EXAMINING INDIVIDUAL TENDENCY TO RESPOND TO PHISHING E-MAILS FROM THE PERSPECTIVE OF PROTECTION MOTIVATION THEORY

Allen Peter Diman,
Titik Khawa Abdul Rahman

ABSTRACT

Phishing e-mails are major cyber threats not only to organisations but also to individuals. In many cases of reported phishing incidents, individuals fall prey to the trap of phishing e-mails because they believe the e-mails they received are legit. Previous studies have identified individual personality traits as one of the factors that can cause a person to become a victim of phishing attacks. Separately, different studies have also revealed that individuals' handling of phishing threats and their actions to cope with such threats as other factors that can lead to a similar problem. To help understand the reason why certain types of personality traits are more inclined to respond to phishing e-mails, this study examined the role of individual protection motivation as the possible determinant that could further explain the relationships between personality traits and an individual's response to phishing e-mails. The findings from 400 analysed data revealed that different personality traits except the trait of openness, exhibit different levels of perception in terms of their respective protection motivation. The study also found that individuals' tendency to respond to phishing e-mails depends on how they perceive the phishing threats and how they cope with such threats. Specifically, analysis of the results revealed that individuals with the trait of neuroticism have a high likelihood of responding to phishing e-mails. The study contributes to the body of knowledge by expanding the application of the Protection Motivation Theory to explain why certain types of personality traits have a higher tendency to respond to phishing e-mails than others. To avoid becoming phishing victims, individuals and as well as organisations should, therefore, put in greater efforts to ensure effective and sufficient coping strategies are in place to counter such threats. The implementation of anti-phishing training and phishing awareness campaigns can facilitate the attainment of this objective.

Keywords: Personality traits, protection motivation, phishing e-mails, threat appraisal, coping appraisal

INTRODUCTION

Phishing is a serious and costly threat to both individuals and organisations (Burns et al., 2019). The consequences as a result of being a phishing victim include financial losses, an effect on the individual's or organisation's reputation, loss of confidential data, and an effect on the organisation's competitiveness (Jampen et al., 2020). Various reports indicate that phishing incidents have been on the rise year after year (Stojnic et al., 2021). According to data collected by the cyber security firm AAG IT Services, phishing incidents have cost American business victims more than United States Dollars (USD) 2.7 billion in 2022 alone. Between 2020 and 2021, the reported cybercrime which includes phishing has increased by 168% in the Asia-Pacific region (Griffiths, 2023).

Malaysia has also not sparred from being the target of cyber criminals using the tactic of phishing. Based on the information presented by Muharram et al. (2022) on average 31 cybersecurity incidents such as phishing occur in Malaysia daily. Moreover, Muharram et al. (2022) also stated that in 2019 alone, CyberSecurity Malaysia reported that the country lost RM539 million from the 13,000 reported cybercrime cases. This number according to the authors has since increased to 17,000 in 2020 and for 2021, there were more than 20,000 reported cases resulting in losses amounting to RM560 million. In 2022, Malaysia National News Agency, Bernama reported that almost RM600 million were lost due to cybercrime (Bernama, 2023). If this trend continues, it is expected that cybercrime in Malaysia in 2023 will surpass the previously recorded cases in 2020, 2021 and 2022.

LITERATURE REVIEW

Phishing is a type of cybercrime where attackers use social engineering techniques to manipulate individuals into disclosing sensitive information such as login credentials, financial data, or personal information (Salahdine & Kaabouch, 2019; Taib et al., 2019). The consequence of phishing incidents can greatly affect the organisations' and individuals' reputations and trust as well as financial losses (Jampen et al., 2020). According to Abroshan et al (2021), the main reason why individuals become tempted to respond to phishing e-mails is that they believe the e-mails they received are genuine and that phishers would usually entice them to take action on the e-mails using persuasive tactics. To understand the reason behind individuals' tendency to respond to phishing e-mails, past researchers have tried to look at different factors that could contribute to such a phenomenon. This includes looking from the perspective of individual personality traits – agreeableness, conscientiousness, extroversion, neuroticism and openness. Several recent studies such as those by Anawar et al. (2019), Frauenstein and Flowerday (2020), Ge et al. (2021), Lawson et al. (2020), Lau et al. (2022) and Yang et al. (2022) have applied personality traits as one of the variables in their studies. In the context of social sciences, personality traits can be defined as unique characteristics that can be used to describe different individuals (Abood, 2020). Broadly, five types of traits can be used to describe a person, which are briefly described in Table 1.

Table 1. Results of outer model assessment

Trait	Description
Agreeableness	Agreeableness refers to someone who can be trusted, is not demanding, is warm towards others, is not stubborn and showing off and, finally, is sympathetic. As such, they can be categorised as individuals who are prosocial in their behaviour, cooperative, and have a great deal of interest in other people.
Conscientiousness	Conscientiousness refers to a person who is competent, organised or goal-oriented, not careless, thorough in things they do, highly self-disciplined, i.e., they are not lazy, and finally, they are not impulsive (reasonable impulse control to follow the rules or maintain goal pursuit).
Extroversion	Extroversion refers to someone who has the trait of an extrovert. Their characteristics include being friendly, forceful, energetic, adventurous, enthusiastic, and outgoing. They also tend to be talkative with a considerable amount of positive emotional expressiveness and sensitive to rewards.
Neuroticism	Neuroticism refers to the individual who has the traits of being tense, irritable, sad, depressed (not contented), shy, moody or impulsive, and low self-confidence, i.e. they tend to be highly vulnerable.
Openness	Openness refers to the characteristics of being curious, imaginative or creative, artistic, having broad interests, excitable, and different from others, i.e., they like to be unconventional.

As different traits are expected to exhibit different kinds of behaviours when subjected to the same situation such as when being subjected to phishing e-mails, researchers in the field of information security have argued that individual personality traits may have played a role in determining how likely someone is to be tricked by phishing attempts. This statement is supported by the findings of recent studies which revealed that certain types of personality traits are inherently at high risk of being phishing victims. As an example, Anawar et al. (2019) found that individuals with the trait of agreeableness which is associated with someone who has high levels of trust in others are more susceptible to phishing attacks as they are more likely to believe and act upon deceptive messages or requests sent by phishing attackers. This is because these groups of individuals according to Zhou et al. (2020) tend to be less sceptical and thus are more willing to engage with phishing emails. This argument is further amplified by Montañez et al. (2020) who found that agreeable individuals are more inclined to become phishing victims because in general, they are cooperative and empathetic and thus tend to comply with phishing requests to help others. However, in separate studies by Frauenstein and Flowerday (2020) and Lawson et al. (2020), the findings are the opposite as their results showed that individuals with the traits of agreeableness are less susceptible to phishing attacks. In both studies, the authors stated that this could be because they are a group of people that usually follow the policy and rules that in return would protect them against responding to phishing e-mails. As for the trait of extroversion, researchers such as Ge et al. (2021), Greitzer et al. (2021) and Yang et al. (2022) asserted that these groups of individuals may be highly susceptible to being phishing victims especially if the phishing e-mails that they receive appear to be originating from individuals that are known to them. Only findings by Anawar et al. (2019) and Lau et al. (2022) found that extrovert individuals are less susceptible to phishing because they tend to follow the majority when it comes to adhering to the rules and protocol when dealing with phishing e-mails.

On the trait of conscientiousness, almost all of the past studies mentioned earlier seem to be consistent in the sense that they may be less likely to fall for phishing attacks because they tend to give attention to detail in their actions (e.g., Anawar et al., 2019; Frauenstein & Flowerday, 2020; Ge et al., 2021). As a result, this group of individuals according to Ge et al. (2021) may be less easily persuaded by emotional appeals. As such if the phishers were to succeed in trapping the persons with the trait of conscientiousness, they may need to provide strong, fact-based arguments to change their opinions. While in general, the trait of conscientiousness may be the least susceptible to phishing attacks, the same cannot be said for individuals with the trait of neuroticism. In that sense, the majority of the studies reviewed found that neurotic people are the most susceptible to phishing attacks. The main reason behind the situation is that they tend to be emotionally unstable when faced with a threat such as phishing e-mails (Eftimie et al., 2022; Frauenstein & Flowerday, 2020; Lopez-Aguilar & Solanas, 2021; Power & Bello, 2022). Consequently, they may not carefully evaluate the potential risks associated with their actions and this may lead to them responding to phishing e-mails (Parker & Flowerday, 2020). In other words, as stated by Parker and Flowerday (2020), they may take action without thinking of the consequences and this in turn makes them easier targets for phishing attacks. As for the people with the trait of openness, the findings seem to be inconsistent. In that sense, one group of studies (e.g., Hamoud et al., 2022; Li et al., 2020; Sarno et al., 2023) revealed that they may have a higher tendency to respond to phishing e-mails. According to Sarno et al. (2023), one potential explanation for this phenomenon is that individuals with the trait of openness tend to engage in phishing e-mails out of curiosity to discover what would happen should they respond to such e-mails. On the opposite, a study by Alhaddad et al. (2023) found that people with the trait of openness may be less susceptible to phishing e-mails because they may be open to the measures provided to them to cope with the threat of phishing e-mails and thus making them less susceptible to phishing attacks.

Despite acknowledging that individuals' personality traits do have a role in influencing the individual decision to either reply or to click the attachment related to suspicious e-mails, to the knowledge of the current researcher, previous studies have not examined the role of individual protection as one of the many factors that may have important influence on individual decision making when faced with phishing e-mails. Therefore, this study intends to fill the gap by taking into consideration individual protection motivation as a possible determinant that could explain the variation in the level of relationships between personality traits and individual tendency to respond to phishing e-mails. Elaborating on Protection Motivation Theory (PMT), Li et al. (2022) explained that the PMT which was initially conceptualised by Rogers in 1975, is a useful theory that can help to explain how people would assess threats such as phishing e-mails and subsequently apply the coping mechanisms to protect themselves from such threat. The

basic elements of PMT consist of threat appraisal and coping appraisal. Threat appraisal refers to the evaluation of potential threats that an individual may encounter as a consequence of their actions upon receiving any suspicious emails while coping appraisal looks at how an individual sees themselves coping with the threat through the necessary actions (Williams & Joinson, 2020). As personality traits reflect individual unique characteristics and eventually influence how an individual takes action, it will also affect how people perceive their protection motivation level (Aharony et al., 2020; Ioannou et al., 2021). As an example, open individuals may be more willing to consider innovative or unconventional protective strategies, whereas those high in conscientiousness may prefer well-established and structured approaches (Leszko et al., 2020). It is for this reason that Bayl-Smith et al. (2021), suggested that PMT can be applied to the context of phishing susceptibility studies to understand how individuals assess the threat posed by phishing attacks, their motivation to protect themselves, and how their perceptions and personality traits influence their responses to phishing threats. On a separate note Vestad (2022), stated that personality traits related to motivation, such as the need for achievement or the desire for affiliation, can impact an individual's motivation to engage in protective behaviours. Vestad (2022) further gave an example, where individuals with high achievement motivation may be more driven to adopt protective measures to achieve specific protective goals.

Based on the identified research gaps and the opportunity provided by the PMT as a potential determinant that could explain why individuals would respond to phishing e-mails, two research questions were raised and therefore needed to be answered in this study. They are;

1) What is the relationship between individual personality traits and the level of individual protection motivation based on PMT?
2) What is the relationship between individual protection motivation and the tendency of an individual to respond to phishing e-mails?

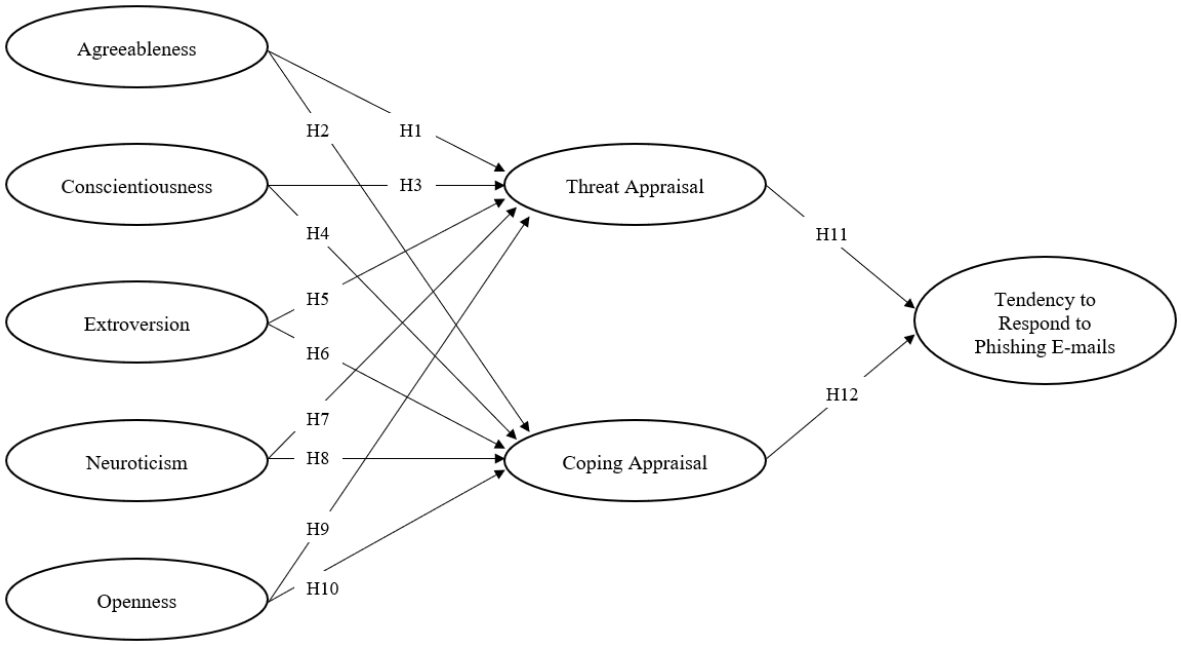
Therefore, the objectives of the study have been set as follows;

1) To determine the relationship between individual personality traits and the level of individual protection motivation based on PMT.
2) To determine the relationship between individual protection motivation and the tendency of an individual to respond to phishing e-mails.

STUDY CONCEPTUAL MODEL AND HYPOTHESES

Based on the above discussion, a conceptual model was developed (Figure 1) by combining PMT in relationships between personality traits based on the Big-Five Personality Model and an individual's tendency to respond to phishing e-mails. The independent variables will be the Big-Five Personality Model (which consists of Agreeableness, Conscientiousness, Extroversion, Neuroticism and Openness), PMT (Threat Appraisal and Coping Appraisal) and the dependent variable is a tendency to respond to phishing e-mails.

Figure 1. The study's conceptual model



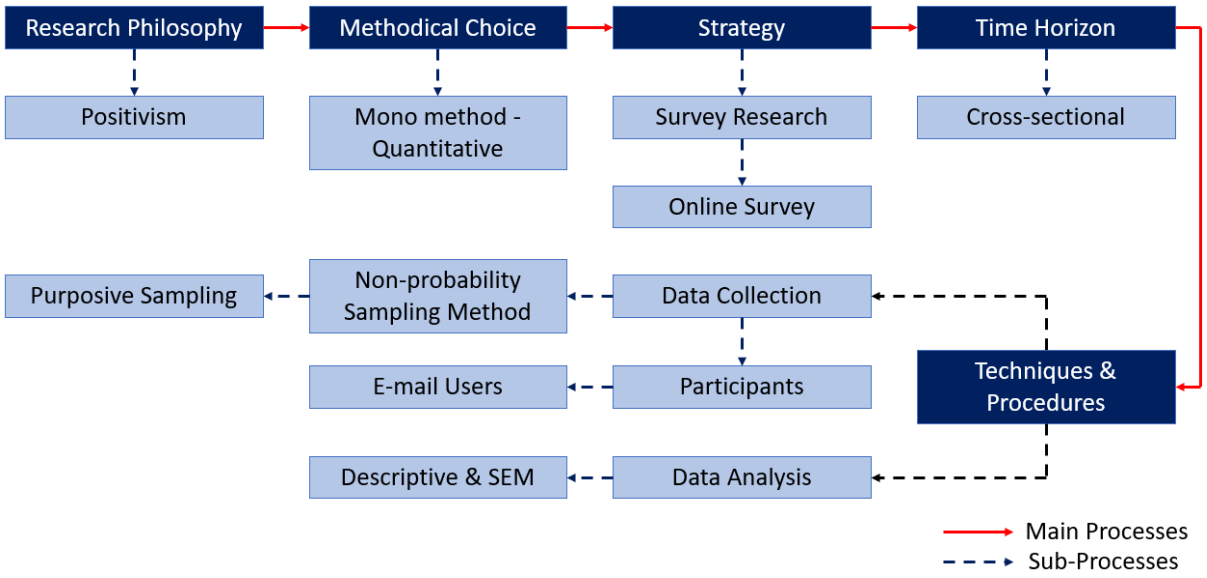
As illustrated in Figure 1, twelve relationships were investigated in this study and hence twelve hypotheses were tested to determine their directions and significance. The hypotheses are described below;

- H1: Agreeableness has a negative and significant relationship with threat appraisal.
- H2: Agreeableness has a positive and significant relationship with coping appraisal.
- H3: Conscientiousness has a negative and significant relationship with threat appraisal.
- H4: Conscientiousness has a positive and significant relationship with coping appraisal.
- H5: Extroversion has a negative and significant relationship with threat appraisal.
- H6: Extroversion has a positive and significant relationship with coping appraisal.
- H7: Neuroticism has a negative and significant relationship with threat appraisal.
- H8: Neuroticism has a positive and significant relationship with coping appraisal.
- H9: Openness has a negative and significant relationship with threat appraisal.
- H10: Openness has a positive and significant relationship with coping appraisal.
- H11: Threat Appraisal has a positive and significant relationship with the individual tendency to respond to phishing e-mails.
- H12: Coping Appraisal has a negative and significant relationship with the individual tendency to respond to phishing e-mails.

METHODOLOGY

This study followed a systematic research process illustrated in Figure 2 below. The process recommended by Chua (2020), covers all the main elements which include the research philosophy to be adopted, the choice of methodical to conduct the research, the strategy to get the data, the time horizon or the period of data collection and finally the techniques and procedures to collect and analyse the data.

Figure 2. The study's research process



As illustrated in Figure 2, this study adopted the positivist research philosophy in which this study will utilise the scientific method to gather the data and subsequently analyse the gathered data. Following that, only a quantitative method was employed to collect the data using the survey questionnaires which were distributed online through GoogleForm©. The data were only collected once, thus implying that the cross-sectional time horizon was used in this study. The current researcher employed a purposive sampling strategy to obtain participants in which the target audience consists of individuals who incorporated e-mail usage into their everyday work routines. To get a confidence level of 95%, a minimum sample size of 385 users was deemed necessary (Uakarn et al., 2021). The gathered data were analysed initially using the SPSS to describe the respondents and subsequently using the SmartPLS to provide the inferential analysis relationships.

The instrument used to collect the data consists of the following elements;

1) The Big Five Inventory (BFI) scale, a widely recognised and established tool in the public domain, was developed by John and Srivastava (1999) to assess personality traits. The questionnaire comprises a total of 44 items, each of which is evaluated on a five-point Likert scale ranging from 1 (Strongly disagree) to 5 (Strongly agree).
2) The measurement of PMT was conducted using the instrument devised by Williams and Joinson (2020). The questionnaire has 25 questionnaire items that evaluate individuals on their perception of Perceived Severity (PS) and Perceived Vulnerability (PV) for the Threat Appraisal, Response Efficacy (RE), Self-Efficacy (SE), Perceived Ability (PA), and Response Costs (RC) for the Coping Appraisal. All responses were graded on a scale of 1 to 5. (1 - Strongly disagree; 5 - Strongly agree).

3) The measurement of an individual tendency to respond to phishing e-mails was adapted from the work of Ferreira and Teles (2019). A total of 12 pictorial e-mail messages were used in which the respondents were asked on a multiple-choice item scale coded as 1 = Extremely Unlikely, 2 = Somewhat unlikely, 3 = Neither likely nor unlikely, 4 = Somewhat likely and 5 = Extremely likely.

Face and content validity were carried out and minor adjustments were made based on the advice from the consulted experts. Subsequently, a pilot study was conducted to check the instrument for reliability and based on the results of Cronbach's Alpha for all the variables, the questionnaires were deemed to meet the acceptable level of reliability as the values of Cronbach's Alpha all exceeded 0.70 (Hair et al., 2021).

RESULTS

Initially, a total of 403 participants participated in completing the questionnaires. Before conducting the descriptive and inferential analysis, the data were first examined for any missing data, suspicious response patterns, data outliers and data distribution. Upon examination of the data for the selected criteria, 3 gathered data were rejected due to suspicious response patterns, making the final data which are deemed fit for further analysis reduced to 400. Therefore, this study is considered to have fulfilled the criterion of a minimum sample of 385 mentioned earlier.

Table 2. Demographic analysis of the respondents

Items	Options	Frequency	Percentage (%)
Gender	Male	292	73.0
	Female	108	27.0
Age Group	Below 20 years old	0	0
	20 - 29	29	7.2
	30 - 39	136	34.0
	40 - 49	195	48.8
	50 years old and above	40	10.0
Employment Status	Public Sector	79	19.8
	Private Sector	284	71.0
	Self-employed	25	6.2
	Unemployed	12	3.0
Educational Status	SPM / MCE	5	1.3
	Certificate / Diploma	45	11.3
	Bachelor's Degree / Equivalent Professional Qualification	303	75.8
	Postgraduate Degree (Master or PhD)	47	11.8

In terms of the final 400 respondents, demographic analysis revealed that the majority of them are male which accounted for 292 individuals or 73% of the total, while female participants accounted for 108 individuals or 27%. On the age group of respondents, most are from the 40-49 age group (48.8%), followed by the age group of 30-39 years old (34%), 50 years and above (10%) and finally 7.2% are from the age group of 20-29 years old. None of the respondents are from the age group below 20 years old. As for the employment status, most are working for the private sector which constituted 71% of the total followed by the public sector 19.8%, self-employed 6.2% and unemployed 3%. Concerning educational status, 75.8% have at least a bachelor's degree or equivalent professional qualification while almost the same percentage of respondents have at least a certificate or diploma (11.3%) and a postgraduate degree (Master's or PhD) (11.8%). Only 5% of respondents have at least an SPM or MCE level of education.

Following the descriptive analysis, the next analysis will be the inferential analysis. Structural Equation Modelling (SEM) approach was used to conduct the inferential analysis on the conceptual model using a statistical software tool SmartPLS® 3.2. As recommended by Hair et al. (2019), the analysis must follow certain steps which must first start with an outer model assessment and followed by an inner model assessment. Table 3 shows the results of the outer model assessment of the conceptual model.

Table 3. Results of outer model assessment

Latent Variable	Indicators	Convergent Validity			Internal Consistency Reliability	
		Loadings (>0.70)	Indicator Reliability (>0.50)	AVE (>0.50)	Composite Reliability (>0.60)	Cronbach's Alpha (>0.70)
Agreeableness	A2	0.789	0.622	0.610	0.891	0.851
	A7	0.820	0.672			
	A12	0.747	0.558			
	A17	0.799	0.638			
	A22	0.805	0.648			

	A27	0.803	0.644			
	A32	0.805	0.648			
	A37	0.717	0.514			
	A42	0.734	0.538			
Conscientiousness	C3	0.737	0.543	0.600	0.895	0.847
	C8	0.731	0.534			
	C13	0.770	0.593			
	C18	0.790	0.624			
	C23	0.803	0.644			
	C28	0.784	0.614			
	C33	0.817	0.667			
	C38	0.777	0.604			
	C43	0.760	0.577			
Extroversion	E1	0.786	0.618	0.618	0.879	0.853
	E6	0.779	0.607			
	E11	0.762	0.581			
	E16	0.837	0.701			
	E21	0.766	0.587			
	E26	0.799	0.638			
	E31	0.733	0.537			
	E36	0.782	0.611			
Neuroticism	N4	0.777	0.603	0.622	0.927	0.901
	N9	0.711	0.505			
	N19	0.755	0.570			
	N24	0.826	0.682			
	N29	0.740	0.547			
	N34	0.837	0.700			
	N39	0.862	0.743			
Openness	O10	0.757	0.573	0.600	0.878	0.874
	O15	0.766	0.587			
	O20	0.815	0.664			
	O25	0.781	0.610			
	O30	0.778	0.605			
	O35	0.787	0.619			
	O40	0.806	0.649			
	O41	0.737	0.543			
	O44	0.743	0.552			
Threat Appraisal	PS1	0.744	0.553	0.530	0.802	0.803
	PS2	0.704	0.496			
	PS3	0.705	0.497			
	PS4	0.727	0.528			
	PS5	0.721	0.520			
	PS6	0.702	0.493			
	PV1	0.735	0.540			
	PV2	0.733	0.537			
	PV3	0.750	0.562			
	PV4	0.753	0.567			
	PV5	0.734	0.539			
Coping Appraisal	PA1	0.760	0.577	0.551	0.831	0.821
	PA2	0.734	0.539			
	PA3	0.739	0.546			
	RC1	0.739	0.546			
	RC2	0.750	0.562			
	RC3	0.753	0.567			
	RC4	0.743	0.552			
	RE1	0.742	0.550			
	RE2	0.735	0.540			
	RE3	0.742	0.550			
	SE1	0.754	0.568			
	SE2	0.721	0.520			
	SE3	0.750	0.562			
	SE4	0.733	0.537			
Tendency to Respond to Phishing E-mails	AUT1	0.772	0.596	0.568	0.837	0.822
	AUT2	0.769	0.591			
	AUT3	0.726	0.527			
	COM1	0.760	0.577			

COM2	0.728	0.530
COM3	0.741	0.549
LIK1	0.756	0.571
LIK2	0.731	0.534
LIK3	0.751	0.564
SCA1	0.741	0.549
SCA2	0.761	0.579
SCA3	0.801	0.642

As with any analysis involving the SEM, the first step in the assessment of the other model involved the examination of the outer loadings for each of the indicators which should be more than 0.70. Any value less than 0.70 will affect indicator reliability values which should be at least 0.50. In this study, two indicators were rejected due to their factor loadings of less than 0.70. They are N14 of the Neuroticism construct and O5 of the Openness construct. On the values of the average variance extracted (AVE), the values for all the constructs were all greater than 0.5 (Agreeableness 0.610, Conscientiousness 0.600, Extroversion 0.618, Neuroticism 0.622, Openness 0.600, Threat Appraisal 0.530, Coping Appraisal 0.551 and Tendency to Respond to Phishing E-mails 0.568). As for the composite reliability, the construct reliability of all constructs is considered satisfactory since all its values are greater than 0.60 (Agreeableness 0.891, Conscientiousness 0.895, Extroversion 0.879, Neuroticism 0.927, Openness 0.878, Threat Appraisal 0.802, Coping Appraisal 0.831 and Tendency to Respond to Phishing E-mails 0.837). As such based on the results of the average variance extracted (AVE) and composite reliability, it is confirmed that the model met the requirement for satisfactory convergent validity. Finally, the value of Cronbach Alpha which was used for testing the internal reliability of the variables showed that all the constructs were above the minimum of 0.70 (Agreeableness 0.851, Conscientiousness 0.847, Extroversion 0.853, Neuroticism 0.901, Openness 0.874, Threat Appraisal 0.803, Coping Appraisal 0.821 and Tendency to Respond to Phishing E-mails 0.822). Therefore, the values confirmed that the constructs fulfil the requirement for internal reliability.

Meanwhile, the variables' discriminant validity is measured using the Fornell-Larcker Criterion. The Fornell-Larcker's criterion value for a particular construct is considered satisfactory if the square root of each variable's AVE is larger than the highest correlation value of the particular variable against other variables (Hair et al., 2019). The results of Fornell-Larcker's criterion value are indicated in Table 4.

Table 4. Fornell-Larcker Criterion

	A	C	C. A.	E	N	O	RPE	T. A.
A	**0.781**							
C	0.472	**0.775**						
C. A.	-0.115	0.124	**0.742**					
E	0.255	0.125	-0.141	**0.786**				
N	0.221	0.118	-0.112	-0.119	**0.789**			
O	0.330	0.489	0.073	0.175	0.077	**0.775**		
RPE	-0.162	-0.137	-0.277	-0.023	-0.029	-0.051	**0.753**	
T. A.	-0.218	-0.106	0.254	-0.210	-0.043	-0.029	0.382	**0.728**

Note,
A = Agreeableness, C = Consciousness, C.A. = Coping Appraisal, E = Extroversion, N = Neuroticism, O = Openness, RPE. = Responding to Phishing E-mail, T.A. = Threat Appraisal

As indicated in Table 4, the results of discriminant validity were satisfactory as evidenced by the fact that the square root of each variable's Average Variance Extracted (AVE) exceeded its correlation value with any other variables (values in bold).

Following the satisfactory assessment of the outer model, the next analysis will involve conducting the inner assessment of the conceptual model which will provide the assessment of the relationships between the constructs. The results from the relationship or path analysis will then be used to determine the acceptance or rejection of the hypotheses of this study.

In that sense, the primary objective of relationship or part analysis is to establish, whether the model used in this study can provide a meaningful explanation of the relationships between constructs of the model (Hair et al., 2019). Therefore, evaluation of the relationships of the constructs will help the researcher to determine the existence of whether changes in the values of one construct will cause changes in the corresponding construct (also known as causal relationships) or none (non-causal relationships). This is provided by two distinctive parameters; the magnitude of the relationships between the constructs of the model and whether the relationships between any two of the variables are statistically significant or vice-versa (Hair et al., 2019). The magnitude of the relationships is provided through the values of β. The higher the values, the greater would be the magnitude of relationships between the constructs. The positive or negative values of β imply whether changes in the preceding variable will cause a change in the corresponding construct in the same direction (positive) or the opposite direction (negative). As for the significance of the relationships, it is determined by the values of *p* which must be smaller than 0.05 and the value of *t* which must be greater than 1.96. Both values are automatically computed by the SmartPLS® software.

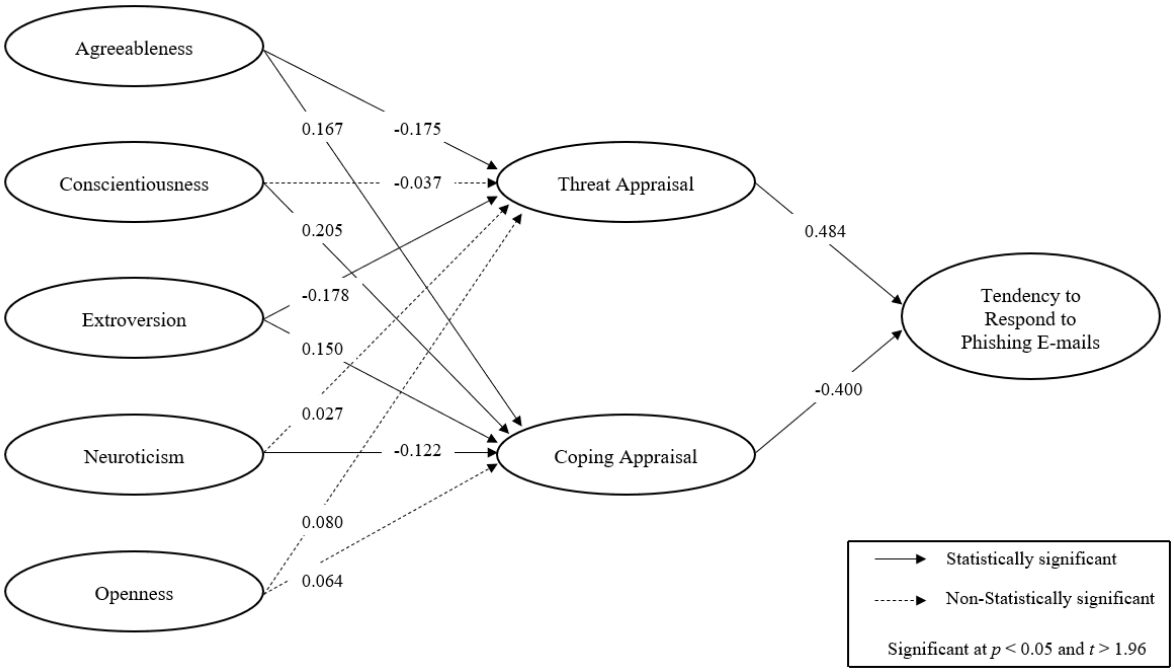
In addition to testing the magnitude and significance of the relationships, Hair et al. (2019) also recommended the evaluation of the path relationships for their effect size. Effect size essentially provides the evaluation of how much the changes in values of one construct will have an impact on the corresponding construct and it is indicated by the f^2 values. Through the f^2 values, researchers can determine the study's overall contribution (Hair et al., 2019). As a guide, f^2 values are assessed based on certain value ranges. The f^2 values that are between 0.02–0.14 are considered to have a small effect, 0.15–0.34 represent a medium effect and values of 0.35 and above represent large effects of the relationships between the exogenous latent variable on an endogenous latent variable. The f^2 value that is less than 0.02 indicates that there is no effect on the relationships between the constructs (Hair et al., 2019). Table 5 provides the results of the inner model assessment as well as decisions on the hypotheses.

Table 5. Results of inner model assessment

Tested	Relationship	β	*t*-value	*p*-value	Effect Size *f*	Decision (Based on *p*-values)	Decision (Based on f^2-values)	Decision on Hypothesis
H1	Agreeableness → Threat Appraisal	-0.175	3.063	0.002	0.023	Significant	Small effect	Accepted
H2	Agreeableness → Coping Appraisal	0.167	2.859	0.004	0.021	Significant	Small effect	Accepted
H3	Conscientiousness → Threat Appraisal	-0.037	0.548	0.584	0.01	Not Significant	No Effect	Rejected
H4	Conscientiousness → Coping Appraisal	0.205	3.629	0.000	0.030	Significant	Small effect	Accepted
H5	Extroversion → Threat Appraisal	-0.178	3.950	0.000	0.031	Significant	Small effect	Accepted
H6	Extroversion → Coping Appraisal	0.150	2.705	0.007	0.022	Significant	Small effect	Accepted
H7	Neuroticism → Threat Appraisal	0.027	0.319	0.750	0.001	Not Significant	No effect	Rejected
H8	Neuroticism → Coping Appraisal	-0.122	2.003	0.045	0.025	Significant	Small effect	Rejected
H9	Openness → Threat Appraisal	0.080	0.757	0.449	0.005	Not Significant	No effect	Rejected
H10	Openness → Coping Appraisal	0.064	0.981	0.327	0.003	Not-Significant	No effect	Rejected
H11	Threat Appraisal → Tendency to Respond to Phishing E-mails	0.484	9.249	0.000	0.311	Significant	Medium effect	Accepted
H12	Coping Appraisal → Tendency to Respond to Phishing E-mails	-0.400	10.311	0.000	0.213	Significant	Medium effect	Accepted

Based on the results of the inner model assessment in Table 5, the path diagram as illustrated in Figure 3 provides a pictorial view of the significance or non-significance of the relationships as well as the direction of the relationships between the constructs. The negative values of beta (ß) indicate that the increase in the value of one construct will cause the value of the connected construct to increase in the opposite direction and vice-versa. Meanwhile, the positive values of beta (ß) show that the increase in the value of one construct will cause the value of the connected construct to increase in the same direction. As for the *p*-values, the significant relationships are indicated by solid lines while the non-significance relationships are indicated by the dotted lines.

Figure 3. Study's Structural Model



DISCUSSION

To understand the findings of this study and how it can impact the knowledge on why certain types of individuals have a higher tendency to respond to phishing e-mails, it is necessary to first evaluate the result of relationships between coping and threat appraisal and the tendency to respond to phishing e-mails. The findings of this study found that threat appraisal has a significant relationship and positive path coefficient with the tendency to respond to phishing e-mails (β = 0.484, *p*-value =0.000, medium effect). This shows that a person who appraises themselves as vulnerable to phishing attacks would likely respond to phishing e-mails. In other words, a person who scores high threat appraisal would likely fall victim to phishing attacks. On the other hand, the results of a significant relationship and negative path coefficient (β = -0.400, *p*-value =0.000, medium effect) between coping appraisal and the tendency to respond to phishing e-mails imply that an individual who scores high in coping appraisal would likely be less likely to become a victim of phishing attacks. Therefore based on values of values of both β and *p*, this study accepted H11 and H12. The results of these relationships seem to be consistent with the findings by Jansen and Van Schaik (2019) and Li et al. (2022) concerning the application of the PMT framework when it comes to the individual's threat and coping level perception.

Once the relationships between threat and coping appraisal have been determined, the next step is to determine the status of relationships between the five personality traits and coping and threat appraisal. This will help to discover which of the five personality traits will most likely respond to phishing e-mails and subsequently provide an indication of which of the traits would potentially become a victim of phishing attacks. In this sense, the indication of the trait that inclines to respond to phishing e-mails will be both determined by whether the relationship is significant or non-significant as well as the direction of such relationships. The first personality trait to be examined is the trait of agreeableness. Based on the results illustrated in Table 5, it was found that agreeableness had significant relationships with both the threat and coping appraisal, however, it had a negative relationship with threat appraisal and a positive relationship with coping appraisal (β = -0.175, *p*-value =0.002, small effect and β = 0.167, *p*-value =0.004, small effect) for the relationships with threat appraisal and coping appraisal respectively. This implies that they believe they are not affected by the threat of being a phishing victim as indicated by the negative path coefficient of the relationship. At the same time, they perceived that they could cope with phishing threats satisfactorily. As a result, they may be less likely to respond to phishing e-mails. As such both hypotheses H1 and H2 are accepted. The findings for the trait of extroversion are similar in pattern to that of the trait of agreeableness. Both had significant and opposite directions of relationships with threat and coping appraisal i.e., a negative relationship with threat appraisal and a positive relationship with coping appraisal (β = -0.178, *p*-value =0.000, small effect and β = 0.150, *p*-value = 0.007, small effect) respectively. Thus, similar to the trait of agreeableness, individuals with the trait of extroversion are predicted to be less likely to respond to phishing e-mails. As such, similar to the trait of agreeableness, this study accepted the hypotheses H5 and H6.

Meanwhile, for the trait of conscientiousness, the analysis of the results revealed that it had a non-significant relationship with threat appraisal but a significant relationship with coping appraisal. On the direction of the relationships, it had a negative, non-significant relationship with threat appraisal and a positive significant relationship with coping appraisal (β = -0.037, *p*-value = 0.584, small effect and β = 0.205, *p*-value = 0.000, small effect) respectively. As a result, this study rejected hypothesis, H3 but accepted hypothesis, H4. Commenting further on the results, it can be said that individual with the trait of conscientiousness is not concerned with the threat of phishing e-mails as shown by the non-significant relationship and negative direction of the relationship.

As for its relationship with coping appraisal, owing to its characteristics which are more particular, disciplined and not wanting to take any risks, the result of the relationship was as expected in which the direction of the relationship was positive, i.e., persons with the trait of conscientiousness are expected to cope well with any phishing threats and thus making them unlikely to respond to phishing e-mails send to them.

On the other hand, the results for the trait of neuroticism show that it has a positive and non-significant relationship with threat appraisal and a negative significant relationship with coping appraisal (β = 0.027, *p*-value = 0.750, no effect and β = -0.122, *p*-value = 0.045, small effect). Based on the results, it can be concluded that in general people with the trait of neuroticism perceived that are vulnerable to phishing attacks although the perception may not be significant. In addition, they perceived that they may not have sufficient coping strategies to deal with phishing attacks as indicated by the negative relationship. They are therefore predicted to respond to any phishing e-mails sent to them. Therefore, based on the path analysis values, this study rejected the hypotheses H8 and H9. Finally, as for people with the trait of openness, the results from the analysis appeared to be inconclusive as both of their relationships with threat and a coping appraisal are non-significant as shown by β = 0.080, *p*-value = 0.449, no effect and β = 0.064, *p*-value =0.327, no effect respectively and thus rejecting both hypothesis H9 and H10. In that sense, the PMT cannot be used to predict whether an individual with the trait of openness would respond to phishing e-mails sent to them or vice-versa. The findings of the relationships between personality traits, threat and coping appraisal are very much aligned with the findings by Pilch et al. (2021) who found that different personality traits would generally exhibit different levels of treatment towards the threat and coping appraisal and thus influence their levels of threat avoidance.

THEORETICAL AND PRACTICAL CONTRIBUTION OF THIS STUDY

This study contributed to the body of knowledge from two perspectives; theoretical and practical contribution. From the theoretical perspective, this study further extends the application of both individual personality traits and PMT in the field of information security. This study re-affirms the findings of previous studies by demonstrating that individual personality traits do play a role in determining the likelihood of a person responding to phishing e-mails. In the same manner, this study has also shown the role of threat and coping appraisal as determinants that could determine how individuals of different personality traits would be expected to respond to phishing e-mails and thus helps to address a critical inquiry into the underlying factors contributing to an individual's vulnerability to phishing attacks. Therefore, the application of combined theories of the Big-Five Personality Model and PMT as used in this study can enhance our understanding of explaining the 'why factor' of how an individual can potentially fall victim to phishing attacks due to their unique characteristics which in turn determine their different level of motivation. The successful application of the combined theories of this study can thus be utilised in future research to explore various information security concerns, including susceptibility to phone scams and phishing in social media settings.

Secondly, this study provides practical contributions by providing knowledge to information security practitioners in which any programs that aim to protect individuals from phishing attacks must take into account activities that will increase their coping strategies on how to handle phishing e-mails effectively. In that sense, the current researcher recommended several activities that may potentially increase individual coping strategies when handling phishing e-mails. The suggested activities include; (1) conducting effective phishing awareness training, education programs, and awareness campaigns; (2) increasing the dissemination of cues regarding phishing issues, particularly within the organisation; (3) discouraging inadequate anti-phishing behaviours such as bad e-mail habit handling process while simultaneously devising strategies to promote good anti-phishing practices among users; and (4) formulating and updating information security policies related to phishing as necessary. It is expected through the above activities, policymakers and decision-makers within an organisation as well as individuals may be able to protect themselves from the vulnerability to phishing attacks.

LIMITATIONS OF THE STUDY AND DIRECTION OF FUTURE RESEARCH

The current researcher identified several limitations in the current study, which could be improved by future studies. Among them is the limited location from which the data was collected i.e., it is limited only to Klang Valley. As such future studies may expand the area of data collection to perhaps the whole country as this would provide a better generalisation of the findings. Secondly, this study only used images of phishing e-mails as a means to determine individuals' perceptions as to whether they would respond to such e-mails. This can be improved in future studies by experimenting with the process involving sending actual e-mail messages to the target respondents to gauge their responses. Thirdly, the effect of demographic variations such as age and gender were not evaluated in the model. Therefore, future studies can consider age and gender as additional variables in the model, possibly as the moderating variables. Finally, this study did not take into consideration the knowledge level of the participants as previous studies have shown that people's tendency to respond to phishing e-mails can be reduced through the educational method. Therefore, it is suggested that future studies will take this consideration as it will help to provide a more holistic understanding of the model used in this study.

CONCLUSION

In the literature review section, two research questions were outlined. Based on the findings of this study, the answers to the research questions are illustrated as follows. On the first research objective which is to determine the relationship between individual personality traits and the level of individual protection motivation based on PMT, the study found that the traits of agreeableness, conscientiousness, extroversion and neuroticism do exhibit certain levels of relationships with both or either one elements of PMT. On the second research objective which is to determine the relationship between individual protection motivation and the tendency of an individual to respond to phishing e-mails, this study revealed that those who have adequate levels of coping strategies will be less likely to fall victim to phishing attacks while those who believe that they are vulnerable to phishing attacks

and yet did not take any measure to have coping strategies in dealing with phishing attacks will likely to fall victims into phishing attacks.

Therefore, this study can be concluded as follows; (1) individuals' tendency to respond to any phishing e-mails will depend on their level of protection motivation. In that sense, those who score higher on coping appraisal than threat appraisal and at the same time exhibit the direction of relationships mentioned in the previous section will be less likely to respond to phishing e-mails and (2) individual level of protection motivation towards responding to phishing e-mails is determined by their personality traits and in particular individuals with the trait of neuroticism are expected to respond to phishing e-mails.

REFERENCES

Abood, N. (2019). Big Five Traits: A critical review. *Gadjah Mada International Journal of Business*, 21(2), 159–186. https://doi.org/10.22146/gamaijb.34931

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

Aharony, N., Bouhnik, D., & Reich, N. (2020). Readiness for information security of teachers as a function of their personality traits and their assessment of threats. *Aslib Journal of Information Management, 72*(5), 787–812. https://doi.org/10.1108/ajim-12-2019-0371

Alhaddad, M., Mohd, M., Qamar, F., & Imam, M. (2023). Study of student personality trait on spear-phishing susceptibility behavior. *International Journal of Advanced Computer Science and Applications, 14*(5). https://doi.org/10.14569/ijacsa.2023.0140571

Anawar, S., Kunasegaran, L. D., Mas'ud, M. Z., & Zakaria, N. A. (2019). Analysis of phishing susceptibility in a workplace: A big-five personality perspectives. *Journal of Engineering Science and Technology*, 14(5), 2865–2882. https://jestec.taylors.edu.my/Vol%2014%20issue%205%20October%202019/14_5_30.pdf

Bayl-Smith, P., Taib, R., Yu, K., & Wiggins, M. (2021). Response to a phishing attack: Persuasion and protection motivation in an organisational context. *Information & Computer Security, 30*(1), 63–78. https://doi.org/10.1108/ics-02-2021-0021

Bernama (2023, January 14). Almost RM600 million was lost to cybercrime in 2022. *New Straits Times*. *https://www.nst.com.my/news/nation/2023/01/870171/almost-rm600-million-lost-cyber-crime-2022*

Burns, A. J., Johnson, M. E., & Caputo, D. D. (2019). Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organisational Computing and Electronic Commerce*, *29*(1), 24–39. https://doi.org/10.1080/10919392.2019.1552745

Chua, Y. P. (2020). *Mastering research methods (3rd ed.)*. McGraw-Hill (Malaysia).

Eftimie, S., Moinescu, R., & Racuciu, C. (2022). Spear-phishing susceptibility stemming from personality traits. *IEEE Access*, 10, 73548–73561. https://doi.org/10.1109/access.2022.3190009

Ferreira, A., & Teles, S. (2019). Persuasion: How phishing e-mails can influence users and bypass security measures. *International Journal of Human-Computer Studies*, *125*, 19–31. https://doi.org/10.1016/j.ijhcs.2018.12.004

Frauenstein, E. D., & Flowerday, S. (2020). Susceptibility to phishing on social network sites: A personality information processing model. *Computers & Security*, *94*, 101862. https://doi.org/10.1016/j.cose.2020.101862

Ge, Y., Lu, L., Cui, X., Chen, Z., & Qu, W. (2021). How personal characteristics impact phishing susceptibility: The mediating role of mail processing. *Applied Ergonomics*, *97*(6), 103-105. https://doi.org/10.1016/j.apergo.2021.103526

Greitzer, F. L., Li, W., Laskey, K. B., Lee, J., & Purl, J. (2021). Experimental investigation of technical and human factors related to phishing susceptibility. *ACM Transactions on Social Computing*, *4*(2), 1–48. https://doi.org/10.1145/3461672

Griffiths, C. (2023, March 24). *The latest phishing statistics*. AAG IT Services. https://aag-it.com/the-latest-phishing-statistics/

Hair, J. F., C., B. W., Babin, B. J., & Anderson, R. E. (2021). *Multivariate data analysis*. Pearson Prentice Hall.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review, 31*(1), 2–24. https://doi.org/10.1108/ebr-11-2018-0203

Hamoud, A., Aimeur, E., & Benmohammed, M. (2022). Individual processing of phishing emails: Towards a phishing detection framework. *International Journal of Security and Privacy in Pervasive Computing, 14*(1), 1–22. https://doi.org/10.4018/ijsppc.311060

Ioannou, A., Tussyadiah, I., & Marshan, A. (2021). Dispositional mindfulness as an antecedent of privacy concerns: A protection motivation theory perspective. *Psychology & Marketing, 38*(10), 1766–1778. https://doi.org/10.1002/mar.21529

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: Towards an effective anti-phishing training. A comparative literature review. *Human-Centric Computing and Information Sciences*, *10*(1). https://doi.org/10.1186/s13673-020-00237-7

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

John, O. P., & Srivastava, S. (1999). *Handbook of personality theory and research*. The Guilford Press.

Lau, N., Wang, L., Hur, I., & Clarke, M. (2020). The influence of cognitive factors and personality traits on mobile device user's information security behavior. *Issues In Information Systems*, *21*(2), 279–288. https://doi.org/10.48009/2_iis_2020_279-288

Lawson, P., Pearson, C. J., Crowson, A., & Mayhorn, C. B. (2020). E-mail phishing and signal detection: How persuasion and personality influence response patterns and accuracy. *Applied Ergonomics*, *86*, 103084. https://doi.org/10.1016/j.apergo.2020.103084

Leszko, M., Iwański, R., & Jarzębińska, A. (2020). The relationship between personality traits and coping styles among first-time and recurrent prisoners in Poland. *Frontiers in Psychology*, *10*. https://doi.org/10.3389/fpsyg.2019.02969

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, *5*, 100165. https://doi.org/10.1016/j.chbr.2021.100165

Li, W., Lee, J., Purl, J., Greitzer, F., Yousefi, B., & Laskey, K. (2020). Experimental investigation of demographic factors related to phishing susceptibility. *Proceedings of the 53rd Hawaii International Conference on System Sciences*. https://doi.org/10.24251/hicss.2020.274

Lopez-Aguilar, P., & Solanas, A. (2021). Human susceptibility to phishing attacks based on personality traits: The role of neuroticism. *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC).* https://doi.org/10.1109/compsac51774.2021.00192

Montañez, R., Golob, E., & Xu, S. (2020). Human cognition through the lens of social engineering cyberattacks. *Frontiers in Psychology, 11*. https://doi.org/10.3389/fpsyg.2020.01755

Muharram, S. S., Suhaimi, M. Z., & Marcus, M. (2022). Cybercrime in Malaysia. *Journal of Education and Social Sciences*, *22*(1), 34–38. https://doi.org/https://doi.org/10.1016/j.cose.2016.03.015

Parker, H. J., & Flowerday, S. V. (2020). Contributing factors to increased susceptibility to social media phishing attacks. *SA Journal of Information Management, 22*(1). https://doi.org/10.4102/sajim.v22i1.1176

Pilch, I., Wardawy, P., & Probierz, E. (2021). The predictors of adaptive and maladaptive coping behavior during the COVID-19 pandemic: The protection motivation theory and the big five personality traits. *PLOS ONE*, *16*(10). https://doi.org/10.1371/journal.pone.0258606

Power, V., & Bello, A. (2022). Individual differences in cyber security behavior using personality-based models to predict susceptibility to sextortion attacks. *Cybersecurity and Cognitive Science,* 89–113. https://doi.org/10.1016/b978-0-323-90570-1.00004-8

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(4), 89. https://doi.org/10.3390/fi11040089

Sarno, D. M., Harris, M. W., & Black, J. (2023). Which phish is captured in the net? understanding phishing susceptibility and individual differences. *Applied Cognitive Psychology, 37*(4), 789–803. https://doi.org/10.1002/acp.4075

Stojnic, T., Vatsalan, D., & Arachchilage, N. A. (2021). Phishing email strategies: Understanding cybercriminals' strategies of crafting phishing emails. *Security and Privacy*, 4(5). https://doi.org/10.1002/spy2.165

Taib, R., Yu, K., Berkovsky, S., Wiggins, M., & Bayl-Smith, P. (2019). Social engineering and organisational dependencies in phishing attacks. *Human-Computer Interaction – INTERACT 2019*, 564–584. https://doi.org/10.1007/978-3-030-29381-9_35

Uakarn, C., Chaokromthong, K., & Sintao, N. (2021). Sample size estimation using Yamane and Cochran and Krejcie and Morgan and Green Formulas and Cohen statistical power analysis by g*power and comparisons. *Apheit International Journal*, *10*(2), 76–86. https://doi.org/https://doi.org/10.1277/1541931213601769

Vestad, A. (2022). Personality traits and security motivation. *Stud Health Technol Inform*, *4*(22), 183–188. https://doi.org/10.3233/SHTI220980

Williams, E. J., & Joinson, A. N. (2020). Developing a measure of information seeking about phishing. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa001

Yang, R., Zheng, K., Wu, B., Li, D., Wang, Z., & Wang, X. (2022). Predicting user susceptibility to phishing based on multidimensional features. *Computational Intelligence and Neuroscience*, *2022*, 1–11. https://doi.org/10.1155/2022/7058972

Zhou, J., Luo, S., & Chen, F. (2020). Effects of personality traits on user trust in human–machine collaborations. *Journal on Multimodal User Interfaces*, 14(4), 387–400. https://doi.org/10.1007/s12193-020-00329-9

Allen Peter Diman,
School of Graduate Studies,
Asia e University,
47500 Subang Jaya, Selangor.
E-mail: allen.diman@aeu.edu.my

Professor Dr. Titik Khawa Abdul Rahman
School of Graduate Studies
Asia e University,
47500 Subang Jaya, Selangor, Malaysia
Email: titik.khawa@aeu.edu.my