Journal of Engineering Science and Technology
Vol. 14, No. 5 (2019) 2865 - 2882

ANALYSIS OF PHISHING SUSCEPTIBILITY IN A WORKPLACE: A BIG-FIVE PERSONALITY PERSPECTIVES

SYARULNAZIAH ANAWAR*, DURGA L. KUNASEGARAN, MOHD Z. MAS'UD, NURUL A. ZAKARIA

Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia
*Corresponding Author: syarulnaziah@utem.edu.my

Abstract

Employee is frequently referred to as the weakest link in the cyber security in an organization. Differences in the employees' personality makes it hard for any organization to design a proper mitigation strategy in order to prevent them from being a victim of phishing attack. Besides, users' general life experience and technological experience will also influence the type of user's personality traits while handling or interacting with the security system, which affects their susceptibility towards phishing. The objective of this paper is to examine the personality traits that influence phishing susceptibility among employees in a workplace, and to investigate the influence of employees' experience in shaping employees' personality and consequently their behaviour in resisting phishing attack. This study used quantitative method. A survey (N = 252) of employees in mid-sized IT related companies in Malaysia attempted to identify individual's characteristics that relate to phishing susceptibility and characterize the higher-risk employees that pose threats to the companies. This paper presents three notable findings. First, the results of correlation analysis emphasized the importance of employees' technical and general experience in shaping their personality to resist phishing attack. Secondly, the results of correlation analysis show that conscientiousness and self-monitoring personality traits were positively related with employee's secure behaviour towards phishing threats. Finally, this study concluded that extroversion personality had the strongest influence towards phishing susceptibility, followed by self-monitoring, agreeableness and conscientiousness. The findings suggest that there is an inverse influence between personality traits (independent variables) and user behaviour (dependent variable). The proposed framework is useful for research attempting to shift concern on human factors in order to help organization improving employees' cyber security compliance.

Keywords: Cyber security, Personality, Phishing, Social Engineering.

1. Introduction

Over the years, phishing is increasingly recognized as a serious, worldwide cybersecurity concern for both individuals and organizations. According to KnowBe4 [1], the most alarming aspect is that 90-95 percent of all successful cyber-attacks begin with a phishing email. PhishMe [2] conducted a recent study involving 8 million phishing-simulation emails to more than 3.5 million employees in 23 industries worldwide and revealed that 87 percent of the employees responded to a phishing simulation by emailing the same day it was sent. Attackers are crafty in devising various strategies to tempt an individual to click or open an attachment or link. According to security software firm Trend Micro, 91 percent of all phishing attack targeted employees within an organization, known as "spear-phishing" email [3]. This type of more sophisticated phishing scams, appears genuine to the employees, hence, explaining the reasons they fall for the phishing scam easily.

Zaki et al. [4] and Swart et al. [5] reported that employees are easier targets due to their susceptibility to various emotional and contextual triggers, and they may disregard certain security requirements when handling their emails. Defence measures that are currently used in organizations such as patches, anti-virus software and many more do not function as a full security mechanism for employees because they are their biggest threat. Conducting phishing, security tests and security awareness training are few mitigation strategies to decrease unintentional insider threats in an organization. However, if significant concerns are not put in place to effectively gauge the employee's response patterns from a human landscape perspective, phishing tests and assessment can create organizational social engineering blind spots.

Therefore, understanding employee's behaviour patterns in responding to phishing mail should go beyond assessment metrics because it is relative to their personality traits and cognitive reasoning. Employees response decision when receiving a target phishing email is based on the information cues that mediate between the email and the internal perceptions, shaped by their characteristics and past experience [6]. Without a proper mitigation strategy that is catered properly for employees with different personalities, someone will somehow be subjected to a phishing attack in that particular organization regardless of the type of organization (IT or non-IT) or educational background possessed by the employee.

This study focuses on the following research questions: (1) To what extent employees' personality traits affect their likelihood to respond to the phishing scam in the workplace? (2) To what extent employees' experience is related to their personality and consequently their decision outcomes, thus, revealing the nature of phishing victims? Guided by a theoretical foundation in Big-Five Personality Model [7], our research model attempts to examine the individual experience (such as experience of email-based scam) and individual personality traits, and investigates their impacts on the likelihood of user behaviour subject to phishing (such as installing software from an advertisement or pop up window).

The rest of the paper is organized as follows: Section 2 explains social engineering and phishing susceptibility concept. Section 3 provides understanding of employees' behaviours in phishing, by reviewing related work on phishing susceptibility in the organizational setting. This section also presents the Big-Five Personality Model as the theoretical foundation for the proposed phishing susceptibility framework. Section 5 provides the details of quantitative

methodology used in this study that covers the process in research model development, instrument design and data collection. Subsequently, Section 6 presents the findings of data analyses. Section 7 provides a discussion on the findings. Finally, Section 8 presents the contributions of the proposed framework and concludes this paper.

2. Overview

2.1. Social engineering

Social engineering is an act of manipulating a person to execute an action willingly or unwillingly [8]. As shown in its term, which is social engineering, the act is linked with social science but it is more related to computers and information security personnel. While a variety of definitions of the term social engineering have been suggested, this paper will use the definition suggested by Rouse [9] who saw it as an attack vector that depends greatly on human communication and often includes tricking people into breaching regular security measures. Social engineering attacks do not depend on high-tech equipment to start the attack. On the other hand, it is performed through a skilful attack on the mind of the victim [10]. Furthermore, the purpose of a social engineering attack is also defined as a way to obtain direct access to an organization's data or information system using physical or digital access [11].

Social engineering is known as internal threat that does not compromise or exploit any particular software or systems, thus, making it different from the usual traditional threat made by attackers. The victim of social engineering attack is often scammed into giving out their valuable sensitive information by giving them ideas that they are interacting with a trusted computer system [12]. This method, which is technology-based social engineering, is basically closely related to the traditional hacking technique [13] because an electronic device is present in the attack into getting the desired information. Some of the attack methods used in technical-based social engineering are popup windows, email attachments, online social engineering, phishing, and rogue security software.

2.2. Phishing susceptibility

Phishing susceptibility is known as the likelihood of the user falling prey to the phishing attacks. Phishing involves a process where an attacker attempts to steal sensitive information such as the bank account number, email ID, password for the online accounts and many more from the intended victims. This process is done by impersonating as someone whom the victim would trust so that they would give out the required information easily without any doubt [14]. Phishing attack usually consists of three components; the hook, lure and catch. The hook is known as a tool used by attackers to collect victim's confidential information such as e-mail form, social media site, banking site, company site that are legitimate looking. On the other hand, the lure is the motivation given by attackers to the user to trick the user into giving out their required information. Examples of lure include providing a sense of urgency in the mail, sense of authority in the mail and many more. The catch is known as the information that will be retrieved by attackers, which will be used to start invading the victims' private profile and others [15].

The attack is usually done by sending a masqueraded e-mail, which will look like an e-mail originally generated by legitimate companies, banks, credit card companies or even popular social media sites, which will require the victims to verify any information, which will ensure that users enter their personal credential [14]. A study by Williams et al. [16] found greater susceptibility to phishing threats for emails with the presence of authority cues. Victims will usually fall prey for these kinds of attacks because the messages or the websites sent by attackers will be designed very well that it will look like the actual web site deceive users from identifying that it is actually a faked site. Once the user has entered their personal credential that was required in the page, the attacker will use the information provided to hack into the victims' accounts [17].

3. Understanding Employee's Behaviour towards Phishing Threats

In recent years, understanding employees' behaviours in phishing is an increasingly important area as countermeasure to security threats in organizations. Previous research has indicated that various employees' factors may create a security threat to the organization. Zaki et al. [4] revealed that analysis on employees' behaviour or interest in email communication in an organization would help phishers to categorize the email topics of the employees' interest, thus, increasing the likelihood of phishing susceptibility in the future. The synthesis was done according to big data analysis on e-mail communication of a big organization like Enron. Swart et al. [5] performed a similar series of experiments to examine the vulnerabilities of security solutions deployed in organizational and data centre environments. By understanding employees' interest and behaviour, initial foothold into an organization was obtained by sending individual tailored spear phishing emails to targeted employees [5]. Due to inherent differences among employees, this study focuses on investigating the personality traits that may influence employees' response decision to phishing attack.

Previous research has found that phishing susceptibility in organization varies with employees' demographic variable. The two keys of demographic factors that affect the susceptibility towards phishing attacks are age and gender. For example, Sebescen and Vitak [18] found that younger employees were most vulnerable to phishing threats. The study found that vulnerability increases consistently with the length of employment. This finding is in agreement with Bandi [19] findings, which showed that younger people have lower online security behaviours in comparison to older age groups. On the other hand, some studies found that women are significantly more susceptible to phishing than men. Darwish et al. [20] stated that this could be a result of their more agreeable personality, while Sheng et al. [21] argued that this is due to their lower technical knowledge and experience.

A considerable amount of literature has been published on the relationship of employee's personality with phishing susceptibility. These studies have attempted to explain the association from various theoretical perspectives. For example, Bandi [19] applied Big Five Personalities model to examine the relationship of personalities with related online security behaviour that influence organizational cyber security such as device securement and password generation. The study found that conscientiousness, extraversion, and risk avoidance are significantly associated with online security behaviour. However, as the organization studied is a university and the respondents mostly constitute of young students, the results of

this study might not hold true for other organizations that have more diversified employees. In addition, the study does not show actual effect of personalities towards phishing susceptibility. In contrast, Martin [22] who applied Signal Detection Theory in his study reported no significant relationship between conscientiousness to phishing or spear-phishing email detection. Martin [22], however, argued that an association between conscientiousness and phishing might be attenuated by range restriction.

Undeniably, employees' knowledge and experience play important roles in lowering the risk of phishing susceptibility. Therefore, many organizations stress on the importance of employees' awareness as preventive measures against phishing threats [23, 24]. Campbell [25] indicates that employees view information security training and awareness program to increase participants' technical knowledge and experience as a significant and positive solution to counter phishing threats. According to Halevi et al. [26], lack of technical understanding is a reason that makes a user fall for phishing. A study by Wright and Marett [27] found that experiential factors, which consist of computer self-efficacy, web experience, and security knowledge influence employee's decision to respond to phishers. Similarly, personal or other people's experience may form belief, thus, could be shown in a form of avoidance [28]. For example, a study on a diverse set of organizations located in Sweden [29] revealed that employees' normative beliefs might come from direct personal experience, interaction with others, or from interpersonal or mediated communication [30], which has direct association with intention to resist phishing.

The degree to which, personality and employee's experience are related with phishing susceptibility is a question that has generated interest in this study. Some studies have argued that experience plays a significant role in shaping individual personality [31]. This study suggested that experience might both lead to familiarity and expertise. In the context of phishing, experience may be in the form of general experience and technical experience. It has been shown that numerous studies have indicated a substantial but relatively moderate relation between personality and security threats in organization. However, with regard to the most well established model of personality, the Big Five, none of the studies has empirically shown association between employee's experience and personality and its effect toward phishing susceptibility in a workplace.

In this study, self-monitoring is also included as one of the personality traits that could be studied to determine the users' susceptibility to phishing. Self-monitoring is one of the most frequently examined personalities in organizational setting [32]. An individual with high self-monitoring is known to be able to observe their surrounding and follow the behaviour presented around them with the main purpose of pleasing others. On the other hand, an individual with low self-monitoring will not try to please or impress other people but they tend to stand their ground and behave like who they really are [33].

4. Methodology

4.1. Research model

Tailored to the specific personality traits as discussed in previous works, this study proposes the research model shown in Fig. 1, which is based on Big-Five Personality Model [7]. This study classifies the variables mainly into three broad

categories, namely independent variables (Openness, Conscientiousness, Extroversion, Agreeableness, Neuroticism, Self-monitoring), dependent variable (User behaviour), and modifying factors (General experience, and technical Experience). In the context of this study, user behaviour variable measures employee's secure behaviour that is not susceptible to phishing. The operational definitions of the independent variables used in this study are shown in Table 1. Based on the previous studies, we propose the following hypothesis:

*H*1*:* All personality traits variables are significantly related to user behaviour.
*H*1*a:* Openness is significantly related to phishing susceptibility.
*H*1*b:* Conscientiousness is significantly related to phishing susceptibi*lity.*
*H*1*c:* Extraversion is significantly related to phishing susceptibility.
H1d: Agreeableness is significantly related to phishing susceptibility.
*H*1*e:* Neuroticism is significantly related to phishing susceptibility.
*H*1*f:* Self-monitoring is significantly related to phishing susceptibility.
*H*2*:* General experience is significantly related to all personality traits variables.
*H*3*:* Technical experience is significantly related to all personality traits variables.

Table 1. Conceptual and operational definitions.

Variables	Operational definition
General experiences	User general experiences could be divided into positive and negative experience, in which, both could influence the reason for them to possess a certain personality trait.
Technological experiences	Technological experience could be influenced by the amount, purpose and the knowledge on the usage of the technology. A person that spends more time in technology usage and uses it for multiple purposes would have more experience on how it works. A person that has undergone training will gain knowledge on the technological aspect thus possessing a certain behaviour that could protect them.
Openness	Openness trait makes a person to be more curious, to enjoy learning new things, and to explore new experiences. A person with this trait gives priority to trying and exploring new things regardless of the risks.
Conscientiousness	High-conscientiousness person is well known for their trustworthiness. They are also responsible and make an effort to be precise in everything they do by following the standards and regulations.
Extroversion	Extroverted individuals are known as an individual that likes to be around people and attempts to be interested to attain and provide information to be socially accepted. They are known to be dominant, sociable and energetic in public.
Agreeableness	A person with agreeableness trait is less aggressive and strives for harmony. They tend to trust others easily and like to please others by accepting others saying to avoid an argument.
Neuroticism	High level of neuroticism trait in a person causes a person to go through negative feelings such as being highly insecure and highly worried about the possible failures or risks. Due to their focus on negative events and anxiety causing them to be bothered and worried about privacy.
Self-monitoring	High level of self-monitoring enables a person to adapt to a certain social situation and behave according to the situation they are involved in.

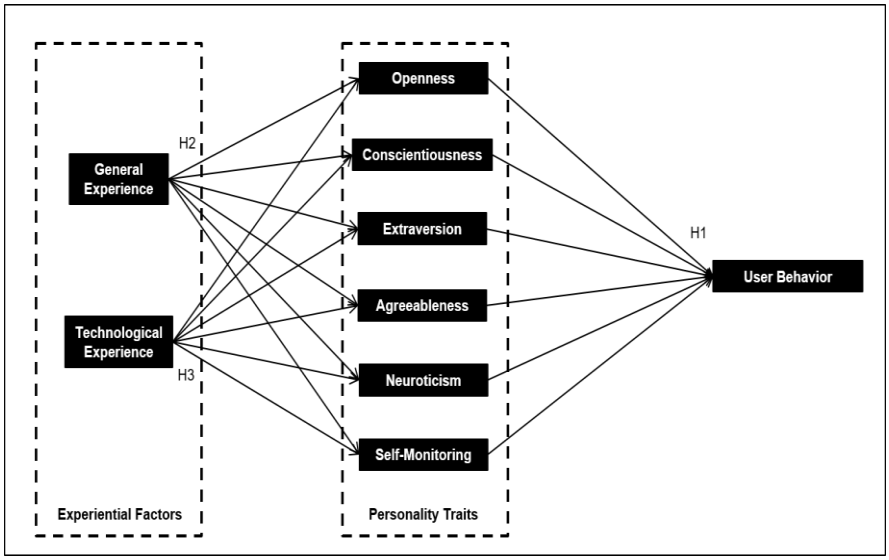

Fig. 1. Phishing susceptibility framework (adapted) [15, 34].

4.2. Instrument design

In this study, structured questionnaire was used for data collection. O'Brien and Toms [35] adapted a questionnaire construction involved a few stages. The questionnaire was divided into four parts namely Sections A, B, C and D. Section A was to collect the demographic profile of the respondent and the data collected were nominal data. Section B was carried out to determine general experience and technological experience faced by the respondents in their life. Furthermore, Section C was carried out to identify the personality trait possessed by a user and Section D was to identify the user behaviour carried out by the user, which makes them to subject to phishing attack. Sections B and D were measured through ordinal data and Section C used the continuous data. Items in Part C were adapted from Big Five Personality scale [7], whereas other items were self-developed from critical review of literature in social engineering.

Content validity was carried out to verify the suitability of the research questions. It is also to verify the language used and investigate any biases. A total of three experts were chosen for the content validation purpose based on their expertise in the field of information security with a minimum experience of 5 years. All the comments were taken into consideration and some changes and corrections were made to the questionnaire to ensure that the questionnaire is more effective and clear. The questionnaire is made bilingual (English and Malay), to ensure that those who are poor in English or finding it difficult to understand the sentence in English could refer to the Malay version. The process of translating the questionnaire into the Malay language was done using a forward-backward translation procedure [36].

A pilot study was carried out after the research instrument was validated by experts. Fifty respondents were chosen, as in this case the number of items for each variable was 10. The selected participants were easily contacted and reached for any feedback purpose. The purpose of a pilot study was to determine whether the questions worded would achieve the desired results. It is also to identify whether the

questions are understood by all classes of target respondents and if any questions should be rephrased, added or eliminated. IBM SPSS 20 software was used to calculate the Kaiser-Meyer-Olkin (KMO) value and Cronbach Alpha value for each variable and set of items in that variable. Pilot study was conducted for 4 weeks. After a complete revision, the modified research instrument was checked by an expert.

4.3. Instrument design

In this study, structured questionnaire was used for data collection. O'Brien and Toms [35] adapted a questionnaire construction involved a few stages. The questionnaire was divided into four parts namely Sections A, B, C and D. Section A was to collect the demographic profile of the respondent and the data collected were nominal data. Section B was carried out to determine general experience and technological experience faced by the respondents in their life. Furthermore, Section C was carried out to identify the personality trait possessed by a user and Section D was to identify the user behaviour carried out by the user, which makes them to subject to phishing attack. Section B and D were measured through ordinal data and Section C used the continuous data. Items in Part C were adapted from Big Five Personality scale [7], whereas other items were self-developed from critical review of literature in social engineering.

Content validity was carried out to verify the suitability of the research questions. It is also to verify the language used and investigate any biases. A total of three experts were chosen for the content validation purpose based on their expertise in the field of information security with a minimum experience of 5 years. All the comments were taken into consideration and some changes and corrections were made to the questionnaire to ensure that the questionnaire is more effective and clear. The questionnaire is made bilingual (English and Malay), to ensure that those who are poor in English or finding it difficult to understand the sentence in English could refer to the Malay version. The process of translating the questionnaire into the Malay language was done using a forward-backward translation procedure [36].

A pilot study was carried out after the research instrument was validated by experts. Fifty respondents were chosen, as in this case the number of items for each variable was 10. The selected participants were easily contacted and reached for any feedback purpose. The purpose of a pilot study was to determine whether the questions worded would achieve the desired results. It is also to identify whether all classes of target respondents understand the questions and if any questions should be rephrased, added or eliminated. IBM SPSS 20 software was used to calculate the Kaiser-Meyer-Olkin (KMO) value and Cronbach Alpha value for each variable and set of items in that variable. Pilot study was conducted for 4 weeks. After a complete revision, an expert checked the modified research instrument.

5. Results and Discussion

5.1. Reliability analysis

The Cronbach's Alpha value for each factor must be higher than its threshold, which was 0.7, hence, indicating that the items (questions provided in the questionnaire) represent the same general factor. Table 2 shows the results of the reliability analysis before and after revision is made. In the beginning, it can be seen that only technological experience, neuroticism, self-monitoring and user

behaviour had the Cronbach alpha value above the threshold, which was 0.07. Other variables showed lower Cronbach alpha value, thus, some items from the variables were deleted and the reliability analysis was carried out again to ensure that all variables had a Cronbach Alpha value of 0.7 and higher.

After removing a few items from the variables with Cronbach Alpha lower than 0.7, all variables had an acceptable value of Cronbach Alpha value. The Cronbach's Alpha value for each factor respectively was General experiences (0.862), Technological experiences (0.925), Openness (0.829), Conscientiousness (0.737), Extroversion (0.893), Agreeableness (0.799), Neuroticism (0.773), Self-monitoring (0.808) and User behaviour (0.888). After the final revision during reliability analysis, a total of 33 items in the questionnaire were selected for further analysis.

Table 2. Results of reliability analysis before of after revision.

Variable	Before revision		After revision	
	Cronbach alpha	**No. of items**	**Cronbach alpha**	**No. of items**
General experiences	0.551	5	0.862	3
Technological experiences	0.903	5	0.925	3
Extroversion	0.574	5	0.893	4
Agreeableness	0.580	5	0.799	3
Conscientiousness	0.484	5	0.737	3
Neuroticism	0.719	5	0.773	4
Openness	0.614	5	0.829	3
Self-monitoring	0.808	5	0.808	5
User behaviour	0.888	5	0.888	5

5.2. Descriptive analysis

Table 3 shows the number of respondents, the mean and the standard deviation of the data collected. The number of respondents from the IT Department and Non-IT Department were equally divided into 126 respondents from each working department. The mean comparison between the working department and the variables studied in this study are also shown in the table. According to the data shown in the table, respondents working in the IT Department had a higher level of general and technological experience compared with respondents working in Non-IT Department.

As for the personality trait variables, respondents working in IT Department only possessed higher mean in the conscientiousness trait indicating that they obey the rules and procedures given to them while the respondents working in Non-IT Department possessed higher mean in the remaining traits, which were extroversion, agreeableness, neuroticism, openness and self-monitoring.

Furthermore, for the phishing susceptibility that measured, which group possessed user behaviour that was not susceptible to phishing, it could be seen that respondents working in IT Department possessed a higher mean in that variable. Hence, respondents working in IT Department were less susceptible to phishing attack compared to respondents working in Non-IT Department with a mean difference of 1.3254.

Table 3. Descriptive statistics.

Variable	Information Technology (IT) Department (*N* = 126)		Non-Information Technology (IT) Department (*N* = 126)	
	Mean	**SD**	**Mean**	**SD**
General experiences	3.0873	.77995	2.0397	.85230
Technological experiences	4.1032	.70233	2.7937	1.14065
Extroversion	2.5397	1.19767	3.1429	1.07862
Agreeableness	2.9524	1.07225	3.6190	.94536
Conscientiousness	3.2063	1.03782	3.1905	1.15040
Neuroticism	2.2857	.94536	2.4921	.85553
Openness	3.0952	.83358	3.2143	.79606
Self-monitoring	3.1270	.95485	3.4921	.98587
User behaviour	3.8413	.51245	2.5159	1.00187

5.3. Correlation analysis

An association between variables was based on the Pearson Correlation analysis. In this case, only the significant level of 0.01 was taken into consideration, as most associations were moderate, hence, a high statistically significant correlation value was chosen.

To address research question 1, the correlation coefficient was determined in Table 4 among the personality traits (independent variables), and phishing susceptibility (dependent variables). In the context of this study, the phishing susceptibility variable measures employee's behaviour that is not susceptible to phishing. Conscientiousness traits were positively significant with phishing susceptibility, therefore, *H*1*b* was accepted.

On the contrary, extroversion traits had a strong negative correlation with phishing susceptibility. The relation between agreeableness and self-monitoring traits with phishing susceptibility were also negatively significant, but moderate. Openness and neuroticism variables produce non-significant results. Therefore, *H*1*a* and *H*1*e* are rejected.

To address research question 2, correlations were determined between the experience variables and personality traits. General experience and technical experience were significantly associated (rs =0.705, p <0.01).

For an association between general experience with personality traits, several correlations were negatively significant and range from moderate to weak (in descending order: self-monitoring, extroversion, and agreeableness).

Notably, conscientiousness yielded the sole positive significant correlation with general experience. Similarly, conscientiousness, self-monitoring, extroversion, and agreeableness were negatively significant with technical experience. Openness and neuroticism were not significantly related to any of the employees' experience variables.

Table 4. Pearson correlation.

	General experience	Technical experience	Openness	Conscientiousness
General experiences	1	-	-	-
Technological experiences	0.705**	1	-	-
Openness	0.010	0.057	1	-
Conscientiousness	0.236**	-0.487**	-0.142*	1
Extroversion	-0.422**	-0.553**	-	0.223**
Agreeableness	-0.481**	-0.407**	-	-
Neuroticism	-0.069	-0.179	-0.141*	0.505**
Self-monitoring	-0.208**	-0.347**	-	-
User Behavior	-	-	0.010	0.306**

**Correlation is significant at the 0.01 level (2-tailed).
*Correlation is significant at the 0.05 level (2-tailed).

Table 4. Pearson correlation (continuation).

	Extroversion	Agreeableness	Neuroticism	Self-monitoring
General experiences	-	-	-	-
Technological experiences	-	-	-	-
Openness	-	-	-	-
Conscientiousness	-	-	-	-
Extroversion	1	-	-	-
Agreeableness	0.658**	1	-	-
Neuroticism	-0.166**	-	1	
Self-monitoring	-	-	-	1
User behaviour	-0.533**	-0.400**	-0.142*	0.414**

**Correlation is significant at the 0.01 level (2-tailed).
*Correlation is significant at the 0.05 level (2-tailed).

5.4. Structural equation modelling

To establish a valid model, structural model was evaluated using Structural Equation Modelling. The Amos software computed a number of goodness-of-fit indices but only certain values were taken into account such as the Goodness of Fit Indices (GFI), Tucker- Lewis Index (TLI), Normed Fit Index (NFI), Comparative Fit Index (CFI) and Root Mean Square (RMR). According to Hu and Bentler [37], the acceptable model fit that is indicated for the CFI value was 0.90 or greater. On the other hand, other model fits such as GFI, TLI, NFI and CFI should have at least the value of 0.90 to be accepted as a fit model but a good model should have at least 0.95 and greater [38].

Based on five common fit statistics, the evaluated model shown in Table 5 and Fig. 2, reveals sufficient goodness of fit, in which, extroversion, agreeableness, conscientiousness, and self-monitoring variables had significant negative effects on phishing susceptibility, supporting *H*1*b*, *H*1*c*, *H*1*d*, and *H*1*f*.

Table 5. Model fit indices.

Model	*x*2/*df*	GFI	CFI	TLI	NFI	RMR
Accepted value	<=5	>0.95	>0.95	>0.95	>0.95	<0.05
Framework value	2.511	0.965	0.971	0.968	0.961	0.041

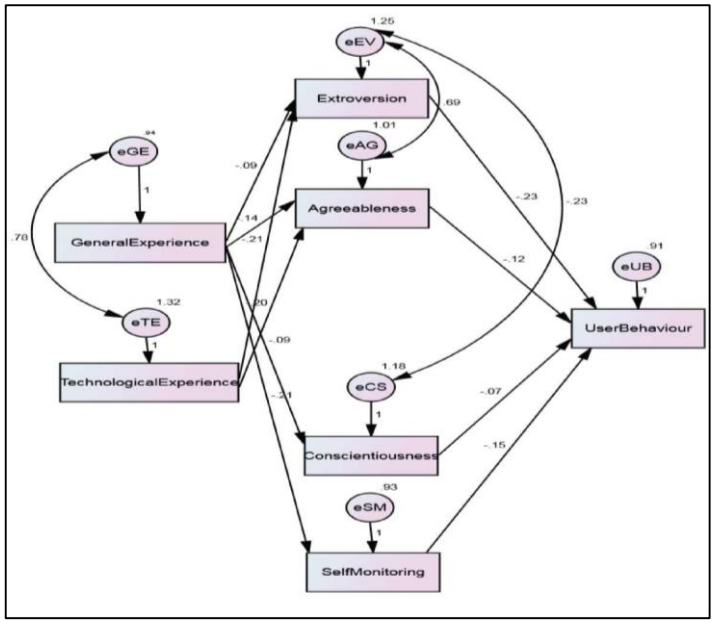

Fig. 2. Phishing susceptibility framework.

Table 6 shows the regression weight obtained during the SEM analysis of the phishing susceptibility framework. The table shows all the direct and indirect relationship of the variables in the study. Table 6 consists of the Estimate value, which is the regression value between the variables, S.E., which stands for Standard Error and C.R., which is Critical Ratio. The P-value shows the significance between the variables and if it consists of three asterisk symbols, it represents that the relationship between the variables is very significant.

Table 6. Regression output.

		Estimate value	Standard error	Critical ratio	P-value
Exroversion	General experience	-.0.95	.102	-3.927	***
Agreeables	General experience	-.140	.092	-3.512	***
Conscientiousness	General experience	-.090	.071	-1.265	.008
Self-monitoring	General experience	-.212	-.063	-3.373	***
Extroversion	Technologial experience	-.209	.085	-2.450	.014
Agreeableness	Technologial experience	-.201	.078	-2.580	.010
User behaviour	Extroversion	-.235	.070	-3.355	***
User behaviour	Agreeableness	-.121	.076	-1.604	.014
User behaviour	Conscientiousness	-.067	.057	-1.172	.043
User behaviour	Self-monitoring	-.150	.061	-2.444	.015

Based on the results in Table 6, it could be seen that all the values are significant. Based on the estimate value obtained during the SEM analysis, the regression equation that was obtained during multiple regression analysis could be verified because all the estimates were the same as the value obtained previously.

$$UserBehavior = 1.228 - 0.235E - 0.150S - 0.121A - 0.067C$$

where: E = Extroversion, A = Agreeableness, C = Conscientiousness, S = Self-Monitoring.

To summarize, four of the six hypothesized personality traits had a significant influence on the employees' likelihood to respond to the phishing scam in the workplace. According to the regression equation, the output data shows that the correspondence between the independent and dependent variables is going in the negative direction; that is, the lower is the personality traits, the more secure employee behaviour towards phishing threats. Results of these regressions suggest that there is an inverse influence of personality traits (independent variables) towards secure user behaviour (dependent variable). Specifically, regression coefficient for personality traits predicting secure user behaviour for Extroversion (*E*), Self-monitoring (*S*), Agreeableness (*A*), and Conscientiousness (*C*), are -0.235 (standard error= 0.070), -0.150 (standards error = 0.061), -0.121 (standard error = 0.076), and -0.067 (standard error = 0.057). The regression output is statistically significant with all p values being less than 0.05.

From the regression function, it can be seen that there are discrepancies between the positive correlation results and the negative regression coefficient for self-monitoring and conscientiousness variables. As the multiple regression analysis tend to minimize variation in the dependent variable, there is a possibility of the presence of multicollinearity, where one of the personality traits are accounted for the negative regression coefficient. This suggests mediated relationships for the independent variables.

6. Discussion

This study was carried out to test the influence of employee's personality traits on secure user behaviour towards phishing attack in the workplace. This study focuses more on phishing susceptibility because phishing attacks have become very sophisticated to the extent of no organization or person could detect that they are being attacked until later. Even though today organizations have stringent security policies, procedures and carry out frequent security assessment, but they focus more on the tangible vulnerabilities such as in software and also network infrastructures. It fails to give information about the organization or the employees' susceptibility to phishing attacks [39]. Thus, this study is able to produce insight and provide guidelines to organizations in what personality traits in a user that makes them susceptible to phishing and does experience influence their personality traits towards phishing susceptibility.

Based on the descriptive analysis findings, it could be seen that respondents working in Information Technology (IT) Department possessed a higher level of general and Technological Experience compared to respondents working in Non-Information Technology (IT) Department. Besides that, respondents working in Non-Information Department possessed higher level on most of the personality traits that could make them more susceptible to phishing attacks such as extroversion, agreeableness, neuroticism, openness and self-monitoring. As a result, it could be seen that respondents working in Information Technology (IT) Department demonstrate better behaviour towards phishing attacks compared to respondents working in Non-Information Technology (IT) Department.

Based on the findings in the correlation analysis, extroversion had the highest effect on user behaviour that was not susceptible to phishing. The findings observed in this study mirror those of the previous studies that have examined the effect of Extroversion as a trait that makes a user with higher risk to fall prey for a phishing attack [20, 40]. A less sociable and recluse employee showed low level of extroversion, and would restrain themselves from sharing sensitive information such as their password [41]. On the contrary, an employee with high level of extroversion traits would want to be accepted by other employees in their workplace, thus causing them to give out important information. A possible explanation for this might be that extroversion is related to high affective commitment, and employee with a strong commitment is very much involved and enjoyed being a part of their organization [42, 43].

As previously mentioned, this study attempt to incorporate self-monitoring trait, which is one of the most frequently examined personality traits in organizational setting. Contrary to expectations, this study did not find a significant correlation between self-monitoring with other personality trait. This could be due to the lower extroversion trait value throughout the current study, thus, the self-monitoring trait has not been able to come through the respondents. The findings of the current study differ with those of Schleicher et al. [44] who found that self-monitoring is highly correlated to extroversion trait. This discrepancy could be attributed to the respondents working environment, which has a stringent security policies and procedures that cause the respondents to possess low self-monitoring trait. Individual that has low self-monitoring trait tries hard to be authentic and follows a set of core principles and thinking [33].

This study has been unable to demonstrate the relationship of openness personality traits towards user behaviour that is not susceptible to phishing. Previous research by Alseadoon et al. [45] does not support the current study. This rather contradictory result may be due to different methods and type of respondents used in the study. Openness trait effect towards phishing susceptibility had been experimented in a real setting where an email was sent to the respondents to ascertain their response and the study was carried out among undergraduate students in Saudi Arabia [45] while the current study used survey method only and focused more on respondents working in an organization. Thus, the openness trait in the respondents could not be captured clearly, because they were not intellectually stimulated [40]. In addition, the respondents of the study consist of undergraduate students between 18 to 25 years old that made them more susceptible to phishing due to lack of experience and training [21] compared to the respondents in this current study that were already working and much older.

The modifying factors, which consist of general experience and technological experience, are taken into consideration due to their relationship in the previous studies. Further assessments during the regression analysis showed that technical experience only influenced extroversion and agreeableness traits in comparison with general experience that influenced extroversion, self-monitoring, agreeableness and conscientiousness. A possible explanation for this might be that technical experience involves knowledge on the usage of the security technology. The results indicate that employees who are highly knowledgeable are more opinionated and willing to share their knowledge with others, indicating their altruistic nature [46]. The absence of technical experience influence towards Self-monitoring and conscientiousness may be due to the fact that all respondents consists of employees who are working in IT related companies, which already have stringent security practices and policies.

7. Contribution

In general, the study is essentially important to provide empirical assessment on the influence of personality traits towards phishing susceptibility in a workplace. While the concept in the big-five personality model was empirically validated in different domains, it is not evident in organizational setting; hence, there has been a contribution to knowledge in this area. Combining self-monitoring personality variables with the existing model will provide greater insights on how personality traits affect phishing susceptibility in a workplace. In addition, this study is the first attempt to show how employees' experience is related to their personality and consequently their decision outcomes, thus, revealing the nature of phishing victims.

The proposed framework has the potential to be developed into a full conceptual framework for personality traits toward phishing susceptibility in organizational setting. Knowledge of these constructs is useful for research attempting to shift research on phishing towards human factors aspects. This study provides insights on which, personality trait in an individual could make them susceptible towards phishing attacks and it provides guidelines for organization to design security policies that could cater all personality types that exist in their organizations.

8. Conclusions

The present study was designed to determine the most common employees' personality traits that affect their likelihood to respond to the phishing scam in the the workplace. This study concludes that extroversion personality has the strongest influence towards phishing susceptibility, followed by self-monitoring, agreeableness and conscientiousness. It was also shown the importance of employees' experience in shaping employees' personality to resist phishing attack. Future studies could seek to expand the present study by examining different types of organization, investigating the influence of organization culture and practices on employees' personality in resisting phishing attack.

There are limitations in this study in three aspects. First, this study is conducted in IT-related companies only. Therefore, one can argue that the context of this study has introduced bias as it has been conducted in IT-related setting and thus any generalizability to other research settings is limited. Testing the conceptual framework in other research settings may provide different results. Second, this study does not apply phishing simulation to see the pattern on phishing response among employees. Third, the presence of multicollinearity in the SEM regression analysis requires further analysis to study mediated relationships between the independent variables.

Acknowledgement

The authors would like to thank our research instrument reviewers; Radzi Motsidi, Robiah Yusof, and Erman Hamid for their insightful comments. This paper is funded by the Global Commission on the Stability of Cyberspace (GCSC) Grant (GLUAR/HGCC/2018/FTMK-CACT/A00015). A high appreciation to Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka (UTeM) for facilitating the work done in this paper.

References

1. KnowBe4. (2016). The phishing breakthrough point. Retrieved January 16, 2017, from https://www.digitree.it/wp-content/download/KnowBe4_Phishing-Breakthrough-Point_EN.pdf.
2. PhishMe. (2016). Enterprise phishing susceptibility and resiliency report. Retrieved January 16, 2017, from https://www.infosecurityeurope.com/__novadocuments/351537?v=636276130024130000.
3. Caldwell, T. (2013). Spear-phishing: How to spot and mitigate the menace. *Computer Fraud and Security*, 2013(1), 11-16.
4. Zaki, T.; Uddin, M.S.; Hasan, M.M.; and Islam, M.N. (2017). Security threats for big data: A study on Enron e-mail dataset. *Proceedings of the 5th International Conference on Research and Innovation in Information Systems (ICRIIS).* Langkawi, Malaysia, 1-6.
5. Swart, I.; Irwin, B.; and Grobler, M. (2015). Data centre vulnerabilities: Physical, logical and trusted entity security. *Proceedings of the Conference on Southern Africa Telecommunication Networks and Applications* (SATNAC), Western Cape, South Africa, 6 pages.
6. Wang, J.; Herath, T.; Chen, R.; Vishwanath, A.; and Rao, H.R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, 55(4), 345-362.
7. Costa Jr., P.T.; and McCrae, R.R. (1992). *Revised NEO personality inventory (NEO-PI-R) and NEP five-factor inventory (NEO-FFI).* Odessa, Florida, United States of America: Psychological Assessment Resources.
8. Hadnagy, C. (2010). *Social engineering: The art of human hacking*. Indianapolis, Indiana, United States of America: Wiley Publications Inc.
9. Rouse, M. (2016). *Definition Social Engineering*. Retrieved January 16, 2017, from http://searchsecurity.techtarget.com/definition/social-engineering.
10. Long, J. (2011). *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing*. Burlington, New Jersey, United States of America: Syngress Publishing, Inc.
11. Foozy, C.F.M.; Ahmad, B.R.; Abdollah, C.M.F.; Yusof, D.R.; and Mas'ud, E.M.Z. (2011). Generic taxonomy of social engineering attack. *Proceedings of the Malaysian Technical Universities International Conference on Engineering and Technology (MUiCET).* Batu Pahat, Johor, Malaysia, 1-7.
12. Gulati, R. (2003). The threat of social engineering and your defense against it. *SANS Institute Information Security Reading Room*.
13. Janczewski, L.J.; and Fu, L. (2010). Social engineering-based attacks: Model and New Zealand perspective. *Proceedings of the International Multiconference on Computer Science and Information Technology* (IMCSIT). Wisla, Poland, 847-853.
14. Jagatic, T.N.; Johnson, N.A.; Jakobsson, M.; and Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10), 94-100.
15. Parrish Jr., J.L.; Bailey, J.L.; and Courtney, J.F. (2009). A personality based model for determining susceptibility to phishing attacks. *Little Rock: University of Arkansas*, 285-296.

16. Williams, E.J.; Hinds, J.; and Joinson, A.N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 120, 1-13.
17. Yeboah-Boateng, E.O.; and Amanor, P.M. (2014). Phishing, SMiShing and Vishing: An assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, 5(4), 297-307.
18. Sebescen, N.; and Vitak, J. (2017). Securing the human: Employee security vulnerability risk in organizational settings. *Journal of the Association for Information Science and Technology*, 68(9), 2237-2247.
19. Bandi, S. (2016). *An empirical assessment of user online security behavior: Evidence from a university*. Master Thesis. University of Maryland, College Park, United States of America.
20. Darwish, A.; El Zarka, A.; and Aloul, F. (2012). Towards understanding phishing victims' profile. *Proceedings of International Conference on Computer Systems and Industrial Informatics* (ICCSII*)*. Sharjah, United Arab Emirates, 1-5.
21. Sheng, S.; Holbrook, M.; Kumaraguru, P.; Cranor, L.F.; and Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Atlanta, Georgia, United States of America*, 373-382.
22. Martin, J. (2017). *Something looks phishy here: Applications of signal detection theory to cyber-security behaviors in he workplace*. Master Thesis. University of South Florida, Tampa, United States of America
23. Henningsen, E.K. (2013). *The defense and popularity of social engineering in Norway*. Master Thesis. Department of Computer Science and Media Technology, Gjøvik University College, Norway.
24. Korpela, K. (2015). Improving cyber security awareness and training programs with data analytics. *Information Security Journal: A Global Perspective*, 24(1-3), 72-77.
25. Campbell, C.C. (2017). *Exploring future solutions to counter social engineering attacks: A delphi study*. Doctoral Dissertation. University of Phoenix, United States of America.
26. Halevi, T.; Lewis, J.; and Memon, N. (2013). Phishing, personality traits and facebook, *arXiv preprint arXiv:1301.7643*.
27. Wright, R.T.; and Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, 27(1), 273-303.
28. Corcoran, N. (Ed.). (2013). *Communicating health: Strategies for health promotion (2nd ed.)*. London, United Kingdom: SAGE Publication
29. Flores, W.R.; and Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers and Security*, 59, 26-44.
30. Fishbein, M.; and Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Boston, United States of America: Addison-Wesley.
31. Rammstedt, B.; Danner, D.; and Martin, S. (2016). The association between personality and cognitive ability: Going beyond simple effects. *Journal of Research in Personality*, 62, 39-44.

32. Day, D.V.; Shleicher, D.J.; Unckless, A.L.; and Hiller, N.J. (2002). Self-monitoring personality at work: A meta-analytic investigation of construct validity. *Journal of Applied Psychology*, 87(2), 390-401.
33. Barrick, M.R.; Parks, L.; and Mount, M.K. (2005). Self-monitoring as a moderator of the relationships between personality traits and performance. *Personnel Psychology*, 58(3), 745-767.
34. Tobin, B. (2014). *Disclosing personal information online; links between extraversion, neuroticism, self-monitoring, narcissism and online privacy awareness.* Dublin, , Ireland: Dublin Business School.
35. O'Brien, H.L.; and Toms, E.G. (2010). The development and evaluation of a survey to measure user engagement. *Journal of the American Society for Information Science and Technology*, 61(1), 50-69.
36. Pan, Y.; and Puente, M.d.l. (2005). Census bureau guideline for the translation of data collection instruments and supporting materials: Documentation on how the guideline was developed. *Survey Methodology*, 6.
37. Hu, L.-t.; and Bentler, P.M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, 6(1), 1-55.
38. Hox, J.J. (2007). An introduction to structural equation modeling. *Family Science Review*, 11, 354-373.
39. Moore, J. (2013, August 8). *Phishing attacks: Measuring your susceptibility*. Retrieved January 16, 2017, from https://www.mwrinfosecurity. com/our-thinking/phishing-attacks-measuring-your-susceptibility/.
40. Uebelacker, S.; and Quiel, S. (2014). The social engineering personality framework. *Proceedings of Workshop on Socio-Technical Aspects in Security and Trust (STAST).* Vienna, Austria, 24-30.
41. Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, 59(4), 662-674.
42. Allen, N.J.; and Meyer, J.P. (1990). Organizational socialization tactics: A longitudinal analysis of links to newcomers' commitment and role orientation. *Academy of Management Journal*, 33(4), 847-858.
43. Shore, L.M.; and Wayne, S.J. (1993). Commitment and employee behavior: Comparison of affective commitment and continuance commitment with perceived organizational support. *Journal of Applied Psychology*, 78(5), 774-780.
44. Schleicher, D.J.; Day, D.V.; Mayes, B.T.; and Riggio, R.E. (2002). A new frame for frame-of-reference training: Enhancing the construct validity of assessment centers. *Journal of Applied Psychology*, 87(4), 735-746.
45. Alseadoon, I.; Chan, T.; Foo, E.; and Nieto, J.G. (2012). Who is more susceptible to phishing emails?: A Saudi Arabian study. *Proceedings of the 23rd Australasian Conference on Information Systems* (ACIS). Geelong, Melbourne, Australia, 1-11.
46. Gupta, B. (2008). Role of personality in knowledge sharing and knowledge acquisition behavior. *Journal of the Indian Academy of Applied Psychology*, 34(1), 143-149.