at university B, it does not necessarily imply a corresponding increase in their risk perception and awareness. This observation challenges the notion held by some researchers, such as Parsons et al. (2019), who suggest that those trained and knowledgeable in information systems are more adept at identifying phishing emails. The outcomes of this study resonate with the argument by Slovic (1987), who posited that individuals might underestimate everyday risks due to familiarity and confidence in managing these risks. This insight is a pivotal contribution of our research to the field of behavioral science, as it extends the application of these theories to cybersecurity.

Discussion of Main Results

TAM, traditionally used to understand technology adoption, can be utilized to explore how academic staff perceive and react to phishing threats. The findings corroborate the validity of TAM constructs, as evidenced by numerous scholarly research efforts (Lai & Zainal, 2015; Mutahar et al., 2022; Park & Park, 2020; Tuah et al., 2022). Specific relationships, such as PEOU influencing PU, PU impacting ATT, PEOU affecting ATT, and ATT influencing USE, are all supported. However, the study notes that ATU exerts only a minor influence on USE, suggesting a nuanced dynamic in the context of phishing observation behavior. This observation implies that while participants hold positive attitudes towards phishing observation, these attitudes do not necessarily translate into strong behavioral responses. This discrepancy underscores the need for further exploration into additional factors that may bridge the gap between phishing observation attitudes and actual phishing observation behavior in cybersecurity.

When participants were assessed using TAM constructs, the findings corroborated the validity of the TAM, consistent with prior research (Khlaisang et al., 2021; Park & Park, 2020; Tuah et al., 2022; Vukovic et al., 2019). For instance, PEOU was found to influence ATT, PU influenced ATT, PEOU impacted PU, and ATT influenced USE. However, the analysis revealed intriguing dynamics when PR and PHA were incorporated into the model. Although the research anticipated identifying significant relationships between PR and ATT and between PR and PHA, the findings indicated that these relationships are relatively minor. This outcome suggests that while perceived phishing risk influences attitudes towards phishing observation behavior and phishing risk awareness, the strength of these influences is less pronounced than initially expected. This observation can be attributed to the fact that perceived risks are intricately linked to an individual's knowledge and confidence about these risks, which play a pivotal role in shaping perceptions and understanding the emotional dimensions associated with risk evaluation. As noted by Kasperson et al. (2003) and Slovic (1987), perceived risks may be underestimated or exaggerated, thereby potentially being assigned more or less value compared to unknown risks. This discrepancy underscores the complex interplay between cognitive assessments and emotional responses in perceiving risks. In addition, these results underscore the need to broaden the investigation scope to include a wider array of variables that might affect the dynamics of perceived phishing risk and phishing observation behavior.

Nevertheless, the results revealed that PR exerts a stronger influence on USE than ATT's influence on USE. Additionally, PR had a more substantial impact on PHA than USE did on PHA. These results highlight the significant role of perceived risk within the framework of phishing risk awareness and phishing observation behavior. This significant impact of PR suggests that understanding and addressing the perceived risks associated with phishing are paramount in influencing the practical engagement with cybersecurity measures and the awareness levels of potential threats. This observation advocates for the integration of perceived phishing risk within cybersecurity education and policy development, aiming to

enhance the effectiveness of interventions designed to mitigate phishing risks. This aligns with the findings of Lai and Zainal (2015), who asserted that perceived risk should be considered when designing e-payment systems. Similarly, Mutahar et al. (2022) argued that perceived risk should be incorporated into the Technology Acceptance Model (TAM) to elucidate its relationship with TAM constructs in the context of mobile banking adoption.

Limitations

This research has illustrated that using TAM within a security context is crucial for broadening our understanding of behavioral responses to cyber threats. Such research can be instrumental in organizations identifying and overcoming barriers to adopting and complying with security measures. These barriers might include trust in the security systems (Hanif et al., 2021). Besides, it would be helpful to explore whether similar patterns of awareness exist in corporate or public sectors and how these compare to the academic context. Additionally, considering cultural factors is crucial, especially given the Thai context of the study. Thailand's unique cultural attributes, such as communication styles and societal values, might influence the perception and response to phishing threats. These cultural nuances could offer a deeper understanding of the findings and their implications (Patterson et al., 2023). Continued research and experimentation into cyber threats' varying security awareness levels across different demographic groups may yield more significant implications for behavioral science.

Implications for Behavioral Science

This study demonstrates significant contributions and implications to behavioral science by applying the TAM to understand cybersecurity awareness, focusing on risk factors such as perceived phishing risks and phishing risk awareness. Firstly, the results underscore that PEOU significantly influences ATT, indicating that ease of phishing observation is likely to foster more positive attitudes towards phishing observation. Additionally, the results reveal that PU significantly affects ATT, suggesting that perceived benefits of phishing observation play a crucial role in shaping user attitudes. Additionally, the study demonstrates that PEOU positively influences PU, indicating ease of phishing observation can enhance the perceived benefits of phishing observation. The results reveal that ATT exerts a modest influence on USE, suggesting that while positive attitudes towards phishing observation are important, they do not overwhelmingly predict actual phishing observation behavior in this research. The study revealed that frequent observations of phishing elements do not necessarily correlate with heightened user awareness of phishing threats. This finding aligns with Beu et al. (2023), who asserted that lower detection accuracy of phishing emails modestly predicted riskier cybersecurity behavior.

Primarily, the results reveal that integrating TAM constructs with experimental conditions like PR and PHA could enhance the understanding of factors influencing academic staff's phishing risk awareness. The results indicate a notably higher influence of PR on USE compared to the influence of ATT on USE. Additionally, PR also shows a stronger impact on PHA than USE on PHA, even though these influences are relatively modest. These findings highlight the critical role of perceived risk in driving the actual phishing observation behavior and the awareness of potential threats associated with it (Lai & Zainal, 2015). This suggests that individuals' perceived risk significantly shapes their phishing observation and phishing risk awareness levels, potentially more so than their general attitudes toward phishing observation.

This study underscores the need for further PR and PHA experiments within TAM or other related models to validate these results for understanding and improving human behavior in cybersecurity, particularly in academic environments. This research thus contributes to behavioral science by highlighting how individuals perceive and respond to cyber threats and proposing avenues for future research to deepen our understanding in this area. Understanding the factors influencing user behavior within security contexts is essential for organizations aiming to formulate more effective, user-centered security strategies that are likely to be embraced and adhered to by employees and other stakeholders. Integrating behavioral insights into cybersecurity strategies enables organizations to better understand the perceptions and interactions of

different user groups with security protocols. Hillman et al. (2023) highlighted that the importance of employee awareness and proactive behavior in cybersecurity will remain critical in the foreseeable future.

Conclusion

In conclusion, this research has offered a comparative analysis of the academic staff from university A and university B, revealing distinct perceptions and behaviors regarding phishing threat awareness. Academic staff at university B demonstrated a higher level of perceived risk and phishing awareness than those at University A, suggesting that regional or institutional contexts might influence cybersecurity awareness and behaviors. Furthermore, the study substantiated the foundational principles of TAM by demonstrating significant interrelationships among its constructs, such as PEOU, PU, and ATT, and their collective impact on USE. However, the research uniquely highlighted the modest influence of ATU on USE within the context of phishing threat awareness. This divergence from typical TAM predictions suggests that while positive attitudes towards phishing observation are necessary, they may not be sufficient to predict robust phishing observation behavior, particularly in security and risk areas. Moreover, the stronger impact of perceived phishing risk on phishing observation behavior and phishing awareness than traditionally observed attitudinal impacts suggests that perceived phishing risk plays a critical role in shaping both behavioral intentions and awareness of phishing threats. These insights underscore the importance of incorporating risk assessment components into designing and implementing technological solutions and cybersecurity measures.

Declarations

Funding: The authors thank the National Research Council of Thailand (NRCT) and Phuket Rajabhat University (PKRU) for their financial support.

Conflicts of Interest: The authors declare no conflicts of interest.

Ethical Approval Statement*:* The study was conducted in accordance with the Declaration of Helsinki, and approved by the Institutional Review Board (or Ethics Committee) of Phuket Rajabhat University (PKRU 2019-002, 10 May 2019) for studies involving humans.

References

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. *IEEE Access, 9*, 44928–44949. https://doi.org/10.1109/ACCESS.2021.3066383

Ajzen, I. (1991). The theory of planned behavior. *Organisational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Beu, N., Jayatilaka, A., Zahedi, M., Babar, M. A., Hartley, L., Lewinsmith, W., & Baetu, I. (2023). Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation. *Computers & Security*, *131,* 103313. https://doi.org/10.1016/j.cose.2023.103313

Cronbach, L. (1951). Coefficient alpha and the internal structure of tests. *Psychomerika, 16*, 297–334. https://doi.org/10.1007/BF02310555

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

Davis, F. D. (1993). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies*, *38*(3), 475–487. https://doi.org/10.1006/imms.1993.1022

Diaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia, 44*, 53–67. https://doi.org/10.1080/01611194.2019.1623343

Fishbein, M., & Ajzen, I. (2009). *Predicting and changing behavior: The reasoned action approach*. Psychology Press. https://doi.org/10.4324/9780203838020

Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PLoS ONE*, *12*(2), 1-16. https://doi.org/10.1371/journal.pone.0171620

Hanif, Y., & Lallie, H. S. (2021). Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM - with perceived cyber security, risk, and trust. *Technology in Society*, *67,* 101693. https://doi.org/10.1016/j.techsoc.2021.101693

Hillman, D., Harel, Y., & Toch, E. (2023). Evaluating organizational phishing awareness training on an enterprise scale. *Computers & Security*, *132,* 103364. https://doi.org/10.1016/j.cose.2023.103364

Hong, X., Zhang, M., & Liu, Q. (2021). Preschool teachers' technology acceptance during the Covid-19: An adapted technology acceptance model. *Frontiers in Psychology*, *12*, 691492. https://doi.org/10.3389/fpsyg.2021.691492

Kasperson, J., Kasperson, R., Pidgeon, N., & Slovic, P. (2003). The social amplification of risk: Assessing fifteen years of research and theory. *The Social Amplification of Risk* (pp. 13–46). Cambridge University Press. https://doi.org/10.1017/CBO9780511550461.002

Khlaisang, J., Teo, T., & Huang, F. (2021). Acceptance of a flipped smart application for learning: A study among Thai university students. *Interactive Learning Environments, 29*(5), 772–789. https://doi.org/10.1080/10494820.2019.1612447

Lai, P. C., & Zainal, A. B. A. (2015). Perceived risk as an extension to TAM model: Consumers' intention to use a single platform e-payment. *Australian Journal of Basic and Applied Sciences*, *9,* 323–331. https://doi.org/10.1177/2319510X18776405

Leesa-Nguansuk, S. (2022). *Thailand leads in e-shop phishing*. Bangkok Post. https://www.bangkokpost.com/business/2341932/thailand-leads-in-e-shop-phishing

Musuva, P. M. W., Getao, K. W., & Chepken, C. K. (2019). A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility. *Computers in Human Behavior*, 94, 154–175. https://doi.org/10.1016/j.chb.2018.12.036

Mutahar, A. M., Aldholay, A., Isaac, O., Jalal, A. N., & Kamaruddin, F. E. B. (2022). The moderating role of perceived risk in the technology acceptance model (TAM): The context of mobile banking in developing countries. In M. Al-Emran, M. A. Al-Sharafi, M. N. Al-Kabi, & K. Shaalan (Eds.), *Proceedings of International conference on emerging technologies and intelligent systems* (pp. 389–403). Springer. https://doi.org/10.1007/978-3-030-82616-1_34

Naagas, M. A., Mique, E. L., Palaoag, T. D., & Dela Cruz, J. S. (2018). Defense-through-deception network security model: Securing university campus network from DOS/DDOS attack. *Bulletin of Electrical Engineering and Informatics*, *7*(4), 593–600. https://doi.org/10.11591/eei.v7i4.1349

NCSA Annual Report 2022. (2023). *National cyber security agency*. https://drive.ncsa.or.th/s/5pNCYTM9sQ46SZF

Orunsolu, A., Afolabi, O., Sodiya, S., & Akinwale, A. (2018). A users' awareness study and influence of socio-demography perception of anti-phishing security tips. *Acta Informatica Pragensia*, *7*(2), 138–151. https://doi.org/10.18267/j.aip.119

Park, E. S., & Park, M. S. (2020). Factors of the technology acceptance model for construction IT. *Applied Sciences*, *10*(22), 8299. https://doi.org/10.3390/app10228299

Parsons, K., Delfabbro, P., Lillie, M., & Butavicius, M. (2019). Predicting susceptibility to social influence in phishing e-mails. *International Journal of Human-Computer Studies*, *128*, 17–26. https://doi.org/10.1016/j.ijhcs.2019.02.007

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). Phishing for the truth: A scenario-based experiment of users' behavioural response to e-mails. In L. J. Janczewski, & H. B. Wolfe, S. Shenoi (Eds.), *Security and privacy protection in information processing systems, SEC 2013, Advances in information and communication technology* (Vol. 405). Springer. https://doi.org/10.1007/978-3-642-39218-4_27

Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*, *132*, 103309. https://doi.org/10.1016/j.cose.2023.103309

R Core Team (2023). *R: A language and environment for statistical computing*. R Foundation for Statistical Computing. https://www.R-project.org

Rahimi, B., Nadri, H., Afshar, H. L., & Timpka, T. (2018). A systematic review of the technology acceptance model in health informatics. *Applied Clinical Informatics*, *9*(3), 604–634. https://doi.org/10.1055/s-0038-1668091

Riantini, R. E., & Wandrial, S. (2018). Adoption of e-banking services in south Tangerang using technology acceptance model (TAM) approach. *Pertanika Journal of Social Sciences & Humanities*, *26*(T), 161–172. http://www.pertanika.upm.edu.my/pjssh/browse/regular-issue?article=JSSH-T0718-2018

Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024). Which factors predict susceptibility to phishing? An empirical study. *Computers & Security*, *136,* 103558. https://doi.org/10.1016/j.cose.2023.103558

Rosseel, Y. (2012). Lavaan: An R package for structural equation modeling. *Journal of Statistical Software*, *48*(2), 1–36. https://doi.org/10.18637/jss.v048.i02

Seuwou, P., Banissi, E., & Ubakanma, G. (2016). User acceptance of information technology: A critical review of technology acceptance models and the decision to invest in information security. In H. Jahankhani, A. Carlile, D. Emm, A. Hosseinian-Far, G. Brown, G. Sexton, & A. Jamal (Eds.), *Global security, safety and sustainability—The security challenges of the connected world* (pp. 230–251). Springer International Publishing. https://doi.org/10.1007/978-3-319-51064-4_19

Shi, D., Lee, T., & Maydeu-Olivares, A. (2019). Understanding the model size effect on SEM fit indices. *Educational and Psychological Measurement, 79*(2), 310–334. https://doi.org/10.1177/0013164418783530

Shi, D., & Maydeu-Olivares, A. (2020). The effect of estimation methods on SEM fit indices. *Educational and Psychological Measurement*, *80*(3), 421–445. https://doi.org/10.1177/0013164419885164

Slovic, P. (1987). Perception of risk. *Science, 236*, 280–285. https://doi.org/10.1126/science.3563507

Tian, C., Jensen, M. L., & Durcikova, A. (2023). Phishing susceptibility across industries: The differential impact of influence techniques. *Computers & Security*, *135*, 103487. https://doi.org/10.1016/j.cose.2023.103487

Tuah, N. M., Yoag, A., Nizam, D. M., & Chin, C. W. (2022). A dashboard-based system to manage and monitor the progression of undergraduate IT degree final year projects. *Pertanika Journal of Science and Technology, 30*(1), 235–256. https://doi.org/10.47836/pjst.30.1.13

Vandebos, G. (2015). *APA dictionary of psychology* (2nd ed.). American Psychological Association.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems*, *17*(5), 328–376. https://doi.org/10.17705/1jais.00428

Vukovic, M., Pivac, S., & Kundid, D. (2019). Technology acceptance model for the Internet banking acceptance in Split. *Business Systems Research*, *10*(2), 124–140. https://doi.org/10.2478/bsrj-2019-022

Yamane, T. (1973). *Statistics: An introductory analysis* (3rd ed.). Harper and Row.