International Journal of
Environmental Research and Public Health

MDPI

Hypothesis

Thwarting Instant Messaging Phishing Attacks: The Role of Self-Efficacy and the Mediating Effect of Attitude towards Online Sharing of Personal Information

Yi Yong Lee, Chin Lay Gan * and Tze Wei Liew

Faculty of Business, Multimedia University, Melaka 75450, Malaysia
* Correspondence: gan.chin.lay@mmu.edu.my

Abstract: Context: The cause of cybercrime phishing threats in Malaysia is a lack of knowledge and awareness of phishing. Objective: The effects of self-efficacy (the ability to gain anti-phishing knowledge) and protection motivation (attitude toward sharing personal information online) on the risk of instant messaging phishing attacks (phishing susceptibility) are investigated in this study. The protection motivation theory (PMT) was tested in the context of attitudes toward sharing personal information online with a view to improving interventions to reduce the risk of phishing victimisation. Methods: Data were collected using non-probability purposive sampling. An online survey of 328 Malaysian active instant messaging users was collected and analysed in SmartPLS version 4.0.8.6 using partial least squares structural equation modelling. Results: The results showed that a person's cognitive factor (either high or low self-efficacy) affected their chance of being a victim of instant message phishing. A higher level of self-efficacy and a negative attitude towards sharing personal information online were significant predictors of phishing susceptibility. A negative attitude towards sharing personal information online mediated the relationship between high levels of self-efficacy and phishing susceptibility. A higher level of self-efficacy led to the formation of negative attitudes among internet users. Attitudes toward the sharing of personal information online are critical because they allow phishing attempts to exist and succeed. Conclusions: The findings give government agencies more information on how to organise anti-phishing campaigns and awareness programmes; awareness and education can improve one's ability to acquire anti-phishing knowledge (self-efficacy).

Keywords: self-efficacy; attitude; phishing susceptibility; anti-phishing knowledge; protection motivation theory

Citation: Lee, Y.Y.; Gan, C.L.; Liew, T.W. Thwarting Instant Messaging Phishing Attacks: The Role of Self-Efficacy and the Mediating Effect of Attitude towards Online Sharing of Personal Information. *Int. J. Environ. Res. Public Health* **2023**, *20*, 3514. https://doi.org/10.3390/ijerph20043514

Academic Editor: Heng Choon (Oliver) Chan

Received: 6 January 2023
Revised: 5 February 2023
Accepted: 10 February 2023
Published: 16 February 2023

1. Introduction

Internet communication technologies have changed the nature of para-social interaction from passive to an approximation of concrete or real social interaction [1]. Internet communication technologies (i.e., instant messaging applications) are the most popular social media applications among Malaysian citizens [2,3]. Sending daily messages, group messages, and other forms of communication via the internet has become a user's daily routine in order to facilitate social activities and relations [4,5]. Phishing, such as click baits (links or text embedded in messages or emails to entice users to view and read, with the intent of deceiving internet users), is an ongoing issue [6,7]. Clicking on attached links in instant messages without verifying the source could unintentionally lead internet users into a phishing trap [6,8,9]. According to the International Criminal Police Organization (also known as Interpol), phishing attacks in ASEAN countries show no signs of abating or slowing down [10]. Kaspersky, a cybersecurity and anti-virus software company, has successfully blocked over 1.6 million phishing attempts. This has kept internet users safe from phishing attacks in the modern era [10]. Kaspersky's anti-phishing systems stopped

12,127,692 malicious links in South-East Asia from January to June 2022, an increase of one million over the 11,260,643 malicious links that were discovered during the same time period in the previous year. Phishing attacks in South-East Asia (i.e., Malaysia) outnumbered those in the previous year [11]. Kaspersky also identified and thwarted 91,895 similar assaults in the first half of 2022 that were made against Malaysia's 27,458 banks [12]. In Malaysia, phishing threats are on the rise [13], and the majority of phishing victims were vulnerable to instant messaging phishing attacks [14–18]. In Malaysia, phishing attempts increased in the first six months of 2020, accounting for 749, 915 cases, compared to the first half of 2019 [10]. Phishing attacks on social media platforms increased by 20% in the second quarter of 2020, compared to the first three months of the year [10]. The phishing attacks were primarily motivated by attacks against WhatsApp and Facebook [10]. Therefore, the purpose of this study is to investigate the factors that influence the risk of phishing victimisation, specifically the risk of instant messaging phishing victimisation.

According to Das et al.'s [19] meta-analysis, while it is critical to provide technological solutions, such as warning indicators and browser extensions, or designing games-based solutions to thwart spear-phishing attacks [20], identifying specific human traits that a phisher can use to successfully exploit the user is critical for detection, prevention, and mitigation techniques. Psychology research on victimised users should focus on their mental models and the characteristics that make them vulnerable to such attacks [19,21]. In Malaysia, there is a growing corpus of literature and study on the consequences and challenges of phishing attacks [22–24]. The most significant consequence will be financial losses [13,24]. Phishing threats can cost internet users money as well as the costs of organisation support [25]. Specifically, phishing threats have exposed vulnerable victims to risks or dangers, as well as consequences [26]. Aside from monetary losses, customers will lose trust in a company if they believe legitimate messages are phishing messages [25]. Prior empirical research indicated and measured the level of cybercrime awareness among Malaysians [27]. According to the findings, respondents had little knowledge of phishing scams and were unaware of them [27]. The cause of cybercrime phishing threats in Malaysia is a lack of knowledge and awareness of phishing [21]. When an internet user has a lower level of cybercrime risk awareness, knowledge, or skills, they will be less cautious, resulting in fraud victimisation and monetary losses [28]. Internet users must therefore exercise caution when using the internet because they are essential to establishing online security [29,30].

Self-efficacy, which refers to people's perceptions of what they can accomplish with their abilities [14], is linked to knowledge [31]. For example, when internet users are more confident in taking the necessary precautions to avoid phishing attempts (self-efficacy), they are aware and knowledgeable of the risks involved, resulting in the avoidance of phishing attacks [31]. For example, a high level of ability to acquire anti-phishing knowledge (self-efficacy) may reduce the risk of phishing victimisation [32]. According to Hameed et al.'s [33] meta-analysis, researchers confirmed that self-efficacy is a key predictor in the context of information system security, particularly in mitigating the risk of information system security. In contrast, researchers discovered a significant and positive relationship between self-efficacy and susceptibility to phishing [34–36]. Internet users who have a high level of self-efficacy are more vulnerable to phishing attacks. People with a high level of self-efficacy are less likely to recognise a security attack [36] because they are overconfident in their ability to detect online fraud or phishing [37]. As a result, it begs the question of whether self-efficacy is related to one's susceptibility to phishing victimisation.

Additionally, cybercrime incidents can be reduced if internet users are knowledgeable about cybersecurity [38]. Precautionary online behaviour, for example, is also necessary for achieving online security [29,30]. A lower level of self-efficacy has been linked to lower levels of protection motivation and behaviour [39], for instance, people are more likely to share personal information online, exposing themselves to phishers [32]. According to Jansen and van Schaik's [30] research, there is a scarcity of research on behavioural or attitude change interventions for cybersecurity. Precautionary online behaviour (i.e., a

negative attitude toward the sharing of personal information online) may aid in preventing phishers from impersonating or deceiving internet users [32]. Therefore, this paper aims to investigate the relationship between self-efficacy and attitude towards precautionary behaviour.

The protection motivation theory (PMT) served as the foundation for attitude toward protective behaviour, which is more specifically operationalised as attitude towards sharing personal information online [32,40,41]. When determining whether someone will engage in security behaviour, attitude acts as a mediator [42,43]. It was discovered that a negative attitude toward sharing personal information online was a key predictor as well as a mediator in predicting phishing vulnerability in order to encourage security behaviour, particularly against phishing attacks [30]. Nowadays, the internet makes it easier for individuals to communicate and share personal information on social media [6]. However, when it comes to online privacy, internet users are having difficulty protecting their personal information [44]. As cybercrime becomes more prevalent, there is an urgent need to educate people about the risks of excessive information sharing, information control, information visibility, and privacy issues [45]. In today's rapidly evolving digital environment, user privacy has emerged as a critical issue that must be addressed [46]. A recent study recommended a game-based strategy to teach people about the dangers involved in information sharing on the internet [44]. Notably, the purpose of this research is to investigate the factors that contribute to the risk of phishing victimisation. Identifying the mediator which can reduce or mitigate the risk of phishing victimisation is therefore critical. With a nod to and theoretical justification from PMT, the attitude toward protection behaviour (attitude toward sharing personal information online) was chosen as a predictor as well as a mediator in this study.

The subsequent Section 2 discusses the theoretical foundation, which is then followed by the development of the research model and a discussion of the hypotheses. Section 4 describes the research methods, while Section 5 discusses the results. Section 6 explores the discussions and implications. The study's limitations are covered in Section 7, and the study's conclusion is presented in Section 8.

2. Theoretical Background

Protection Motivation Theory

Protection Motivation Theory (PMT) was established by Rogers [47]. PMT was developed to illustrate and comprehend individuals' risk-aversion behaviour in the field of health research [32,42]. PMT has been used to gain better insights into the intention to engage in protective behaviour [30,32,40]. Similarly, Warkentin et al. [48] presume that PMT assists in developing communication strategies that encourage people to take precautionary measures to avoid becoming a victim of cybercrime.

In the PMT, two major cognitive processes have been recognised (i.e., threat appraisal and coping appraisal) to predict attitude towards protection behaviour [32,40]. Threat appraisal was operationalised as perceived vulnerability/ susceptibility and perceived severity [32,49]. Coping appraisal was operationalised as self-efficacy or response efficacy [30,32,49].

A threat appraisal refers to evaluating a specific threat and the risk it entails [32]. For example, threat appraisal was operationalised as perceived severity in order to investigate its relationship with perceived vulnerability or the "likelihood of being victimised by a specific cybercrime threat" [32,50]. Coping appraisal is the process by which an individual evaluates various methods of protection. Personal ability to comply with protection methods (i.e., self-efficacy) and effectiveness of protection methods (i.e., response efficacy) are two examples [32].

Perceived severity was defined as the "extent someone believes that the consequences of threats would be harmful, increases the motivation toward protecting oneself against those threats" [32,41,47,51,52]. In other words, the more harmful the individuals perceive the threats, the more they would desire to perform security measures in order to avoid be-

coming cybercrime victims [32]. According to the definition, perceived severity was used to assess the outcomes or consequences of a threat, particularly phishing attacks [30,32].

Perceived vulnerability or susceptibility, however, was defined as "the risk or likelihood that an internet user will be deceived by a cybercrime attack" [32,53], particularly, phishing threats [54]. Perceived susceptibility was adopted in the current study as the dependent variable to measure one's risk of phishing victimisation. In other words, perceived susceptibility acted as a dependent variable to assess the perceptions of the respondents towards phishing susceptibility [9,54,55]. These perceptions include the possibility, probability, or risk/likelihood that the respondents think they will become phishing victims [32,54].

From a cybersecurity standpoint, self-efficacy plays a vital role in motivating cybersecurity protection behaviours [30,56]. When an individual possesses a high level of self-efficacy, he or she can detect phishing threats easily and manage to identify the cues, such as content authentication cues and sender verification cues [54,57]. These cues were used by internet users to validate the authenticity of phishing messages before completing any tasks requested by strangers, such as disclosing personal information [54].

In addition, response efficacy was defined as "an individual's evaluation of the perceived effectiveness of the recommended response" [30]. Response efficacy was used to assess the final outcome of whether a particular safety or security measure could effectively prevent phishing attacks [30]. Since the objective of this study was to identify the factors influencing perceived susceptibility to phishing victimisation, perceived severity and response efficacy were not included as an independent variables. This is due to perceived severity being used to measure the severity of the threat, focusing on the victims' perceptions of the consequences of being victimised, and not being victimised [30].

A growing number of empirical studies have recently substituted "attitude toward protection behaviour" for the original term "protection motivation" [32,40,41]. PMT has recently been adopted in the field of information security [30,58] as a mediator by adopting an attitude toward protection behaviour [32,40]. When PMT is used as a theoretical foundation for interventions, attitude plays an important role in avoiding cybercrime phishing victimisation [30]. The current study adopted the viewpoint of Jansen and van Schaik [30], who examined phishing susceptibility and identified attitude as a potential mediator. Figure 1 shows the current study's overall research framework.

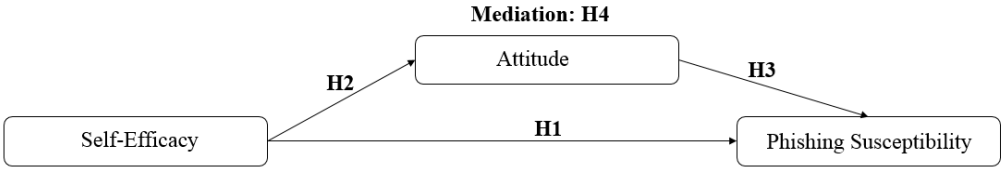

Figure 1. Research Framework.

3. Research Model and Hypotheses Development

3.1. Self-Efficacy, Attitude, and Phishing Susceptibility

Self-efficacy is defined as "a person's confidence in taking the precautionary measures, that is, the perceptions of one ability in protecting oneself online" [31]. Internet users have low levels of perceived privacy self-efficacy, implying that they consistently believe they have little control over their personal information [59]. Higher levels of perceived self-efficacy are associated with increased protection motivation and behaviour [39,47]. Indeed, studies have shown that higher levels of self-efficacy led to increased online security measures, such as communicating safely with others online [60]. In the field of information systems, self-efficacy has been extensively researched [54]. In the context of phishing, self-efficacy was identified as an important driver that could reduce the risk of phishing victimisation. For the purpose of this study, self-efficacy was adopted as researchers have indicated that it is a vital antecedent of attitude toward protection behaviour [30,32,40] and phishing susceptibility [6,61] respectively.

Perceived self-efficacy in knowledge related to phishing attempts significantly and negatively impacts an individual's likelihood of responding to phishing emails [62]. Previous research has acknowledged self-efficacy as a crucial antecedent to thwarting phishing attacks [63]. This is due to the fact one is often inclined to avoid security threats by adopting online precautionary measures when he or she believes that such security measures can be successfully implemented [63]. Verkijika [63], on the other hand, contends that research on the impact of anti-phishing self-efficacy on mobile phishing avoidance behaviour is limited. Since the present study was conducted to examine phishing victimisation, particularly on instant messaging phishing, anti-phishing self-efficacy was adopted as one of the independent variables to examine whether it is applicable in explaining phishing conducted via instant messaging.

Recent empirical studies have found that individuals with a high level of self-efficacy have a lower risk of becoming a victim of crime [64]. Numerous studies have found that self-efficacy influences phishing susceptibility. Recent empirical studies have found that individuals with low self-efficacy are more vulnerable to cyber-social engineering victimisation [65,66]. Researchers, on the other hand, discovered a significant and positive relationship between self-efficacy and phishing susceptibility [34,35]. In light of the contradictory findings, the purpose of this study is to investigate the relationship between self-efficacy and phishing susceptibility. The current study, guided by protection motivation theory [47], seeks to determine whether the influence of self-efficacy can reduce the risk of phishing victimisation [30]. As a result, this study hypothesised the following:

H1. *A higher level of self-efficacy leads to a lower risk of instant messaging phishing victimisation. (i.e., there will be a negative relationship).*

It has been demonstrated that self-efficacy influences an individual's attitude toward protective behaviour [30,51]. In other words, increased self-efficacy leads to a more positive attitude toward protective behaviour, specifically a negative attitude toward online information sharing [32]. This is because when a person believes in his or her own ability to perform a behaviour, he or she is motivated to engage in the protection behaviour [41,67] and thus declines to share personal information online [32]. As a result, the following hypothesis was proposed in this study:

H2. *A higher level of self-efficacy leads to a negative attitude towards sharing personal information online. (i.e., there will be a positive relationship).*

3.2. Attitude and Phishing Susceptibility

Under the guise of ignorance, individuals' risk attitudes influence their final decision-making [68]. A risk attitude, for example, may influence one's ability to recognise phishing attacks correctly [68]. However, there are few studies that look at people's attitudes in the context of cybersecurity research [69]. The attitude of internet users toward cybersecurity issues and cyber deception may influence their vulnerability to cybercrime [70]. Furthermore, people with a high desire to gamble (risk attitude) are more likely to click on phishing messages sent by scammers and fall victim to phishing attacks [71].

Attitudes toward protective behaviour can be critical in raising internet users' awareness of threats [30]. One's attitude can provide behavioural advice on how to process phishing messages and mitigate the threat, especially in cybercrime phishing attacks [30,32]. Because the purpose of this study is to investigate the risk of instant messaging phishing victimisation, it is critical to raise individual threat awareness in order to mitigate or lower the risk. Aside from threat knowledge, one should cultivate an attitude; a positive attitude toward protective behaviour (i.e., not sharing personal information) is essential in security behaviour [30]. Individuals will have a positive attitude toward protective behaviour when they perceive their vulnerability to becoming a cybercrime phishing victim [32,47].

Furthermore, previous research has shown that attitude is an important factor in predicting burnout and violent victimisation [72]. There are, however, few studies that use attitude as an independent variable to predict phishing victimisation. As a result, the purpose of this study is to use attitude as an exogenous variable to investigate instant messaging phishing victimisation, hence the third hypothesis:

H3. *Having a positive attitude towards sharing personal information online leads to a higher risk of instant messaging phishing victimisation. (i.e., there will be a negative relationship).*

3.3. The Mediating Role of Attitude towards Sharing Personal Information Online

The attitude was operationalised in the context of cyber-dependent crime (phishing) as the attitude toward sharing personal information online [30,32,67]. When a person has a positive attitude toward sharing personal information online (revealing information to strangers), he or she is more likely to become a victim of phishing attacks [32]. Nowadays, the internet's penetration and widespread adoption of social media platforms provide a fertile ground for phishing scams [73–75]. Internet users are at high risk of becoming cybercrime victims due to a lack of cybersecurity awareness about online threats and an increased positive attitude toward sharing personal information online [63,73].

A previous study in the cyberspace research context discovered that limiting the visibility of profiles in privacy settings had a significant impact on attitudes toward self-disclosure [76]. There is evidence that an internet user who is concerned about online security management does not necessarily limit self-disclosure in cyberspace, but rather has a negative attitude toward sharing personal information online [77].

Aside from technical safeguards, numerous studies emphasise the importance of attitude in understanding how target victims fall victim to phishing scams [32,78]. Attitude conceptualisation was initiated from the theory of planned behaviour [79] and the theory of protection motivation [32]. Attitude influences risk-taking in relationships, which in turn influences the processes and outcomes [78]. Individual attitudes may have a significant impact on their security perceptions [80].

An individual's ability to gain anti-phishing knowledge—namely, self-efficacy—influenced his/her risk of phishing victimisation significantly [65]. However, because of a lack of in-depth information, a message receiver with less prior knowledge may be influenced by phishing message cues [81]. As a result, this study aims to investigate the role of attitude in mediating the relationships between self-efficacy and phishing susceptibility (risk of instant messaging phishing victimisation). Thus, the fourth hypothesis is as follows:

H4. *Attitude towards sharing personal information online mediates the relationship between self-efficacy and the risk of instant messaging phishing victimisation.*

4. Method

4.1. Participants

All participants were recruited using social media platforms (i.e., Facebook, WhatsApp). Non-probability purposive sampling was used for data collection. The respondents had to be older than 18 and commonly communicate online via instant messaging applications in order to qualify as respondents. This study received 335 questionnaires in total. Following a thorough examination of the 335 datasets, a total of six datasets were detected with straight lining (3 and 5 s) and were omitted [82]. One response stated that they did not use instant messaging platforms on a regular basis. Hence, seven responses were excluded, leaving a final sample of 328 for the subsequent analyses. This resulted in a 97.9% response rate, far exceeding the 80% statistical power suggested by G*Power, which suggested that a sample size of 68 would be sufficient.

Finally, a valid sample of 328 participants was used, with 151 men (46%) and 177 women (54%). They were between the ages of 18 and 43 (mean = 23.78, standard deviation = 3.99).

In terms of years of education, 10.4% had 11 to 14 years (secondary school, diploma holder), while the remaining respondents had 15 to 20 years (bachelor´s degree, master´s degree, PhD). The majority of the respondents were currently residing in the centre of Malaysia (N = 155; 47.3%), followed by the Southern region (N = 78; 23.8%), Northern region (N = 47; 14.3%), East Malaysia (N = 36; 11%), and the East Coast (N = 12; 3.7%). In terms of years of instant messaging use, 30.2% had 1 to 6 years of experience using an instant messaging platform, while 69.8% had more than 6 years of experience using an instant messaging platform. In terms of occupation, 80.2% were students (N = 263), 18.3% were currently employed (N = 60), and 0.9% were unemployed (N = 3). More than half of the respondents (60.4%) did not have a monthly income. This percentage corresponds to the previous percentages for the occupational group, with the majority of the group being students.

The top three instant messaging platforms for online communication were WhatsApp (N = 292), Facebook Messenger (N = 225), and Telegram (N = 143). A total of 6% of those surveyed said they received phishing messages more than once a week (usually receiving phishing messages). One hundred and fifty-eight people stated that they get phishing emails once or twice a month (sometimes receiving suspicious message). Fifteen and a half per cent reported receiving phishing messages once or twice every two weeks (frequently receiving suspicious messages). Only a small percentage of respondents (5.5%) said they respond to phishing messages. The vast majority of respondents delete or ignore phishing messages, and some block the number. Table 1 depicts the respondent's demographic profile.

Table 1. Demographic Profile.

Respondent Characteristics (N = 328)	Frequency	Per cent
Gender		
Male	151	46
Female	177	54
Age (Gen-Z)		
18 to 22 years old	133	40.5
23 to 27 years old	195	59.5
Current Location		
Northern Region (Kedah, Perak, Perlis, Pulau Pinang)	47	14.3
Central Malaysia (Federal Territory: Kuala Lumpur, Putrajaya, Labuan), Negeri Sembilan, Selangor	155	47.3
Southern Region (Johor, Melaka)	78	23.8
East Coast (Kelantan, Pahang, Terengganu)	12	3.7
East Malaysia (Sabah, Sarawak)	36	11.0
Educational Level		
PhD	6	1.8
Master's Degree	49	14.9
Bachelor's Degree	239	72.9
Diploma	23	7.0
Technical/Vocational Education & Training	4	1.2
Secondary School	6	1.8
Others (Foundation)	1	0.3

4.2. Measures

A Google form was used to create an online survey with various subscales of self-efficacy, attitude toward behaviour (sharing personal information online), and phishing susceptibility. Each research variable is based on previous research work, with minor changes for contextual consistency.

4.2.1. Self-Efficacy

This study measured self-efficacy using six survey items adopted from Arachchilage and Love [31]. The scale ranged from 1 = "strongly disagree" to 5 = "strongly agree".

4.2.2. Attitude towards Sharing Personal Information

Attitude towards sharing personal information online was measured using five survey items adopted from Jansen and van Schaik [30]. A five-point semantic differential scale was adopted as the measurement scale to measure attitude towards behaviour.

4.2.3. Phishing Susceptibility

The current study measured phishing susceptibility using five survey items adapted from Chen et al. [54], with scales ranging from 1 to 7, with 1 indicating "strongly disagree" and 7 indicating "strongly agree."

4.3. Procedures

Several procedures were required to validate the survey instrument used in the study [83]. The procedures began with the development of a survey, followed by an expert review and a pilot test [83]. An expert review was conducted in this study, and the questionnaire was revised based on the expert's feedback. Following that, a focus group of at least four participants [84] was formed, and a detailed discussion was held to initiate their comments on the survey in this study. The survey questionnaire is shown in Appendix A. A pilot test was conducted based on 54 responses, and all research construct reliability was greater than 0.70 [82].

Finally, some ethical procedures must be followed both before and after gathering information from subjects [85]. This study followed ethical guidelines and was approved by the university Research Ethics Committee. The purpose of the study was fully explained to all participants, and the survey ensured anonymity by not collecting respondents' personal information. The respondents were fully informed of their other rights, which include confidentiality, privacy, voluntary participation, and the right to withdraw from this study at any time without explanation.

5. Results and Analysis

The SmartPLS 4.0.8.6 version was used as the statistical tool to examine the measurement and structural model as the focus of this paper was to predict the relationships between variables. PLS-SEM, as opposed to covariance-based structural equation modelling (CB-SEM), focuses on predicting how well exogenous constructs predict an endogenous construct [82]. Thus, PLS-SEM, which focuses on the amount of variance explained in the dependent variables, was deemed appropriate for this study.

5.1. Normality Assumption

The findings revealed that the data collected were univariate normal. The skewness and kurtosis for all research variables ranged from −0.313 to −0.026 and −0.179 to −0.943, respectively, which met the requirements of univariate normality of the data, which are ±1 and ±7 [86], respectively.

This study examined multivariate skewness and kurtosis as proposed by Cain et al. [87] and Hair et al. [88]. The results showed that the data were multivariate normal, Mardia's multivariate skewness ($\beta = 1.407$, $p < 0.01$), and Mardia's multivariate kurtosis ($\beta = 14.471$, $p < 0.01$). The values of skewness and kurtosis all fall within the criteria of multivariate normality of the data, which are ±3 and ±20, respectively [87].

5.2. Common Method Bias

The data collection of the present study was self-reported, and the data for the independent and dependent variables were gathered from the same respondents. There may be an issue of common method bias (CMB). Hence, the statistical procedure needs

to be applied in this study to address the CMB issue [89]. Although Harman's one factor has been commonly applied to detect CMB, literature has noted that it is not appropriate to detect CMB [90]. Researchers argued that "Harman's test is insensitive, and it is unlikely that a single-factor model will fit the data, especially as the number of variables increases" [91–93]. A single-factor result might not be able to explain a significant proportion of the total variance in the dataset, and subsequently, is not able to detect the CMB (potential inflation between variables) [93]. Thus, a full collinearity test was suggested for the detection of the CMB [94].

To test the full collinearity, this study follows the suggestions of Kock [95]. A Variance Inflation Factor (VIF) value of above 3.3 is indicative of potential collinearity problems [95,96]. The results of the current study found that all the VIF values of each research construct ranged from 1.048 to 1.087 which are lower than 3.3, as summarised in Table 2. Hence, the finding indicated that the dataset does not suffer from CMB.

Table 2. Full Collinearity Testing.

Attitude	Phishing Susceptibility	Self-Efficacy
1.071	1.048	1.087

5.3. Measurement Model

5.3.1. Validity and Reliability

For the convergent validity, the outer loadings, average variance extracted (AVE), and composite reliability (CR) were assessed. Except for SE6, all of the research constructs' outer loadings remained within a threshold of 0.708 [97], and most indicators are highly loaded on each construct and significant (−0.490). According to Hair et al. [88], a negative loading item was removed. As a result, SE6 was removed from the research model. As shown in Table 3, all AVE and CR values were greater than 0.50 and 0.70, respectively [86].

Table 3. Convergent validity.

	Outer Loading	Composite Reliability	Average Variance Extracted (AVE)	R^2
Attitude (ATB)		0.921	0.701	0.047
The sharing of personal information online is.				
ATB1	0.801			
ATB2	0.857			
ATB3	0.858			
ATB4	0.851			
ATB5	0.818			
Phishing Susceptibility (PS)		0.930	0.728	0.046
… becoming/become victimised by instant messaging phishing attacks.				
PS1	0.851			
PS2	0.858			

Table 3. *Cont.*

	Outer Loading	Composite Reliability	Average Variance Extracted (AVE)	R^2
PS3	0.850			
PS4	0.880			
PS5	0.827			
Self-Efficacy (SE)		0.888	0.614	
I could successfully gain anti-phishing knowledge if . . .				
SE1	0.711			
SE2	0.773			
SE3	0.829			
SE4	0.811			
SE5	0.788			
* SE6	-			

Notes: * item removed due to lower loading.

5.3.2. Discriminant Validity

The heterotrait–monotrait ratio of correlations (HTMT) method was used to determine discriminant validity [98]. It is proposed that if the HTMT value exceeds 0.85 [98,99], the problem of discriminant validity arises. The findings of the current study in Table 4 indicated that all HTMT values met the suggested criterion of 0.85.

Table 4. Heterotrait–Monotrait Ratio of Correlations (HTMT).

	Attitude	Phishing Susceptibility	Self-Efficacy
Attitude			
Phishing Susceptibility	0.112		
Self-Efficacy	0.232	0.175	

5.4. Structural Model

5.4.1. Hypothesis Testing

This study followed the suggestions of Hair et al. [97] by reporting the path coefficients, the standard errors, t-values, *p*-values [100], confidence intervals and effect sizes [101] for the structural model using a 5,000-sample re-sample bootstrapping procedure. Hypothesis H1 of this study posited that there is a negative relationship between self-efficacy and phishing susceptibility (risk of instant messaging phishing victimisation). Despite being significant, self-efficacy had the opposite effect (a positive relationship; $\beta = 0.191$, $t = 3.336$, $p < 0.001$) than what was initially hypothesised (a negative relationship) in the current study. The result, therefore, does not support hypothesis H1.

Hypothesis H2, self-efficacy ($\beta = 0.216$, $t = 3.916$, $p < 0.001$) is positively related to phishing susceptibility (risk of instant messaging phishing victimisation). Thus, H2 is supported. Lastly, attitude towards sharing personal information online ($\beta = -0.147$, $t = 2.449$, $p < 0.01$) was negatively related to and influenced phishing susceptibility (risk of instant messaging phishing victimisation). Thus, hypothesis H3 is supported. Table 5 summarises the results of the hypothesis testing. Figures 2 and 3 depict the research framework's structural analysis results.

Table 5. Hypothesis Testing.

Hypothesis		Std. Beta (β)	Std. Error	t-Value	BCI LL 5%	BCI UL 95%	*p*-Value	Results	f^2	Effect Size	VIF
H1	SE → PS	0.191	0.057	3.336	0.081	0.270	<0.001	Not Supported	0.037	Small	1.049
H2	SE → ATB	0.216	0.055	3.916	0.109	0.292	<0.001	Supported	0.049	Small	1.000
H3	ATB → PS	−0.147	0.060	2.449	−0.237	−0.038	0.007	Supported	0.022	Small	1.049

Note: SE = Self-efficacy, ATB = Attitude towards sharing personal information online, PS = Phishing Susceptibility, BCI = Confidence Interval Bias Corrected, UL = upper level, LL = Lower level.

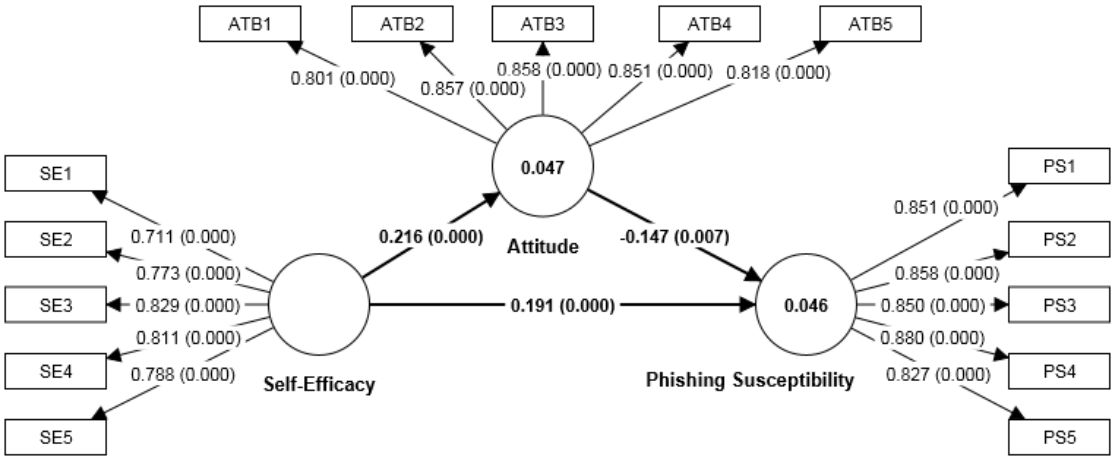

Figure 2. Structure model. Note: Inner model (paths) indicates the coefficients and *p*-values in parenthesis. Outer model (paths) indicates the item loadings and *p*-values in parentheses. Constructs ATB and PS show the R^2 value.

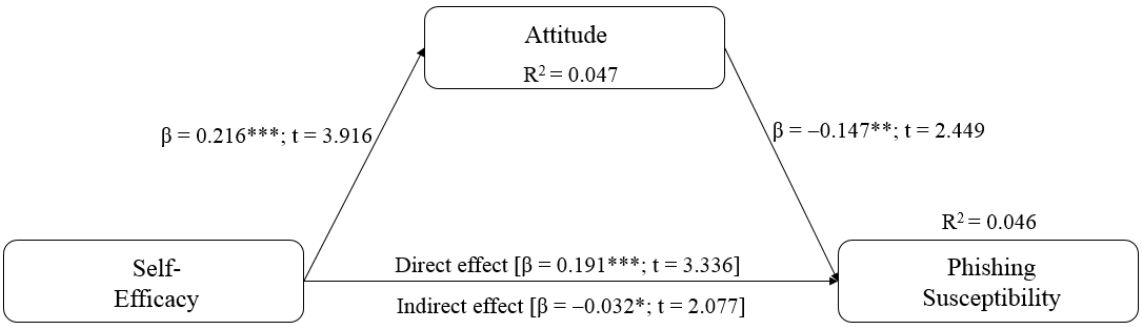

Figure 3. Research framework's structural analysis results. Note: *** = $p < 0.001$, ** = $p < 0.01$, * = $p < 0.05$.

5.4.2. Mediation Analysis

Hypothesis H4 speculates that attitude towards sharing personal information mediates the relationship between self-efficacy and phishing susceptibility (risk of instant messaging phishing victimisation). This study followed Preacher and Hayes's [102] recommendations to test the mediation of attitude toward sharing personal information online in the relationship between self-efficacy and phishing susceptibility, and indirect effects for mediation were tested using bootstrapping. The indirect effects 95% Boot CI bias-corrected (lower level and upper level) for self-efficacy → phishing susceptibility did not cross zero, indicating there is mediation [102]. Table 6 shows the resulting bootstrapping indirect effects analysis. Results were found statistically significant (β = −0.032, t = 2.077, $p = 0.038$), and as a result, this study supports hypothesis H4. The direct effect (0.191) for the self-efficacy → phishing susceptibility relationship was further assessed, yielding a *p*-value

of less than 0.05. The direct effect is still significant, suggesting a complementary partial mediation [103].

Table 6. Mediation Testing.

Hypothesis		Indirect Effect							Direct Effect				Mediation
		Std. Beta (β)	Std. Error	t-Value	*p*-Value	BCI LL 2.5%	BCI UL 97.5%	Results	Std. Beta (β)	Std. Error	t-Value	*p*-Value	
H4	SE → ATB → PS	−0.032	0.015	2.077	0.038	−0.062	−0.003	Supported	0.191	0.057	3.336	<0.001	Complementary Partial Mediation

Note: SE = Self-efficacy, ATB = Attitude Towards Sharing Personal Information Online, PS = Phishing Susceptibility, BCI = Confidence Interval Bias Corrected, UL = Upper Level, LL = Lower Level.

5.4.3. Explanatory Power of the Model

The coefficient of determination or R^2 was examined to determine the explanatory power of the model. As Table 3 shows, the R^2 value of attitude towards sharing personal information was 0.047 and phishing susceptibility was 0.046. Effect sizes, f^2 of self-efficacy (0.037) and attitude towards sharing personal information online (0.022) on phishing susceptibility revealed weak effects. In addition, self-efficacy had a small effect (0.049) in producing the R^2 for phishing susceptibility [104].

5.4.4. Predictive Power of the Model

Shmueli et al. [105] proposed a new evaluation procedure designed specifically for the prediction-oriented nature of PLS-SEM. Therefore, this study expanded the analysis by including a predictive-relevance analysis with PLS-Predict, as suggested by Shmueli et al. [105]. PLSpredict is "a holdout sample-based procedure that generates case-level predictions on an item or construct level" with a 5-fold procedure to check for predictive relevance. Shmueli et al. [105] proposed first checking the latent variable (Q^2 predict), and if that is greater than zero, then examining the item differences (PLS-LM).

If all of the item differences (PLS-LM) are lower, there is strong predictive power; if all are higher, predictive relevance is not confirmed; if the majority is lower, there is moderate predictive power; and if the minority is lower, there is low predictive power [105]. The Q^2 for the latent variable phishing susceptibility is 0.011, which is greater than zero, indicating that the construct had a predictive relevance. Following that, based on Table 7, all of the item differences (PLS-LM) were lower than the LM model, confirming that the current research model had a strong predictive power [105].

Table 7. PLS-Predict Summary.

Construct	Q^2 Predict			
Phishing Susceptibility (PS)	**0.011**			
Items	**PLS**	**LM**	**PLS-LM**	**Q^2 Predict**
	RMSE	**RMSE**	**RMSE**	
PS1	1.681	1.704	−0.023	−0.002
PS2	1.627	1.654	−0.027	0.012
PS3	1.536	1.548	−0.012	0.001
PS4	1.494	1.517	−0.023	0.022
PS5	1.573	1.589	−0.016	0.013

Notes: RMSE = root mean squared error; PLS = partial least squares path model; LM = linear regression model; Q^2 predict = predictive relevancy.

6. Discussion

The overarching goal of this study was to assess the effects of self-efficacy and attitude toward sharing personal information online on the risk of instant messaging phishing victimisation. According to the findings of this study, having the ability to gain anti-phishing

knowledge increases the risk of instant messaging phishing victimisation (phishing susceptibility). The results revealed a positive relationship (opposite to the hypothesised direction) between self-efficacy and phishing susceptibility. This study found that having a higher level of self-efficacy (the ability to learn anti-phishing knowledge) increased the risk of being a victim of instant messaging phishing. One plausible explanation is that people try to reduce mental strain by processing information quickly rather than deliberately [30,106]. As a result, because internet users are overconfident in their ability to detect phishing [37], it may be difficult to convince them to take cyber threats seriously [30]. This observation supports the findings of a recent empirical study, which found that self-efficacy was a significant predictor of phishing victimisation risk [62,107]. This finding, however, contradicts previous research that found that self-efficacy had a negligible impact on susceptibility to social engineering attacks [108,109].

In the current study, it was discovered that the belief that one has the ability and resources to acquire anti-phishing knowledge (self-efficacy) has a positive and significant influence on one's attitude toward sharing personal information online. This finding supports the findings of several studies that self-efficacy is significantly related to attitude formation [110,111]. The previous study's finding of an insignificant relationship between self-efficacy and attitude formation, on the other hand, was contradicted [112,113].

According to the current study, a negative attitude toward sharing personal information online significantly predicted susceptibility to phishing (risk of instant messaging phishing victimisation). This finding corroborates previous research that found that attitude toward behaviour influenced the risk of cyber-enabled crime (burnout and violent victimisation) [72] and cyber-dependent crime (phishing victimisation) [30,32]. This observation, however, contradicts Espelage et al.'s [114] research, which indicates that regardless of attitude toward risky behaviour, it does not necessarily protect individuals from being victimised. More specifically, this study demonstrates that a person who has a negative attitude toward sharing information online is more likely to want to protect his or her information [115], decreasing the risk of becoming a phishing victim. This is due to the fact that if an internet user is not confident that his or her personal information will be handled appropriately and carefully, he or she may develop a more unfavourable (negative) attitude toward sharing information online [116].

The mediation results demonstrated that attitudes toward sharing personal information online did play a role in predicting the relationship between self-efficacy and phishing susceptibility. In other words, this study suggests that a negative attitude towards sharing personal information online mediates the relationship between one's ability to gain anti-phishing knowledge (self-efficacy) and phishing susceptibility. When a negative attitude toward sharing personal information online intervenes, the strength of this relationship deteriorates. One plausible explanation for this finding is that detecting online fraud necessitates extensive knowledge of the fraud [117]. Scholars have suggested that a person's attitude toward resolving fraud or spam issues can be callous [118]. This is due to the fact that the vast majority of internet online fraud is expected to spread quickly [119], making it difficult for individuals to combat it effectively [118].

6.1. Theoretical Implications

PMT identifies several predictors that lead to the intention to implement the recommended precautionary measures [47]. According to researchers [120,121], the use of PMT in the domain of phishing is extremely limited. Jansen and van Schaik [122] found that PMT can be directly applied to the domain of phishing, where self-efficacy increases self-reported precautionary behaviour when securing information and sharing online information. According to the PMT theory, one's attitude change is influenced by one's protection motivation behaviour [47]. People with high self-efficacy, for example, are more likely to change their attitude, allowing them to make better decisions [6]. Because of the nature of PMT in examining human protection motivation behaviour, an increasing number of studies have applied it to phishing [30,32,55]. This is because when a person has a positive

attitude toward online precautionary behaviour (i.e., a negative attitude toward online information sharing) as well as a high perceived self-efficacy, he or she believes that phishing attackers will not compromise him or her [6,30]. As a result, the purpose of this study is to close the research gap by confirming that self-efficacy and attitude as PMT measures significantly predict the risk of phishing victimisation, particularly the risk of instant messaging phishing victimisation.

There was a contradictory study result on the significance of self-efficacy as a predictor of attitude towards protection behaviour [32]. The non-significant result seems strange and surprising as most studies indicated that self-efficacy was the strongest predictor of attitude towards protection behaviour [51,52,67]. As a result, Martens et al. [32] requested that the relationship between self-efficacy and attitude toward protective behaviour be investigated. Because of the non-significant result, the researchers concluded that self-efficacy was losing explanatory power in predicting attitudes toward behaviour in the phishing context [32,123]. As a result, this study has made a theoretical contribution to the understanding of a significant relationship between self-efficacy and attitude formation.

Attitude served as a mediator in predicting the offender's behaviour in both offline and online contexts [124,125]. On the other hand, an individual's (victim's) attitude was also relevant in examining the context of online security behaviour [30]. In the context of intent to engage in precautionary online behaviour, the attitude was defined as attitude toward personal information-sharing online [30]. Precautionary measures help to protect internet users from phishing attacks [30,32]. Thus, using PMT as a model, this study used attitude towards behaviour as both a predictor and a mediator to predict the risk of instant messaging phishing victimisation. Without denying that attitude was an important factor in explaining offender behaviour, the findings of this study contribute to the body of knowledge in this field by indicating that attitude is an important factor in predicting victim behaviour.

6.2. Practical Implications

The current study discovered that a higher level of self-efficacy increases one's risk of being a victim of instant messaging phishing. This study also discovered that having a higher level of self-efficacy reduces one's susceptibility to instant messaging phishing victimisation if one has a negative attitude towards sharing personal information online. Since this study found that self-efficacy (or confidence in one's ability to acquire anti-phishing knowledge) can lower the likelihood of being a victim of instant messaging phishing, it does show that the ability of Malaysian internet users to acquire anti-phishing knowledge is not a problem. The current study's findings emphasise the importance of self-efficacy as the underlying principle for implementing security behaviour. The ability of internet users to practise security practises when unsupervised is critical. Therefore, it is suggested that phishing-related awareness, education, and training programmes could be continued to increase self-efficacy [63,126]. Every internet user may begin with a different level of technical knowledge, competence, and awareness; thus, those who run anti-phishing efforts and informational websites may need to have empathy for and an understanding of this fact. The level of cybercrime awareness may be stated and quantified, for example, by the inclusion of quiz gaming that enables internet users to show their comprehension of phishing.

According to the literature, privacy expectations are decreasing as people become more comfortable disclosing personal information [127]. The internet's popularity has enabled internet users to engage and share significant personal information or experiences on online platforms [128,129]. According to existing literature, people believe that sharing personal information can result in benefits rather than privacy risks [130]. People tend to ignore the risks of disclosing information (high risk-taking attitudes) because they believe they are immune to cyber threats [130,131]. Therefore, it is understandable that guiding internet users to have a negative attitude toward sharing personal information online can be a challenging task. It is suggested that government agencies responsible for combating

phishing attacks inform and remind internet users on a regular basis to make informed sharing decisions in order to foster a negative attitude toward sharing personal information online. For example, in the anti-phishing awareness campaign, internet users are advised to use information verification before disclosing personal information online.

According to the findings of this study, one's attitude toward sharing personal information online can be influenced by one's level of self-efficacy. It does demonstrate that a high level of ability to acquire anti-phishing knowledge, which assists internet users in acquiring anti-phishing knowledge independently, can lead to a negative attitude toward sharing personal information online. When a person is familiar with anti-phishing techniques, he or she has a strong perception of privacy risk. As a result, he or she may regard information sharing as risky behaviour and, as a result, have a negative attitude toward sharing personal information online [132,133]. As a result, it is recommended that internet users regularly update their phishing-related knowledge, such as learning more about privacy risks, reporting any unknown or suspicious messages, and blocking or restricting any unknown senders on instant messaging applications. This is due to heightened awareness of the risks associated with disclosing personal information, which results in limited disclosure and information protection [134], as well as a negative attitude toward sharing personal information online [115].

7. Limitations of the Study and Validity Threats

One of the limitations of this study is that the survey's respondent age limit of up to 43 years old may limit the findings' applicability to all Malaysians. Because the current study's respondents are educated and experienced internet users, the study's findings may not apply to other populations who are less educated or technologically savvy. Future research may replicate the current study's research framework to investigate phishing susceptibility (risk of instant messaging phishing victimisation) among Malaysians of various ages.

Threats to External Validity [135,136] compromise the generalisability of the findings [20]. Although this study cannot claim that the empirical evaluation's findings are generalizable, it is expected that they will not change much by analysing the findings using a longitudinal study. This is because the current study used a purposive sample technique for data collection, with filtering questions (refer to Table A1) used to ensure respondents met the screening requirements and, as a result, establish the validity of the results. Furthermore, follow-up longitudinal studies (e.g., interviews and focus groups) might be done to validate the study's external validity.

Threats to Internal and Construct Validity [135,136]: Internal validity is concerned with the researcher's interpretation and bias of the data, whereas construct validity is concerned with the potential risks/threats associated with the study design [20]. To reduce the threats to construct validity, the survey questionnaires were drawn from the existing research literature (to reduce bias in design or any effect on the results or interpretation). Furthermore, an expert review was done to ensure the validity of the survey (refer to Section 4.3).

8. Conclusions

As cited in Martens et al.´s [32] research, an increasing number of studies are being conducted to investigate cybercrime using variations of the protection motivation theory (PMT) [137,138]. In addition to self-efficacy and attitude toward behaviour (protection motivation), PMT includes several other variables, including perceived severity and response efficacy [32]. However, only self-efficacy and attitude were used as predictors of the risk of instant messaging phishing victimisation in this study. This is because the current study's main goal was to examine the factors of phishing susceptibility rather than measuring one's perception of the consequences of being victimised and not being victimised [30]. As a result, the current study excluded perceived severity and response efficacy. A future study could build on the current research framework by incorporating these two variables as

moderators and examining whether the perceptions of the consequences differed between high and low self-efficacy internet users. Finally, the findings may point to major variations in cyber-security posture based on gender, age group, etc. [19,139]. Future possibilities include performing a strata analysis while taking into account numerous additional demographic factors that can be statistically tested.

Author Contributions: C.L.G.: conceptualization. Y.Y.L. and C.L.G.: literature review, writing original draft and writing. T.W.L.: Review and editing. Y.Y.L., C.L.G. and T.W.L.: Data collection. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Ministry of Higher Education Malaysia under the Fundamental Research Grant Scheme (Grant No. FRGS/1/2020/SS0/MMU/02/4).

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by the Research Ethics Committee of Multimedia University, Malaysia (Approval number: EA0302022 and date of approval: 11 May 2022).

Informed Consent Statement: Informed consent was obtained from all the individual participants included in the study.

Data Availability Statement: Data supporting reported results are available from the authors.

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

Appendix A

Table A1. Survey Questionnaire.

Part I Demographic (Screening Question)
SQ1. Nationality:

☐ Malaysian
☐ Non-Malaysian (Thank you for your participation. The questionnaire ends here)

Part II Instant Messaging Usage (Screening Question)
SQ2. Do you use instant messaging platforms (such as WhatsApp, Facebook Messenger, WeChat, etc.) for online communication?

☐ Yes (Please continue to answer the following survey)
☐ No (Thank you for your participation. The questionnaire ends here)

Part III—Demographic Profile
Q1. Gender:

☐ Male
☐ Female
☐ Others: _____

Q2. Current Location:

☐ Federal Territory (Kuala Lumpur, Putrajaya, Labuan)
☐ Johor
☐ Kedah
☐ Kelantan
☐ Melaka
☐ Negeri Sembilan
☐ Pahang
☐ Perak
☐ Perlis
☐ Pulau Pinang
☐ Sabah
☐ Sarawak
☐ Selangor
☐ Terengganu
☐ Others: _____

Q3. Educational level:

☐ PhD
☐ Master's degree
☐ Bachelor's degree
☐ Diploma
☐ Technical/vocational education & training
☐ Secondary school
☐ Primary school
☐ Others: _____

Q4. Occupation:

☐ Employed
☐ Unemployed
☐ Student
☐ Others: _____

Q5. Monthly Income (RM):

☐ Above RM 10,000
☐ RM 8001 to RM10,000
☐ RM6001 to RM8000
☐ RM4001 to RM 6000
☐ RM 2001 to RM 4000
☐ RM 2000 and Below
☐ Not Applicable

Part III—Mobile Instant Messaging

IMQ1. Which instant messaging platform do you use for online communication? (You may tick (/) more than one)

☐ Facebook Messenger
☐ KaoKao Talk
☐ Line
☐ Skype
☐ Telegram
☐ WeChat
☐ WhatsApp
☐ Discord
☐ Viber
☐ QQ Mobile
☐ Snapchat
☐ Others: _____

Part IV Phishing-Related Issue

PhishingQ1. Have you ever received phishing/spam messages sent to your WhatsApp, FB Messenger, etc.? If yes, please indicate how often you received these messages.
Examples of phishing messages or spam messages: (1)The messages that look like those coming from legitimate businesses or individuals asking for your personal data. /(2) The messages sent by strangers who offer you an/a investment/loan application/job offer opportunity with higher returns.

☐ Rarely (Once or twice in every six months)
☐ Sometimes (Once or twice a month)
☐ Frequently (Once or twice every two weeks)
☐ Usually (More than once a week)

PhishingQ2. What did you do with the phishing messages (sent via WhatsApp, FB Messenger, etc.)? (You may tick (/) more than one)

☐ I respond to the messages
☐ I delete or ignore the messages
☐ I delete and block the number
☐ I delete the message, block the number, and send a report

Part VI Survey Items
Attitude (ATB) The sharing of personal information online is: ATB1—Good (1)—Bad (5) ATB2—Beneficial (1) —Harmful (5) ATB3—Positive (1) —Negative (5) ATB4—Wise (1)—Foolish (5) ATB5—Favourable (1)—Unfavourable (5)
Phishing Susceptibility (PS) . . . . . becoming/become victimised by instant messaging phishing attacks. PS1—I am at risk for . . . PS2—It is likely that I will . . . PS3—It is possible that PS4—My chances of getting instant messaging phished are great. PS5—It is extremely likely that phishing messages will deceive me.
Self-Efficacy (SE) I could successfully gain anti-phishing knowledge if . . . SE1— . . . I had never learned it before. SE2— . . . I had only related resources for reference. SE3— . . . no one else helped me get started. SE4— . . . I had a lot of time. SE5— . . . no one taught me how to do it first. * SE6—I feel I cannot gain anti-phishing knowledge if no one else helped me get started.

Note: *, reverse-coded.

References

1. Tsiotsou, R.H. The social aspects of consumption as predictors of consumer loyalty: Online vs offline services. *J. Serv. Manag.* **2016**, *27*, 91–116. [CrossRef]
2. Kim, G. 80% of Young Malaysians Use Messaging Daily: Spectrum Futures Will Change Everything. 2016. Available online: https://spectrumfutures.org/80-of-young-malaysians-use-messaging-daily/ (accessed on 13 December 2022).
3. Digital Business Lab. Social Media Penetration in Malaysia [Research]. 2022. Available online: https://digital-business-lab.com/2022/07/%E2%91%A1-social-media-penetration-in-malaysia-research/ (accessed on 13 December 2022).
4. Yusop, F.D.; Sumari, M. The use of social media technologies among Malaysian youth. *Procedia-Soc. Behav. Sci.* **2013**, *103*, 1204–1209. [CrossRef]
5. Tang, Y.; Hew, K.F. Is mobile instant messaging (MIM) useful in education? Examining its technological, pedagogical, and social affordances. *Educ. Res. Rev.* **2017**, *21*, 85–105. [CrossRef]
6. House, D.; Raja, M.K. Phishing: Message appraisal and the exploration of fear and self-confidence. *Behav. Inf. Technol.* **2019**, *39*, 1204–1224. [CrossRef]
7. Balakrishnan, V.; Ng, K.S.; Rahim, H.A. To share or not to share—The underlying motives of sharing fake news amidst the COVID-19 pandemic in Malaysia. *Technol. Soc.* **2021**, *66*, 101676. [CrossRef]
8. Balakrishnan, S. Phishing Related Crimes In Malaysia: Challenges & Solutions. Master's Thesis, University of Malaya, Malaysia, 2020.
9. Frauenstein, E.D.; Flowerday, S. Susceptibility to phishing on social network sites: A personality information processing model. *Comput. Secur.* **2020**, *94*, 101862. [CrossRef]
10. Interpol, I.C. ASEAN Cyberthreat Assessment 2021. Available online: https://www.interpol.int/content/download/14922/file/ASEAN_CyberThreatAssessment_2020.pdf (accessed on 2 December 2022).
11. MalayMail, M. Kaspersky: Phishing Attacks on the Rise in Malaysia, SE Asia. 2022. Available online: https://www.malaymail.com/news/malaysia/2022/10/11/kaspersky-phishing-attacks-on-the-rise-in-malaysia-se-asia/32996 (accessed on 30 January 2023).
12. News Straits Times. TECH: Malaysia Continues to See Rise in Financial Phishing More than Its Peers in the Region. 2022. Available online: https://www.nst.com.my/lifestyle/bots/2022/11/845980/tech-malaysia-continues-see-rise-financial-phishing-more-its-peers (accessed on 30 January 2023).
13. Singh, M.M.; Frank, R.; Zainon, W.M. Cyber-criminology defense in pervasive environment: A study of cybercrimes in Malaysia. *Bullet. Electric. Eng. Inform.* **2021**, *10*, 1658–1668. [CrossRef]
14. Zainal, N.C.; Puad, M.H.; Sani, N.F. Moderating Effect of Self-Efficacy in the Relationship Between Knowledge, Attitude and Environment Behavior of Cybersecurity Awareness. *Asian Soc. Sci.* **2022**, *18*, 55–64. [CrossRef]
15. The Sun Daily, T.S. University Student Loses over RM18,000 to Job Scam Syndicate. 2022. Available online: https://www.thesundaily.my/local/university-student-loses-over-rm18000-to-job-scam-syndicate-BH9458726 (accessed on 2 December 2022).
16. Bernama, B. Painter, Student Fall Prey to Online Job Scam. 2022. Available online: https://www.nst.com.my/news/crime-courts/2022/05/795871/painter-student-fall-prey-online-job-scam (accessed on 2 December 2022).

17. Goh, E. M'sian Student Loses RM5.5k To Scammers Disguised As Digital Marketing Agency Offering Her A Job. 2022. Available online: https://worldofbuzz.com/msian-student-loses-rm5-5k-to-scammers-disguised-as-digital-marketing-agency-offering-her-a-job/ (accessed on 3 December 2022).
18. Dayak Daily, D.D. Dayak Daily. Student Loses RM14000 to RM350 Ipad Scam. 2022. Available online: https://dayakdaily.com/student-loses-rm14000-to-rm350-ipad-scam/ (accessed on 3 December 2022).
19. Das, S.; Eng, C.N.; Camp, L.J. Evaluating user susceptibility to phishing attacks. *Inf. Comput. Secur.* **2022**, *30*, 1–18. [CrossRef]
20. Fatima, R.; Yasin, A.; Liu, L.; Wang, J. How persuasive is a phishing email? A phishing game for phishing awareness. *J. Comput. Secur.* **2019**, *27*, 581–612. [CrossRef]
21. Prasad, R.; Rohokale, V. *Cyber Security: The Lifeline of Information and Communication Technology*; Springer International Publishing: Berlin/Heidelberg, Germany, 2020.
22. Kirwan, G.H.; Fullwood, C.; Rooney, B. Risk Factors for Social Networking Site Scam Victimization Among Malaysian Students. Cyberpsychol. *Behav. Soc. Netw.* **2018**, *21*, 123–128. [CrossRef]
23. Asfoor, A.; Rahim, F.A.; Yussof, S. Factors Influencing Information Security Awareness of Phishing Attacks from Bank Customers' Perspective: A Preliminary Investigation. *Rec. Trend. Data. Sci. Soft. Comput.* **2018**, *843*, 641–654.
24. Mohd, Z.N.; Mohd, A.M. Phishing as Cyber Fraud: The Implications and Governance. *Hong Kong J. Soc. Sci.* **2021**, *57*, 120–133.
25. Shan, T.L.; Samy, G.N.; Shanmugam, B.; Azam, S.; Yeo, K.C.; Kannoorpatti, K. Heuristic Systematic model based guidelines for Phishing Victims. In Proceedings of the IEEE 2016 Annual India Conference (INDICON), Bangalore, India, 16–18 December 2016.
26. Kob, T.N.; Abdul Rahim, F.; Azman, F. Phishing Attack Simulation: Measuring Susceptibility among Undergraduate Students. In Proceedings of the 2020 8th International Conference on Information Technology and Multimedia (ICIMU), Langkawi, Malaysia, 24–25 August 2020.
27. Saad, M.E.; Sheikh Abdullah, S.N.; Murah, M.Z. Cyber Romance Scam Victimization Analysis using Routine Activity Theory Versus Apriori Algorithm. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 479–485. [CrossRef]
28. Burgard, A.; Schlembach, C. Frames of fraud: A qualitative analysis of the structure and process of victimisation on the internet. *Int. J. Cyber. Crim.* **2013**, *7*, 112–124.
29. Davinson, N.; Sillence, E. Using the health belief model to explore users' perceptions of "being safe and secure" in the world of technology mediated financial transactions. *Int. J. Hum.-Comput. Stud.* **2014**, *72*, 154–168. [CrossRef]
30. Jansen, J.; van Schaik, P. The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *Int. J. Hum. Comput. Stud.* **2019**, *123*, 40–55. [CrossRef]
31. Arachchilage, N.A.; Love, S. Security awareness of computer users: A phishing threat avoidance perspective. *Comput. Hum. Behav.* **2014**, *38*, 304–312. [CrossRef]
32. Martens, M.; De Wolf, R.; De Marez, L. Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Comput. Hum. Behav.* **2019**, *92*, 139–150. [CrossRef]
33. Hameed, M.A.; Arachchilage, N.A. The role of self-efficacy on the adoption of information systems security innovations: A meta-analysis assessment. *Pers. Ubiquitous Comput.* **2021**, *25*, 911–925. [CrossRef]
34. Wang, J.; Li, Y.; Rao, H.R. Overconfidence in phishing email detection. *J. Assoc. Inf. Syst.* **2016**, *17*, 759–783. [CrossRef]
35. Moody, G.; Galletta, D.; Walker, J.; Dunn, B. Which phish get caught? An exploratory study of individual susceptibility to phishing. In Proceedings of the International Conference on Information Systems, Shanghai, China, 4–7 December 2011.
36. Hewitt, B.; White, G.L. Optimistic Bias and Exposure Affect Security Incidents on Home Computer. *J. Comput. Inf. Syst.* **2020**, *62*, 50–60. [CrossRef]
37. Whitty, M.T. Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims. *Eur. J. Crim. Policy Res.* **2020**, *26*, 399–409. [CrossRef]
38. Pitchan, M.A.; Omar, S.Z.; Ghazali, A.H. Cyber security practice among internet users towards cyberbullying, pornography, phishing email and online shopping. *Malays. J. Commun.* **2019**, *35*, 212–227.
39. Wottrich, V.M.; Reijmersdal, E.A.; Smit, E.G. App Users Unwittingly in the Spotlight: A Model of Privacy Protection in Mobile Apps. *J. Consum. Aff.* **2018**, *53*, 1056–1083. [CrossRef]
40. Herath, T.; Rao, H.R. Protection motivation and deterrence: A framework for security policy compliance in organisations. *Eur. J. Inf. Syst.* **2009**, *18*, 106–125. [CrossRef]
41. Anderson, C.; Agarwal, R. Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Q.* **2010**, *34*, 613–643. [CrossRef]
42. Floyd, D.; Prentice-Dun, S.; Rogers, R. A meta-analysis of research on protection motivation theory. *J. Appl. Soc. Psychol.* **2000**, *30*, 407–429. [CrossRef]
43. Chenoweth, T.; Minch, R.; Gattiker, T. Application of protection motivation theory to adoption of protective technologies. In Proceedings of the 2009 42nd Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 5–8 January 2009.
44. Fatima, R.; Yasin, A.; Liu, L.; Wang, J.; Afzal, W.; Yasin, A. Sharing information online rationally: An observation of user privacy concerns and awareness using serious game. *J. Inf. Secur. Appl.* **2019**, *48*, 102351. [CrossRef]
45. Vervier, L.; Zeissig, E.; Lidynia, C.; Ziefle, M. Perceptions of digital footprints and the value of privacy. In Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, Porto, Portugal, 24–26 April 2017.

46. Dhotre, P.; Olesen, H.; Khajuria, S. User Privacy and Empowerment: Trends, Challenges, and Opportunities. In Proceedings of the International Conference on Intelligent Computing and Communication, Pune, India, 2–4 August 2017.
47. Rogers, R.W. A protection motivation theory of fear appeals and attitude change. *J. Psychol.* **1975**, *91*, 93–114. [CrossRef]
48. Warkentin, M.; Johnston, A.C.; Shropshire, J.; Barnett, W.D. Continuance of protective security behavior: A longitudinal study. *Decis. Support Syst.* **2016**, *92*, 25–35. [CrossRef]
49. Knapova, L.; Kruzikova, A.; Dedkova, L.; Smahel, D. Who Is Smart with Their Smartphones? Determinants of Smartphone Security Behavior. *Cyberpsychol. Behav. Soc. Netw.* **2021**, *24*, 584–592. [CrossRef]
50. Jansen, J.; Leukfeldt, R. Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization. *Int. J. Cyber. Criminol.* **2016**, *10*, 79–91.
51. Dang-Pham, D.; Pittayachawan, S. Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Comput. Secur.* **2015**, *48*, 281–297. [CrossRef]
52. Crossler, R.; Bélanger, F. An Extended Perspective on Individual Security Behaviors. *ACM SIGMIS Database* **2014**, *45*, 51–71. [CrossRef]
53. Goel, S.; Williams, K.; Dincelli, E. Internet security and human vulnerability. *J. Assoc. Inf. Syst.* **2017**, *18*, 22–44.
54. Chen, R.; Gaia, J.; Rao, H.R. An examination of the effect of recent phishing encounters on phishing susceptibility. *Decis. Support Syst.* **2020**, *133*, 113287. [CrossRef]
55. Musuva, P.M.; Getao, K.W.; Chepken, C.K. A New Approach to Modelling the Effects of Cognitive Processing and Threat Detection On Phishing Susceptibility. *Comput. Hum. Behav.* **2019**, *94*, 154–175. [CrossRef]
56. Kwak, Y.S.; Lee, S.Y.; Damiano, A.; Vishwanath, A. Why do users not report spear phishing emails? *Telemat. Inform.* **2020**, *48*, 101343. [CrossRef]
57. Rocha Flores, W.; Holm, H.; Nohlberg, M.; Ekstedt, M.; Furnell, S.; Furnell, S. Investigating personal determinants of phishing and the effect of national culture. *Inf. Comput. Secur.* **2015**, *23*, 178–199. [CrossRef]
58. Jansen, J.; Leukfeldt, R. How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. In Proceedings of the 2015 Workshop on Socio-Technical Aspects in Security and Trust, Verona, Italy, 13 July 2015; pp. 24–31.
59. Park, Y.J. Digital Literacy and Privacy Behavior Online. *Commun. Res.* **2011**, *40*, 215–236. [CrossRef]
60. Boehmer, J.; LaRose, R.; Rifon, N.; Alhabash, S.; Cotten, S. Determinants of Online Safety Behaviour: Towards an Intervention Strategy for College Students. *Behav. Inf. Technol.* **2015**, *34*, 1022–1035. [CrossRef]
61. Wright, R.; Johnson, S.L.; Kitchens, B. A Multi-Level Contextualized View of Phishing Susceptibility. *Soc. Sci. Res. Netw.* **2020**, 1–60. [CrossRef]
62. Vishwanath, A.; Herath, T.; Chen, R.; Wang, J.; Rao, R. Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability Within an Integrated, Information Processing Model. *Decis. Support Syst.* **2011**, *51*, 576–586. [CrossRef]
63. Verkijika, S.F. "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Comput. Hum. Behav.* **2019**, *101*, 286–296. [CrossRef]
64. Samper-García, P.; Malonda-Vidal, E.; Llorca-Mestre, A.; Muñoz-Navarro, R.; Mestre-Escrivá, V. Victimization and Peer and Parents Attachment: The Mediating Effect of Regulatory Emotional Self-Efficacy. *Int. J. Environ. Res. Public Health* **2021**, *18*, 2062. [CrossRef]
65. Alotaibi, M.K.A. Hypothesised Model to Examine Susceptibility to Cyber-Social Engineering Through LinkedIn in The Workplace. In Proceedings of the 13th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019), Nicosia, Cyprus, 15–16 July 2019.
66. Wright, R.T.; Marett, K. The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *J. Manag. Inf. Syst.* **2010**, *27*, 273–303. [CrossRef]
67. Jansen, J.; van Schaik, P. Comparing three models to explain precautionary online behavioural intentions. *Inf. Comput. Secur.* **2017**, *25*, 165–180. [CrossRef]
68. Chen, Y.; YeckehZaare, I.; Zhang, A.F. Real or bogus: Predicting susceptibility to phishing with economic experiments. *PLoS ONE* **2018**, *13*, e0198213. [CrossRef] [PubMed]
69. Flores, P. Digital Simulation in the Virtual World: Its Effect in the Knowledge and Attitude of Students Towards Cybersecurity. In Proceedings of the 2019 6th HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates, 20–21 November 2019.
70. Back, S.; Guerette, R.T. Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks. *J. Contemp. Crim. Justice* **2021**, *37*, 427–451. [CrossRef]
71. Abroshan, H.; Devos, J.; Poels, G.; Laermans, E. Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. *IEEE Access* **2021**, *9*, 44928–44949. [CrossRef]
72. Ellrich, K. Burnout and violent victimization in police officers: A dual process model. *Int. J. Police Strateg. Manag.* **2016**, *39*, 652–666. [CrossRef]
73. Aleroud, A.; Abu-Shanab, E.; Al-Aiad, A.; Alshboul, Y. An examination of susceptibility to spear phishing cyber attacks in non-English speaking communities. *J. Inf. Secur. Appl.* **2020**, *55*, 102614. [CrossRef]
74. Ngo, F.T.; Piquero, A.R.; LaPrade, J.; Duong, B. Victimization in Cyberspace: Is It How Long We Spend Online, What We Do Online, or What We Post Online? *Crim. Justice Rev.* **2020**, *45*, 430–451. [CrossRef]

75. Naci, A.; Christopher, J.L. Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Res.* **2020**, *30*, 1665–1687.
76. Chen, H.T. Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self- efficacy, and social capital on privacy management. *Am. Behav. Sci.* **2018**, *62*, 1392–1412. [CrossRef]
77. Oghazia, P.; Schultheiss, R.; Chirumalla, K.; Kalmerd, N.P.; Rad, F.F. User self-disclosure on social network sites: A cross-cultural study on Facebook's privacy concepts. *J. Bus. Res.* **2020**, *112*, 531–540. [CrossRef]
78. Alyahya, A.; Weir, G.R. Understanding Responses to Phishing in Saudi Arabia via the Theory of Planned Behaviour. In Proceedings of the National Computing Colleges Conference, Taif, Saudi Arabia, 27 March 2021.
79. Ajzen, I.; Fishbein, M. Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychol. Bull.* **1977**, *84*, 888–918. [CrossRef]
80. Sylvester, F.L. Mobile device users' susceptibility to phishing attacks. *Int. J. Comp. Sci. Inf. Technol.* **2022**, *14*, 1–18. [CrossRef]
81. Ge, Y.; Lu, L.; Cui, C.Y.; Chen, Z.; Qu, W.N. How personal characteristics impact phishing susceptibility: The mediating role of mail processing. *Appl. Ergon.* **2021**, *97*, 103526. [CrossRef]
82. Hair, J.J.; Hufit, G.M.; Ringle, C.M.; Sarstedt, M. *A Primer on Partial Least Squares Structural Equation Modelling (PLS-SEM)*; SAGE Publications: Thousand Oaks, CA, USA, 2014.
83. Ruel, E.; Wagner, W.E., III; Gillespie, B.J. *The Practice of Survey Research*; SAGE Publications Inc.: Thousand Oaks, CA, USA, 2016; Available online: https://www.sagepub.com/sites/default/files/upm-binaries/24056_Chapter4.pdf (accessed on 12 December 2022).
84. Saunders, M.; Lewis, P.; Thornhill, A. *Research Methods for Business Students*, 5th ed.; Pearson Education Limited: Harlow, UK, 2009.
85. Kumar, R. *Research Methodology: A Step by Step Guide for Beginners*, 3rd ed.; SAGE Publications Ltd.: New Delhi, India, 2011.
86. Curran, P.J.; West, S.G.; Finch, J.F. The robustness of test statistics to nonnormality and specification error in confirmatory factor analysis. *Psychol. Methods* **1996**, *1*, 16–29. [CrossRef]
87. Cain, M.K.; Zhang, Z.; Yuan, K.H. Univariate and multivariate skewness and kurtosis for measuring nonnormality: Prevalence, influence and estimation. *Behav. Res. Methods* **2016**, *49*, 1716–1735. [CrossRef] [PubMed]
88. Hair, J.F.; Hult, G.T.; Ringle, C.M.; Sarstedt, M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 2nd ed.; SAGE Publications Inc.: Thousand Oaks, CA, USA, 2017.
89. Podsakoff, P.M.; MacKenzie, S.B.; Lee, J.Y. Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *J. Appl. Psychol.* **2003**, *88*, 879–903. [CrossRef]
90. Lowry, P.; Gaskin, J. Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Trans. Prof. Commun.* **2014**, *57*, 123–146. [CrossRef]
91. Lindell, M.; Whitney, D.J. Accounting for common method variance in cross-sectional research designs. *Int. J. Appl. Psychol.* **2001**, *86*, 114–121. [CrossRef]
92. Podsakoff, P.M.; MacKenzie, S.B.; Podsakoff, N.P. Sources of Method Bias in Social Science Research and Recommendation on How to Control It. *Annu. Rev. Psychol.* **2012**, *63*, 539–569. [CrossRef]
93. Jordan, P.J.; Troth, A.C. Common method bias in applied settings: The dilemma of researching in organizations. *Aust. J. Manag.* **2020**, *45*, 3–14. [CrossRef]
94. Kock, N.; Lynn, G.S. Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *J. Assoc. Inf. Syst.* **2012**, *13*, 546–580. [CrossRef]
95. Kock, N. Common method bias in PLS-SEM: A full collinearity assessment approach. *Int. J. e-Collab.* **2015**, *11*, 1–10. [CrossRef]
96. Hair, J.J.; Black, W.; Babin, B.; Anderson, R. *Multivariate Data Analysis: A Global Perspective*, 7th ed.; Prentice Hall: Hoboken, NJ, USA, 2010.
97. Hair, J.; Risher, J.; Sarstedt, M.; Ringle, C. When to use and how to report the results of PLS-SEM. *Eur. Bus. Rev.* **2019**, *31*, 2–24. [CrossRef]
98. Henseler, J.; Ringle, C.M.; Sarstedt, M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J. Acad. Mark. Sci.* **2015**, *43*, 115–135. [CrossRef]
99. Franke, G.; Sarstedt, M. Heuristics versus statistics in discriminant validity testing: A comparison of four procedures. *Internet Res.* **2019**, *29*, 430–447. [CrossRef]
100. Ramayah, T.; Cheah, J.; Chuah, F.; Ting, H.; Memon, M.A. *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using SmartPLS 3.0: An Updated Guide and Practical Guide to Statistical Analysis*, 2nd ed.; Pearson: Kuala Lumpur, Malaysia, 2018.
101. Hahn, E.D.; Ang, S.H. From the editors: New directions in the reporting of statistical results in the Journal of World Business. *J. World Bus.* **2017**, *52*, 125–126. [CrossRef]
102. Preacher, K.J.; Hayes, A.F. SPSS and SAS procedures for estimating indirect effects in simple mediation models. *Behav. Res. Methods Instrum. Comput.* **2004**, *36*, 717–731. [CrossRef] [PubMed]
103. Zhao, X.L.; Lynch, J.G.; Chen, Q. Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *J. Consum. Res.* **2010**, *37*, 197–206. [CrossRef]
104. Cohen, J. *Statistical Power Analysis for the Behavioral Science*, 2nd ed.; Lawrence Erlbaum Associates: Hillsdale, NJ, USA, 1988.
105. Shmueli, G.; Sarstedt, M.; Hair, J.F.; Cheah, J.-H.; Ting, H.; Vaithilingam, S.; Ringle, C.M. Predictive model assessment in PLS-SEM: Guidelines for using PLSpredict. *Eur. J. Mark.* **2019**, *53*, 2322–2347. [CrossRef]

106. Fransen, M.L.; Smit, E.G.; Verlegh, P.W. Strategies and motives for resistance to persuasion: An integrative framework. *Front. Psychol.* **2015**, *6*, 1201. [CrossRef]
107. Sun, J.C.; Yu, S.J.; Lin, S.S.; Tseng, S.S. The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. *Comput. Hum. Behav.* **2016**, *59*, 249–257. [CrossRef]
108. Aribake, F.O.; Aji, Z.M. The Mediating Role of Perceived Security on the Relationship between Internet Banking Users and their Determinants. *Int. J. Adv. Res. Sci. Eng. Technol.* **2020**, *11*, 296–318.
109. Albladi, S.M.; Weir, G.R. Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity* **2020**, *3*, 1–19. [CrossRef]
110. Alfany, Z.; Saufi, A.; Mulyono, L.E. The Impact of Social Influence, Self-Efficacy, Perceived Enjoyment, and Individual Mobility on Attitude toward use and Intention to use Mobile Payment of OVO. *Glob. J. Manag. Bus. Res.* **2019**, *19*, 1–9.
111. Rosander, M.K.F.F.; Hammar, C.E. Attitudes towards being assessed in group work: The effects of self-efficacy and collective efficacy moderated by a short educational intervention. *Psychol. Sch.* **2020**, *57*, 1–13. [CrossRef]
112. Vrhovec, S.; Mihelič, A. Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. *Comput. Secur.* **2021**, *106*, 102309. [CrossRef]
113. Choi, H.S.; Carpenter, D.; Ko, M.S. Risk Taking Behaviors Using Public Wi-Fi™. *Infor. Syst. Front.* **2022**, *24*, 965–982. [CrossRef]
114. Espelage, D.L.; Hong, J.S.; Kim, D.H.; Nan, L. Empathy, attitude towards bullying, theory-of-mind, and non-physical forms of bully perpetration and victimization among U.S. middle school students. *Child Youth Care Forum* **2017**, *47*, 45–60. [CrossRef]
115. Belanger, F.; Crossler, R.E. Dealing with digital traces: Understanding protective behaviors on mobile devices. *J. Strateg. Inf. Syst.* **2019**, *28*, 34–49. [CrossRef]
116. Mutambik, I.; Lee, J.; Almuqrin, A.; Halboob, W.; Omar, T.; Floos, A. User concerns regarding information sharing on social networking sites: The user's perspective in the context of national culture. *PLoS ONE* **2022**, *17*, e0263157. [CrossRef]
117. Kassem, R.; Andrew, H. The New Fraud Triangle Model. *J. Emerg. Trends Econ. Manag. Sci.* **2012**, *3*, 191–195.
118. Dörnyei, K.R. Marketing Professionals' Views on Online Advertising Fraud. *J. Curr. Issues Res. Advert.* **2021**, *42*, 156–174. [CrossRef]
119. Dinev, T.; Qing, H.; Ali, Y. Is There an On-Line Advertisers' Dilemma? A Study of Click Fraud in the Pay-per-Click Model. *Int. J. Electron. Commer* **2008**, *13*, 29–60. [CrossRef]
120. Bayl-Smith, P.; Taib, R.; Yu, K.; Wiggins, M. Response to a phishing attack: Persuasion and protection motivation in an organizational context. *Inf. Comput. Secur.* **2022**, *30*, 63–78. [CrossRef]
121. Williams, E.J.; Joinson, A.N. Developing a measure of information seeking about phishing. *J. Cybersecur.* **2020**, *6*, tyaa001. [CrossRef]
122. Jansen, J.; van Schaik, P. Persuading end users to act cautiously online: A fear appeals study on phishing. *Inf. Comp. Secur.* **2018**, *26*, 264–276. [CrossRef]
123. Menard, P.; Bott, G.; Crossler, R. User motivations in protecting information security: Protection motivation theory versus self-determination theory. *J. Manag. Inf. Syst.* **2017**, *34*, 1203–1230. [CrossRef]
124. Petrescu, M.; John, T.G.; Pradeep, K.K. Online piracy in the context of routine activities. *J. Mark. Manag.* **2018**, *34*, 314–346. [CrossRef]
125. Korgaonkar, P.K.; Gironda, J.T.; Petrescu, M.; Krishen, A.S.; Mangleburg, T.F. Preventing shoplifting: Exploring online comments to propose a model. *Psychol. Mark.* **2019**, *37*, 141–153. [CrossRef]
126. Goel, D.; Jain, A.K. Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Comput. Secur.* **2018**, *73*, 519–544. [CrossRef]
127. Johnson, B. Privacy No Longer a Social Norm, Says Facebook Founder. Available online: https://www.theguardian.com/technology/2010/jan/11/facebook-privacy (accessed on 23 December 2022).
128. Burles, M.C.; Bally, J.M. Ethical, Practical, and Methodological Considerations for Unobtrusive Qualitative Research About Personal Narratives Shared on the Internet. *Int. J. Qual. Methods* **2018**, *17*, 1–9. [CrossRef]
129. Sahoo, S.R.; Gupta, B.B. Classification of various attacks and their defence mechanism in online social networks: A survey. *Enterp. Inf. Syst.* **2019**, *13*, 832–864. [CrossRef]
130. Steijn, W.S. Why concern regarding privacy differs: The influence of age and (non-)participation on Facebook. *Cyberpsychol. J. Psychosoc. Res. Cyberspace* **2016**, *10*, 3. [CrossRef]
131. Debatin, B.; Lovejoy, J.; Horn, A.; Hughes, B. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *J. Comput. Mediat. Commun.* **2009**, *15*, 83–108. [CrossRef]
132. Hajli, N.; Lin, X. Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *J. Bus. Ethics* **2016**, *133*, 111–123. [CrossRef]
133. Buchanan, T.; Benson, V. Spreading Disinformation on Facebook: Do Trust in Message Source, Risk Propensity, or Personality Affect the Organic Reach of "Fake News"? *Soc. Media. Soc.* **2019**, *5*, 1–9. [CrossRef]
134. Parker, H.J.; Flowerday, S. Understanding the disclosure of personal data online. *Inf. Comput. Secur.* **2021**, *29*, 413–434. [CrossRef]
135. Petersen, K.; Gencel, C. Worldviews, Research Methods, and their Relationship to Validity in Empirical Software Engineering Research. In Proceedings of the Joint Conference of the 23nd International Workshop on Software Measurement (IWSM) and the 8th International Conference on Software Process and Product Measurement (Mensura), Ankara, Turkey, 23–26 August 2013.

136. Wohlin, C.; Runeson, P.; Höst, M.; Ohlsson, M.C.; Regnell, B. *Experimentation in Software Engineering*; Springer: Berlin/Heidelberg, Germany, 2012.
137. Dodel, M.; Mesch, G. Cyber-victimization preventive behavior: A health belief model approach. *Comput. Hum. Behav.* **2016**, *68*, 359–367. [CrossRef]
138. Dodel, M.; Mesch, G. Inequality in digital skills and the adoption of online safety behaviors. *Inf. Commun. Soc.* **2018**, *21*, 712–728. [CrossRef]
139. Khan, N.F.; Ikram, N.; Saleem, S.; Zafar, S. Cyber-security and risky behaviors in a developing country context: A Pakistani perspective. *Secur. J.* **2022**. [CrossRef]