Study of Student Personality Trait on Spear-Phishing Susceptibility Behavior

Mohamad Alhaddad[1], Masnizah Mohd[2], Faizan Qamar[3], Mohsin Imam[4]
Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, 43600, Malaysia [1, 2, 3]
Department of Computer Science, ARSDC, University of Delhi, New Delhi, 110021, India[4]

***Abstract*—Spear-phishing emails are an effective cyber-attack method due to the fact that the emails sent are highly personalized to look like a regular legitimate email. Recently, it was discovered that personality traits of the victim have an impact on a person's susceptibility to spear-phishing. This study aims to identify which personality traits affect spear-phishing susceptibility besides other traits such as Information Technology background, gender, and age. In addition, measure of the effectiveness of embedded training systems and see whether message framing can further help increase its effectiveness. A personality trait survey was sent to 100 participants, followed by a real-life spear-phishing simulation to measure a certain personality trait's influence on phishing susceptibility. After a two-week period, the second round of spear-phishing emails was sent again to measure message framing effectiveness. The personality traits analysis results show that users with higher levels of Internet anxiety are less susceptible to spear-phishing emails. While the message framing did not show any significant results, the embedded training program reduced the click rate. Findings revealed that certain people are more susceptible to spear-phishing emails than others. Thus, this work can guide an institution or organizations to identify which group of people are more vulnerable to spear-phishing.**

***Keywords*—Spear-phishing; cyber-attack; personality; trait; embedded training; message framing**

I. Introduction

Phishing attacks have been around for a while now, the first time the word phishing was recorded was in 1996; it was a hacking tool called AOHell [1]. This tool was used to send spam emails pretending to be AOL (America Online service provider) to trick users into giving private and sensitive information. Phishing attacks are usually sent in large volumes, contain malicious links or software, and are non-personalized generic emails. Contrarily, spear-phishing emails are delivered to a much smaller number of recipients, may or may not have malicious links or attachments (zero payloads), are highly tailored, and are specifically designed to deceive the user.

Spear-phishing email was the most popular method of attack, according to Symantec Internet Security Threat Report 2019 [2], with 65% of known groups using spear-phishing as a primary attack vector. It was also reported that 95% of the group's motivation for such an attack was information gathering [2]. Furthermore, the Anti-Phishing Working Group [3] has reported 46,036 phishing websites and 44,497 unique phishing campaigns were conducted in June 2020.

An American security company 'ProofPoint' stated that 88% of organizations had faced spear-phishing attacks in 2019, and 55% of organizations have fallen victim to a successful attack at least once in 2019 [4]. Meanwhile, Verizon stated that 22% of breaches involved phishing [5]. With such alarming numbers and click rate, it is important to explore how well an organization is prepared for a phishing attack and the factors involved.

One of the newer factors that have been shed light on is personality traits. Spear-phishing campaigns target people with similar interests, so personality traits can hold the answer on what makes some people click more than others. Previous studies focused on the Big Five personality traits (Extraversion, Agreeableness, Conscientiousness, Neuroticism, and Openness) [6]. Such studies implement various methodologies such as real-life phishing experiments, in lab simulations, and one-on-one interviews to measure the influence on phishing susceptibility [6–9]. Those personality traits describe essential traits that serve as basic building blocks for individual personality; however, other personality traits can influence spear-phishing susceptibility and are a subset of the Big Five traits.

Understanding who is more susceptible to spear-phishing can be used to make a more targeted training program to increase training efficiency. Multiple researchers have focused on embedded training effectiveness, where the training material is embedded in the simulated spear-phishing emails [10, 11]. This method is also referred to as "slap on the wrist" where the user gets "slapped" when he clicks on a phishing link. Message framing may also influence how effectively user understands instruction, according to certain studies. For instance, a message that emphasizes the advantages of doing something, as opposed to one that does not, may be more effectively received. [12, 13].

In this study, the methodology used by two different researches [12, 14] are followed to measure the effect of personality traits in spear-phishing susceptibility and the effect of message framing in an embedded training. In Moody et al. [14], several personality traits and factors that can affect a person's susceptibility to phishing attacks were identified. This research also implements a training program to measure the effectiveness of message framing in an embedded training following the work of Burns et al. [12].

Thus, the contributions of this study are:

- A smaller subset of traits to have a better-focused vision and results (need to add numbers and mention discarded traits).
- Data were collected through an online survey; however, the instruments used are modified to better fit the population (modification criteria is to be added).
- Majority of the technical terms were modified so students are able to relate to it.
- The instruments used in this experiment were modified to use simpler terms, as well as offered translation to support two languages.
- The instruments used were modified to comply with the population tradition, as some of the questions may be offensive or inappropriate.

New training material that is comic-based was used to retain user's attention longer and convey the information more efficiently.

Spear-phishing emails were sent based on the emails provided. The click rate was observed before and after the embedded training to find any improvement (reduction in click rate) depending on the training material. The personality traits survey was used to analyze the relationship between different traits and spear-phishing susceptibility. Results show that certain personality traits influence spear-phishing susceptibility and can be used as a predictor of who is more susceptible to attacks. The training program also shows a reduction in click rate using embedded training; however, no evidence supports that message framing can increase efficiency.

A smaller selection of qualities is used to have a more narrowly focused vision and outcomes. An online survey been used to gather the data, and the instruments are adjusted to better fit the group. Additionally, most of the technical phrases were changed to make them more relatable to students as respondents. The tools used in this experiment were altered to utilize clearer terminology and to provide translation assistance for two languages. Additionally, the methods utilized were changed to conform to population tradition.

This paper is divided into eight main sections. Section II reviews the literature that includes an introduction to spear-phishing and research questions that explore existing work. Followed by hypothesis in Section III, Section IV discusses the methodology. The results given in Section V are split into two parts, the first part is related to personality traits, and the second part is related to the training materials. The discussion of the results is presented in Section VI and conclusion in Section VII. Finally, there is discussion of future work in Section VIII.

II. Literature Review

Phishing attacks are one of the most widespread cyber-attacks, with spear-phishing being a more targeted version with a much higher devastating effect [32, 33]. The Anti-Phishing Working Group (APWG) has been documenting the increase in phishing attacks as early as 2004; their latest quarterly report shows the increasing trend in phishing attacks [3]. Phishing attacks are generally sent to a large volume of people with a generic and non-personalized topic.

Spear-phishing, on the other hand, is crafted carefully and is tailored to a small group of people; thus, they usually have a much higher success rate compared to phishing, as well as having a lower cost and higher return. A spear-phishing campaign with 1,000 messages sent will result in $160,000, compared to a mass phishing campaign with 1,000,000 messages and revenue of $16,000 only [13]. Understanding the factors that affect spear-phishing is an important step in reducing the success rate of such an attack. Personality traits, which reflect a person's behaviors, thoughts and characteristics can help identify who is more susceptible to spear-phishing [18]. IT background is among the other factors that can have an impact on a person's susceptibility to spear-phishing. Lastly, the framing of the training material can also impact the way the user perceives the training, and thus may increase learning efficiency.

A. Personality Traits affect Spear-Phishing Susceptibility

One of the newer factors is the personality traits of the victims. Understanding which personality traits make you more or less susceptible to spear-phishing attacks can help researchers and organizations better understand future attacks and help them come up with anti-phishing programs to help protect people from phishing attacks. Furthermore, the human link is usually the weakest link in any security chain, thus reinforcing the weakest link can tremendously help in reducing cyber-attacks. That is why understanding personality traits that make a human more susceptible to spear-phishing attacks, can help organizations to identify which department or group of people are at high risk of being phished [21].

Moody et al. [14] have conducted a study to better understand which personality traits affect spear-phishing. The sample size was 632 undergraduate students from Information systems and psychology majors. The participants were asked to complete an online survey to measure their personality traits. The personality traits survey was based on multiple published and well-cited psychology papers to measure different personality traits. The survey asked participants to enter their email so that the second phase of the research can begin, the phishing phase; however, the experiment's true nature was not revealed to the participants at this stage. Several personality traits had a significant effect on the susceptibility of spear-phishing attacks. General internet usage showed a positive relation with phishing susceptibility, which is the opposite of expectation. Internet anxiety also showed unexpected results, where higher Internet anxiety decreased the person's exposure to phishing attacks. Curiosity had a significant effect on susceptibility as well as risk propensity.

A study was conducted in a Malaysian company [6] to study the effect of personality traits on the likelihood of being phished. Total 252 responses were collected from the IT and non-IT departments (126 each). The survey had four sections, a demographic questionnaire, general experience, personality quiz, and user behavior (phishing attack). The results of the study showed that conscientiousness was positively correlated to phishing susceptibility, while extroversion was negatively

correlated. However, no relation was found between linking openness and neuroticism to susceptibility.

A lab-based experiment was conducted in an Australian university [7]; it included 121 undergraduate and postgraduate students from finance, business and accounting departments. The experiment had a series of emails shown to the participants. They were asked to judge the safety of the email on a scale from 1 to 5. Information security awareness was linked with identifying phishing and spear-phishing emails. Similarly, people from countries with a high level of Individualism (national culture) were better at detecting phishing and spear-phishing emails. Furthermore, low cognitive impulsivity and high agreeableness level were linked with identifying phishing emails only, while high neuroticism level was linked with spear-phishing emails only.

A multi-cultural study was conducted over four counties with a sample size of 618 [15]. The research focuses on measuring secure behavior (how secure a person is online), self-efficacy (how confident a person is against cyber risk), and privacy attitude (how dangerous a person feels to share info online). This was measured using an online survey. Risk perception predicts secure behavior and self-efficacy. Gender was found to be a strong predictor of self-efficacy in men. As for personality traits, openness can be used to predict self-efficacy, while conscientiousness can predict secure behavior, and finally, emotional stability can predict self-efficacy.

B. IT Background affect on Spear-Phishing Susceptibility

Spear-phishing attacks take advantage of the user's lack of knowledge and attention to details, thus having an IT background may reduce the person's susceptibility to attacks. Tech-savvy people tend to have higher levels of computer knowledge that can play a role in detecting spear-phishing attacks.

A spear-phishing simulation was conducted at the Universiti Kebangsaan Malaysia [16]. It included 553 staff emails from multiple science and technology (S&T), and non-science and technology (non-S&T) faculties. The spear-phishing bait was "Financial Aid", with a post-analysis survey that was sent after the simulation had ended. 45% of the participants who got phished were under S&T faculties, while 49% were under non-S&T faculties, and the remaining 5% were from other departments.

A study was conducted in the International Islamic University Malaysia [17], including 245 participants from various faculties. The study included a survey that contained demographic questionnaires, Information Technology (IT)-related questions, computer usage, and lastly are questions asking how students behave against cyber-attacks. The survey results show that IT students were more aware of social engineering compared to non-IT; furthermore, the study level also affected the knowledge (postgraduate vs. undergraduate). A small number of students reported being a victim of social engineering (provided private information through an email), which contained more non-IT students than IT students. These findings are in line with [30] that discovered tech-savvy people are more aware of digital attacks and less likely to fall for such attacks.

Another phishing study was conducted in the University of Maryland, Baltimore County [18] that included 1350 students split into three groups (three different phishing emails). This study aimed to better understand the factors such as faculty, academic year progression, cyber training, time spent on the computer, gender, and phishing awareness. The results show that STEM majors (science, technology, engineering and mathematics) had a lower click rate (EIT 65%, NMS 70%), while non-STEM had a higher click rate (AHSS 80%). The study also shows a correlation between academic year progression, cyber training and phishing susceptibility, while gender showed no significant correlation.

C. Message Framing affect on Spear-Phishing Susceptibility

Many resources are put every year by companies to design and carry out cyber awareness training programs for their employees to raise resilience to cyber-attacks such as spear-phishing. Having a more customized training program can help organizations cut time and cost and protect their assets and employees against future attacks.

A study was conducted to measure the effect of message framing in spear-phishing attacks [13]. The training material used was framed in four different ways, stressing positive/negative and individualism/collectivism. 1,359 participants were chosen and put randomly in one of 5 groups, a control group, and 4 framed groups. After the training, the overall click rate was lower, but no significant difference was found compared to the control group. However, the viewing time for the training page was measured, and it suggests that most people skimmed through the training and hence did not fully comprehend the training material.

A study explored embedded training and the effect of message framing in spear-phishing attacks [12] 400 participants were chosen and put randomly into one of six groups, two control groups and four groups that each represent a different way of framing the training message (add reference to support this statement). Results also show a weak association between individual-loss and click rate, as the group had a 12% improvement over the Round 2 control group.

A study was conducted in which 19,180 participants were included and split into 32 groups. Phishing emails were sent over a period of 8 months max, and training was embedded to the phishing link (if the user gets phished, he/she gets trained) [10]. The results showed that 25.94% of people who did not get the training fell for phishing, while only 15.57% of people who got the training fell for phishing (statistically significant p-value).

III. HYPOTHESIS

The hypotheses used in this study are based on findings from the Literature Review section. First, the personality traits, the majority of the papers have tested the relation between the Big Five personality traits and user's susceptibility to phishing emails (susceptibility can be measured by click rate). However, little work has been done on the subcategories of those traits. Research done by Moody et al. [14] focused on seven personality traits that can be seen as subcategories of the Big Five and five other constructs related to the victim's email characteristic and internet experience. Thus, this work will be a

continuation based on Moody et al. [14] work. Furthermore, the effect of message framing was observed when delivering spear-phishing training materials. Previous work that was done by Caputo et al. [13] and Burns et al. [12] will be used as a baseline for spear-phishing training. Based on the groundwork laid out, the instruments used by Moody et al. [14] can be used to test how some personality traits affect susceptibility to spear-phishing.

A. Constructs

The constructs that showed promising results fall into three categories, personality traits, message characteristic, and experience. The personality traits are curiosity, risk propensity, internet usage and anxiety, while message characteristic is represented by Message framing, and lastly, experience is represented by Information Technology (IT) background.

1) Curiosity: Curiosity can be defined as the desire for new knowledge and experience [19]. There are two types of curiosity, which are perceptual and epistemic. Perceptual curiosity is the attention given to novel perceptual stimulation evoked by visual, auditory, or tactile stimulation. In contrast, epistemic curiosity is defined as the desire to know aroused by conceptual puzzles. Furthermore, epistemic curiosity has two types of behaviors, labeled divertive and specific, divisive exploration is motivated by boredom, the desire to seek stimulation regardless of the source or content. While specific exploration is motivated by curiosity and the desire to investigate to acquire new information. Such behavior can be translated into the context of the internet, specificity emails, more curious people are more likely to click on unexpected emails, and are also more likely to click on a link or download attachments in an email.

- H1: Individuals with high levels of curiosity are more likely to fall for spear-phishing emails than individuals with lower curiosity levels.

2) Risk propensity: Risk propensity can be defined as the person's willingness to take risks in various aspects of life. Prospect theory, which was summarized in [20], it predicts that people are more willing to take risk when they are put in a domain of loss, and avoid risk when they are in a domain of gain. This can be linked to why most spear-phishing emails are framed in terms of loss (lose money, lose information), which makes it more likely for the victims to fall for spear-phishing and click on the malicious link.

- H2: High risk propensity levels are more likely to fall for spear-phishing emails than individuals with lower levels of risk propensity Individuals with.

3) Internet usage: Internet usage can be defined as the time spent on the internet doing various tasks and activities, such as browsing, emails, research. People who spend more time on the internet are more likely to be aware of the security concerns and risks of using the internet. Thus the prediction was, the more experience a user has with using the internet (spent more time on the internet), and the less likely he/she is to fall for spear-phishing emails.

- H3: Individuals with high internet usage levels are less likely to fall for spear-phishing emails than individuals with lower levels of internet usage.

4) Internet anxiety: Internet anxiety can be looked at similarly to anxiety, where an individual feels uneasy and worried about certain events such as a job interview or a test. Similarly, a user that has a high level of internet anxiety may feel the need to avoid using the internet, reply to people, or be active on social media. Thus having a high level of Internet anxiety can prevent users from replying or clicking on unexpected emails (spear-phishing emails).

- H4: Individuals with high levels of Internet anxiety are less likely to fall for spear-phishing emails than individuals with lower internet anxiety levels.

5) Information technology (IT) background: IT background refers to previous experience in using computers and technology. This experience can be associated with cyber-security knowledge. Most tech-savvy users are more likely to be aware of the cyber-threats, thus lowering their chances of falling victim to cyber-attacks spear-phishing emails. In the context of this experiment, students from science and technology (S&T) faculties are assumed to have heavy IT background, while other students from non-S&T faculties are assumed to have less comprehensive IT backgrounds.

- H5: Individuals from S&T faculties are less likely to fall for spear-phishing emails than individuals from non-S&T faculties.

6) Message framing: Message framing refers to how the training message is worded in terms of individualism/ collectivism and in terms of gain/loss. Individualism focuses on individual goals, while collectivism focuses on the collective group. Gain emphasizes adding, while loss emphasizes removing. A previous study showed a weak association between training effectiveness (reduction in click rate) and individual/loss [12].

- H6: Framing the training message in terms of individual/loss is more effective compared to framing the message in terms of individual/gain, group/loss, and group/gain.

B. Hypotheses

The previous 6 hypotheses are summarized and can be seen in Table I.

TABLE I. HYPOTHESES

#	Construct	Expectation
H1	Curiosity	Higher susceptibility
H2	Risk propensity	Higher susceptibility
H3	Internet usage	Lower susceptibility
H4	Internet anxiety	Lower susceptibility
H5	IT background	Lower susceptibility
H6	Message framing (individual/loss)	Increase training effectiveness

IV. METHODOLOGY

This study was conducted in four phases, following the spear phishing procedure conducted by [16]. However some of the details in each phase have changed to cope with the scope of this study. The four phases are planning, design and pilot-run, implementation, and analysis. Figure shows the different stages at each phase. During the first phase, a pilot-run will be designed; this includes designing the training page, the contexts of the email, as well as the survey. The pilot run will be run on around 10 students, the students will be a mix of IT and non IT majors of undergraduate and postgraduate degrees. In the design phase, modification can be made on the initial design; furthermore, the technical aspect of the project will be designed here. In the implementation phase, the participants are sent a survey, they are also informed that they will be participating in an experiment; however the true nature of the experiment will not be revealed to them just yet. Then they are split into five groups at random, one of the groups will be a control group which will not receive any sort of training and will only be notified that the email was a spear-phishing email. While the other four groups will receive training, if they click on the link in the first round. After a window of delay of around two weeks to reduce the priming effect (exposure to one stimulus influences the response to subsequent stimulus without conscious), the second round of phishing will be sent. Once the emails have been sent, and a window of time is given to the participants to check their emails, the final phase can begin to analyze and report the findings. The overall methodology is shown in Fig. 1.

Two-round spear-phishing simulation was conducted to find the relation between personality traits and phishing susceptibility and the effect of message framing. Participants were students from the Universiti Kebangsaan Malaysia (UKM) recruited through emails, where a personality traits survey was sent. The true nature of the experiment was not revealed to participants. Participants were told that the study aims to understand students' feelings, behaviors, and personality traits at UKM and their relationship to cyber-security behavior. Total 107 participants filled out the survey, of which seven of them did not provide a valid ID (which is used to send emails through the university email system). The final sample size was 100, of those 71% were female and 29% were male. 86% of participants were between the ages of 18 and 32, and 14% were between the ages of 33 and 48. 56% were postgraduate students and 44% were undergraduate students. As for faculty distribution, 59% are under S&T faculties, and 41% are under non-S&T faculties.

There are three main components needed for this study, personality trait survey, phishing emails, and training material. The personality trait survey was sent to four people to get their feedback on the length, and word choices and overall clarity of the survey. Followed by a pilot-run that included 10 students from UKM, the pilot-run started with sending the survey, and after a delay, a phishing email was sent to each participant to test the instruments.

The first round of spear-phishing emails was sent a month after the personality traits survey. This delay was used to eliminate any priming effect. The spear-phishing email contained a link, if clicked participants were taken to a training page and thus considered trained. Participants were split into five groups, a control group and four other groups to test the effect of message framing. Each participant received a unique link; this will allow us to identify participants who click on the spear-phishing link as well as link the personality traits score with clicking behavior.

After a two weeks' delay from the first round of spear-phishing the second round of emails were sent. This time, the click rate between the different groups to test the effect of message framing was compared. Participants who clicked on the first round, were kept in their respective group, as they were "trained". However, participants who did not click in the first round were moved to a new group "Round 1 non-clickers" because they were not exposed to the training material.

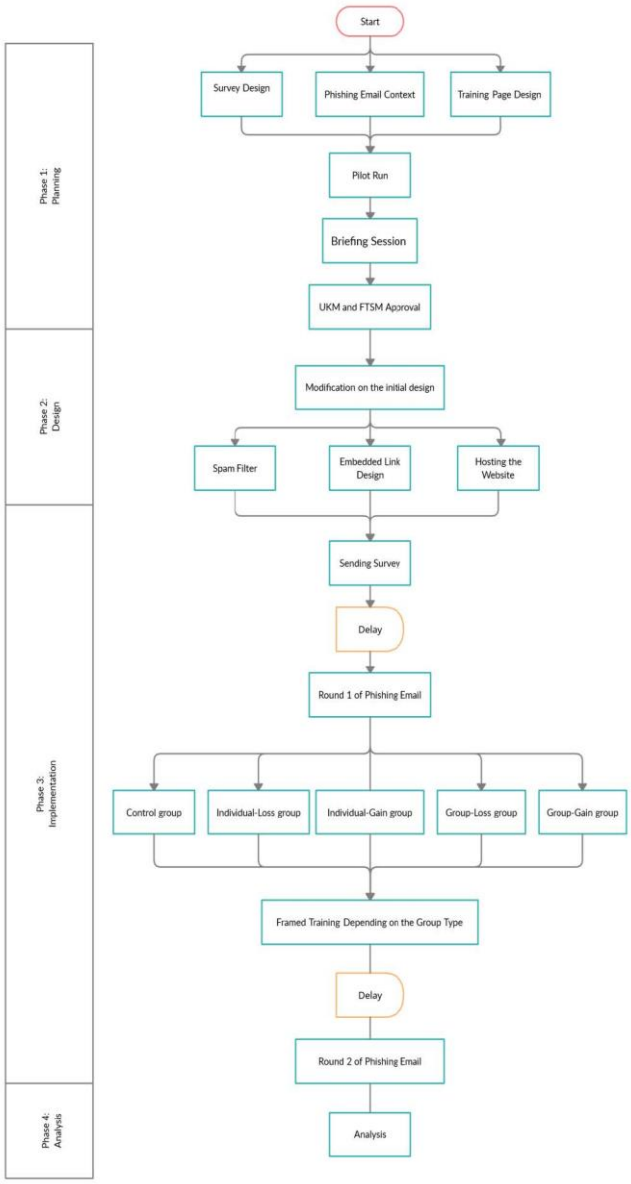


Fig. 1. Methodology flowchart.

A. Personality Traits Survey

The personality trait was based on a set of psychology papers compiled by Moody et al. [14], however, the survey used in that paper requires around 25-30 minutes to complete it. Having such a comprehensive survey may affect the number of students that complete it. Furthermore, it may result in participants filling the form randomly toward the end of the survey. Thus, the survey was shortened to around 7-9 minutes. This was done by focusing on the personality traits that had significant results. The survey must have the option to choose the preferred language; this is because of the diversity of students in the university. The survey vocabulary was also slightly modified to make it easier to read for non-native English readers. This involved some minor reorganization and the use of common parlance.

The survey is split into four main parts:

- Curiosity: 22 questions (normal scale), the scale used is a 4-point scale (min: 22, max: 88).
- Risk: 17 questions (3 questions were reverse scale), the scale used for the first 5 questions is a 7-point scale; for the other 12 questions, a 5-point scale is used (min: 17, max: 95).
- Internet Experience: 17 questions (normal scale), the first 4 uses a 5-point scale, and the last 13 questions, a 7-point scale is used (min: 17, max: 111).
- Internet Anxiety: 6 questions (1 question was reverse scale) with a 7-point scale (min: 6, max: 42).

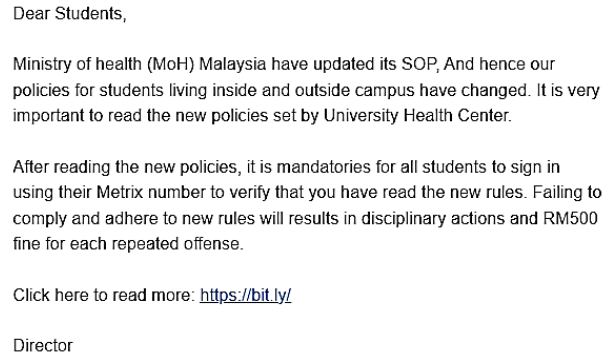
B. Spear-Phishing Emails

Two rounds of phishing emails will be used. During the design, the following points were taken into account:

- The sender: or the actor, as well as his/her positions, is essential, because people tend to trust emails sent from a higher hierarchy.
- Engagement mechanism: What is on the line, and why would the victim engage with the email. This can be a form of a fine, or losing personal information.
- Title: The email title must highlight the importance of the subject at hand to serve as a clickbait.

Since attackers may customize the email to certain employees or businesses to maximize the likelihood of success, the phishing email topic was chosen in a way that can lure victims to click on the email and make the spear-phishing assault as realistic as possible.

1) Spear-phishing: round 1: The first topic of choice was "Covid-19 SOP update (Coronavirus Disease 2019)". This study was being conducted during the Covid-19 pandemic, and the Malaysian government had implemented multiple movement control orders and various Standard Operating Procedure (SOP) for people to comply with. Furthermore, because of different faculties that will be included in this study, the topic must be applicable to all students, post and undergraduate, local and international, S&T and non-S&T students. The engagement mechanism used for this topic is a fine of RM500 imposed on students for each repeated offense. For the actor (the sender), we have chosen the director of UKM Health Center (PK), however, their name was not included to avoid some cases where some students may call the person to double-check if the email is legitimate, on the other side some people may not know the director by name, and hence the name was omitted for those reasons. A sample of the first round phishing email can be seen in Fig. 2.


Dear Students,

Ministry of health (MoH) Malaysia have updated its SOP, And hence our policies for students living inside and outside campus have changed. It is very important to read the new policies set by University Health Center.

After reading the new policies, it is mandatories for all students to sign in using their Metrix number to verify that you have read the new rules. Failing to comply and adhere to new rules will results in disciplinary actions and RM500 fine for each repeated offense.

Click here to read more: https://bit.ly/

Director

Fig. 2. Round 1 phishing email.

2) Spear-phishing: round 2: The second topic of choice is "UKMFOLIO system upgrade". UKMFOLIO is a learning system used by UKM to deliver teaching materials and announcements and a method to submit assessments. During the study, UKMFOLIO was down multiple times, students and lecturers couldn't access the website. Therefore, sending an email informing the students that there will be a system upgrade will be a good bait for the second phishing email. All UKM students use UKMFOLIO, and hence it applies to everyone. As for the engagement mechanism, students were told that they would lose access to their accounts if they fail to update and verify their information. For the actor (the sender), the director of the Information Technology Center (PTM) was chosen.

C. Training Materials and Message Framing

The training materials are divided into two sections; the first sections include materials designed to highlight clues in the spear-phishing emails that the user needs to be on the lookout to detect spear-phishing emails. Those clues include:

- Sense of urgency: The matter at hand is time-sensitive and actions must be taken immediately.
- Fake/mismatch in the sender's email field: Spear-phishing emails impersonate well-known figures or authorities, as such, it is essential to look at the sender's email.
- Malicious link: The link is usually disguised or presented in terms of a hyperlink to hide the actual URL.

Fig. 3. Individual / Gain training message.

Fig. 4. Individual / Loss training message.

The second part is an informative bit on the consequence of spear-phishing, and how to protect yourself from spear-phishing. This part of the message is framed in terms of individual/group gain/loss, where the pronouns (yourself/your co-worker) and the tone (positive/negative) are different in each group. Fig. 3 and Fig. 4 show the second part of the training material for two different groups (Individual/ Gain and Individual/Loss, respectively).

Technical phrases were simplified so that students could relate to the training material, and new training materials that are comic-based were employed to keep users' attention for longer and transmit the knowledge more effectively. Additionally, the materials are constructed in a way that evokes a sense of urgency, hinting that the issue at hand is time-sensitive and requires immediate action.

V. Results

The results and discussion will be split into two main sections; the first section will cover the first round of phishing relating to personality traits, which was used to test hypotheses H1-H5, while the second section will cover the second round of phishing relating to message framing in embedded training, which test hypothesis H6. Because of the nature of the output (dependent variable) being binary, where 1 denotes "got phished" and 0 "did not get phished", multiple logistic regression was used to determine the coefficient value. STATA v. 16.1 SE was used to carry out the regression.

As for message framing, a Binomial test was carried between each group and the control group to test the effect of message framing.

A. Personality Traits Result

First, Cronbach's Alpha was calculated to measure the internal consistency and verify the validity of the test. The Cronbach's Alpha is 0.8425 which is above the acceptable level of 0.70. Looking at the alpha value when the item selected is removed, there is no significant change among all 62 questions, with a minimum value of 0.8362 and a maximum value of 0.8456 (difference less than 0.01). Table II shows the statistics summary of the personality traits test. The multiple logistic regression results can be seen in Table III. Curiosity and risk had a negative coefficient, while internet experience and internet anxiety had a positive coefficient. Furthermore, S&T (refer to students who are in S&T faculties) also had a positive coefficient. Gender and Age were added in the regression; gender (male) had a negative coefficient, while age (young) had a positive coefficient. S&T, gender, and age were coded as binary values such as 1(S&T) and 0 (non-S&T); gender-1 (male) and 0 (female); and for age, 1 represented young (between 18 and 32) and 0 represented participants older than 32.

The Pseudo R2 value is McFadden's pseudo R-squared, because logistic regression does not have a direct equivalent to the R2 value found in OLS linear regression. The Pseudo R2 value is 0.0661, which is still low. However, a low R2 is to be expected when measuring variables related to human behavior, as humans are harder to predict.

TABLE II. Statistics Summary of the Personality Traits

Variable	*Mean*	*Std. Dev.*	*Min*	*Max*
Curiosity	69.98	7.717198	54	87
Risk	31.26	9.691838	17	60
Internet experience	36.27	11.26706	20	69
Anxiety	19.34	5.324273	10	33
S&T	0.59	0.494311	0	1

B. Message Framing Result

Two weeks after the first round of phishing (Round 1), a second email was sent to participants. 100 participants received the second phishing email titled "UKMFolio System Upgrade".

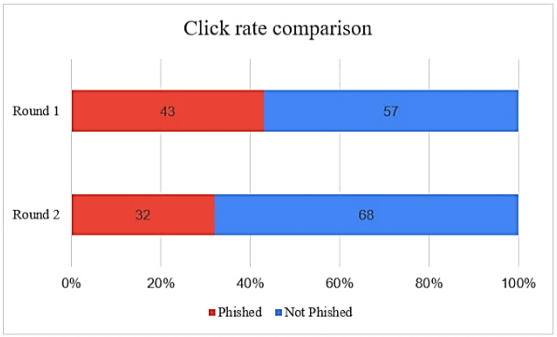


Fig. 5. Click rate comparison.

Comparing the click rate between Round 1 and 2 in Fig. 5, there is a decrease in click rate from 43% to 32%. Similar to Round 1, the majority of clicks happened within the first 24 hours.

First, a Pearson Chi-square test was performed among the five groups from Round 1 to check if there are no unexpected differences between the groups by any chance, and found no significant relation between the groups and the phishing rate, X2 (4, N=100) = 6.0108, p=0.198. Similarly, in Round 2, a Pearson Chi-square was performed and no significant relation was found between the 6 groups and the phishing rate ("non-clicker Round 1" was added as shown in Table IV and Table V.

TABLE III. MULTIPLE LOGISTIC REGRESSION RESULTS

Phished	*Coef.*	*Std. Err.*	*z*	*P>z*	*95% Conf.*	*Interval*
Curiosity	−0.050147	0.031410	−1.60	0.110	−0.11171	0.011416
Risk	−0.021760	0.023325	−0.93	0.351	−0.06748	0.023956
Internet experience	+0.020639	0.019619	+1.05	0.293	−0.01781	0.059092
Anxiety	+0.084030	0.042934	+1.96	0.050	−0.00012	0.168178
S&T	+0.727525	0.457443	+1.59	0.112	−0.16905	1.624096
Gender	−0.744610	0.498756	−1.49	0.135	−1.72215	0.232935
Age	+0.107320	0.660629	+0.16	0.871	−1.18749	1.402129
Cons	+1.205229	2.377349	+0.51	0.612	−3.45429	5.864748

LR chi^2 (7) = 9.04; Prob >chi^2=0.2501; Pseudo R2=0.0661, the bold value indicates a significant value P<0.05

TABLE IV. ROUND 1 RESULTS BY GROUPS

Round 1	*Total*	*Grp-Gain*	*Grp-Loss*	*Ind-Gain*	*Ind-Loss*	*Control*	*Non-clicker Round 1*
Not-phished	57 (57.0%)	8 (50.0%)	11 (84.6%)	9 (50.0%)	8 (44.4%)	21 (60.0%)	N/A
Phished	43 (43.0%)	8 (50.0%)	2 (15.4%)	9 (50.0%)	10 (55.6%)	14 (40.0%)	N/A
Total	100	16	13	18	18	35	N/A

TABLE V. ROUND 2 RESULTS BY GROUPS

Round 1	*Total*	*Grp-Gain*	*Grp-Loss*	*Ind-Gain*	*Ind-Loss*	*Control*	*Non-clicker Round 1*
Not-phished	68 (68.0%)	6 (75.0%)	1 (50.0%)	6 (66.7%)	85 (50.0%)	9 (65.3%)	41 (71.9%)
Phished	32 (32.0%)	2 (25.0%)	1 (50.0%)	3 (33.3%)	5 (50.0%)	5 (35.7%)	16 (28.1%)
Total	100	8	2	9	10	14	57

VI. DISCUSSION

This study's objective was to find which personality traits affect a person's susceptibility to spear-phishing emails. Using a personality traits survey to measure personality score, and a real-life simulation of a spear-phishing email, logistic regression are carried out to find factors affecting spear-phishing susceptibility. Furthermore, training material is provided to participants who got phished to test the effect of message framing in embedded training. The second round of spear-phishing is carried to test the training material's effectiveness by carrying out a Binomial test. The summary of results can be seen in Table VI and Table VII.

A. The Effect of Personality Traits on Spear Phishing

The results of this study show that only anxiety has a significant relation with susceptibility to phishing ($p<0.05$). However, the nature of the relationship is not as theorized in previous sections.

Other factors such as gender and age were also tested. While both had no significant findings ($p=0.135$ and 0.871), gender (male) had a negative coefficient, which means women are likely to fall for spear-phishing emails. This supports previous studies' findings [22], where it was reported that females are more susceptible to phishing. Age (young) had a positive correlation which also supports previous studies suggesting that younger people are more susceptible to spear-phishing emails [23, 24]. This can be caused by the fact that younger people have not fallen for or experienced spear-phishing and have a lower ability to detect spear-phishing emails.

1) Curiosity: First, curiosity did not have a significant finding on phishing susceptibility ($p=0.110$). Thus not supporting hypothesis H1. Furthermore, curiosity had a negative coefficient (-0.050147) on phishing susceptibility, meaning that a person who has a high level of curiosity is less likely to fall for spear-phishing emails. This is counterintuitive because a person who possesses a high level of curiosity may find unexpected emails with a link appealing to explore, and thus clicking on the link. Previous study [25] reported that curiosity was the most common reason for clicking on phishing emails and Facebook messages in the post-experiment survey. Another study [14] reported significant findings on the positive correlation between phishing susceptibility and curiosity. Looking at a broader view on curiosity, openness (from The Big Five) can be defined as a person who is curious. This personality trait was found to be non-significant in some studies [6,7] where no significant finding was found between phishing susceptibility and openness.

TABLE VI. PHISHING DETECTION IMPROVEMENT AND BINOMIAL TEST

	Grp-Gain	***Grp-Loss***	***Ind-Gain***	***Ind-Loss***
Improvement (compared to control group)	+10.7 (+29.9%)	−14.3 (−40.1%)	+2.4 (+6.7%)	−14.3 (−40.1%)
Binomial test (expected value is control group)	0.411217	0.872551	0.591295	0.896560

TABLE VII. ROUND 2 RESULTS WITH BINOMIAL TEST

# Construct	***Expectation***	***Results***	***Coef.***
H1 Curiosity	Higher susceptibility	N.S	Negative
H2 Risk propensity	Higher susceptibility	N.S	Negative
H3 Internet usage	Lower susceptibility	N.S	Positive
H4 Internet anxiety	Lower susceptibility	Sig.(<0.05)	Positive
H5 IT background	Lower susceptibility	N.S	Positive

Looking at the survey's curiosity questionnaire, the questions used from previous studies measure curiosity in various aspects in life. For example, in the epistemic curiosity (Diversive) section, questions such as "I like to learn new things / like to find out more", "I enjoy exploring new ideas", and "It is fascinating to learn new information" was used to measure the desire to acquire knowledge aroused by puzzles and motivated by the feeling of boredom regardless of the source. The questions used are not specific to a certain situation and can be applied to the context of spear-phishing emails. An email suggesting a new idea, or giving a new insight can be intriguing to the user. However, other questions under epistemic curiosity (Specific), included questions such as "I enjoy finding a solution to new kind of arithmetic problem", "If I see a complicated piece of machinery, I will ask someone how it works", and "I try and imagine the solution for incomplete puzzle". Such questions are situation specific; a person that is curious about how machines work may not be interested in an email asking the user to read about a new policy. Moreover, in the perceptual curiosity (Uniquely loading items) section, 12 questions with 4-point scale were used (same tense throughout the experiment description is not followed) to measure it; this means that perceptual curiosity had more weight when measuring the overall level of curiosity. This may not be the correct scale when measuring internet curiosity. While general curiosity questionnaires are still a good measure, a scale favouring the user's curiosity in internet-related topics may be more suitable in this situation. For example, asking the user "how often do you watch new shows that you have never heard of" and "how often do you click on online ads" may be a more accurate measure of online curiosity. This may explain the reason why there is no significant relation between curiosity and phishing susceptibility. Furthermore, the negative correlation between curiosity and spear-phishing susceptibility can also be linked to the topic of spear-phishing. While this study was conducted during the Covid-19 pandemic, and the topic of the spear-phishing email is related to covid-19 policies, Pandemic Fatigue [26] can also explain the negative relation, where users are experiencing Pandemic Fatigue after nearly a year of dealing with Covid-19 related issues, and thus the demotivation of reading related topics.

2) Risk propensity: Hypothesis H2 was not supported as well. Risk also had a non-significant finding (p=0.351), it also had a negative coefficient (-0.021760). This finding contradicts the theory that a more risk-taking person will likely click on an unexpected link in an email regardless of its risk. Previous studies [15] found that the risk of being a significant predictor of phishing susceptibility suggests that people with higher risk perception are experienced in cyber-security and are thus more likely to averse the risks associated with clicking on unknown links. Moody et al. [14] also found risk to be a significant predictor of susceptibility to phishing.

The risk questions included in the survey measure risk beliefs (perceived risk) and risk propensity. Part of the risk beliefs scale was reversed because of the negative relation between risk perception and risk-taking behavior, while risk propensity was scored normally because of the positive relation between risk propensity and risk taking [27]. This means that a high risk score (overall) reflects a high risk taking behavior. In theory and based on previous studies, a more willing to take risk is more likely to click on an unexpected link in an email. However, findings suggest the opposite (even if it is not significant), this might be explained by how people overestimate their ability to identify scam emails. Datar, Cole, and Rogers [28] found that more than half the participants that claimed they can identify a scam email failed to identify them. This means even if a person has a low-risk overall score (person scored high perceived risk (inverted) and a low risk propensity score), he/she may not be able to identify an email as a spear-phishing email and thus not perceive the actual risk of clicking on the link.

3) Internet usage: Internet experience did not have a significant finding (p=0.293); hence hypothesis H3 was not supported, however, there was a positive relation between internet experience and phishing susceptibility. The result is counter-intuitive; however, a study [14] also found similar results. A person who uses the internet is more likely to click on a phishing link. One of the reasons that might explain these results is Habituation [29]. The person's innate response to a stimulus decreases after repeated presentation of the stimulus. In the context of spear-phishing emails. If the user spends a lot of time on the internet (experienced user), he/she may pay less attention over time to spear-phishing clues and this fall for spear-phishing emails.

4) Internet anxiety: The last hypothesis relating to personality trait H4 (internet anxiety) had a significant finding (p = 0.05) with a small positive coefficient. This finding matches previous research [14]; even if the initial hypotheses suggested the opposite effect (negative correlation), Halevi et al. [22] found a positive correlation between neuroticism (from The Big Five personality traits) and phishing susceptibility for women only. A few reasons might explain the results, first people with high anxiety levels may feel bothered by unanswered emails, thus the need to reply or click on a phishing email. Another reason might be related to being a "people pleaser" where a person may find it difficult to say no, and thus feel the need to provide information in phishing emails.

5) IT background: The last hypothesis H5, that was tested in Round 1 of phishing is the relation between IT background and phishing susceptibility, there was no significant finding (p=0.112), however, the correlation coefficient was positive, which means participants from S&T faculties were more likely to get phished. While most studies discussed in chapter 2.1.2 suggest a negative correlation between IT background and phishing susceptibility, habituation may explain the positive correlation found in this experiment. Students under S&T faculties may be constantly reminded about cyber-attacks and hence pay less attention to spear-phishing emails.

B. The Effect of Personality Traits on Spear Phishing

The binomial test shows no significant results, this matches a previous study [13], where no significant relation was found among the four groups, and thus H6 was not supported. However, looking at the improvement rate, group-gain had the highest improvement (although not significant) compared to other groups with a decrease of 10.7 compared to control group click rate in Round 2. Furthermore, gain treatment (both group and individual) saw an improvement in detecting spear-phishing emails, while loss treatment (both group and individual) performed worse than the control group.

Several factors contributed to those findings, first there is no way to make sure that participants have taken part in the training, for example, if the participants immediately closed the training page after clicking without reading any of the content. Furthermore, some people may have skimmed through the training and thus have not fully understood the content. While the use of comics instead of text may have helped in retaining the participant's retention, there is still a possibility that the comics did not convey the information effectively compared to text because the comic's design has to be short and to the point.

Secondly, the information's credibility might not be clear to the participants, as the training was not hosted on an official university website, and hence recipients did not find the training credible. Thirdly, the training effectiveness may require repetition before a noticeable behavior change is observed where the same training is applied multiple times over an extended period of time. Lastly, the sample size for the experiment is relatively small. Because of the experiment's nature, where only people who clicked have received the training, each group's final sample size is very small. It may have produced inaccurate results that do not represent the population.

C. General Implications

Spear-phishing emails are highly targeted by nature; attackers will use current trending topics and events to lure their victims into clicking on malicious links. Spear-phishing emails continue to be a large threat, and with organizations heavily relying on emails for communication, it is more important than ever to understand better the factors that make spear-phishing emails so successful. One of the most important factors is the human link. With humans being the weakest link, it is evident that the attacker will try to exploit such weakness and try to use it to their advantage. A lot of effort has been put into securing information from direct attacks; however, most recent successful attacks have infiltrated organizations through human error. Having a better understanding of what makes a person fall for spear-phishing emails is vital in fortifying the human firewall.

One of the factors that can affect a person's susceptibility is his/her personality traits. Prior research has focused on a wide variety of personality traits, this research narrows down the scope and focuses on key traits that have been found to be a factor in predicting phishing susceptibility [30, 31]. Out of the four personality traits that have been put to the test, internet anxiety has shown significant results in predicting phishing susceptibility. The reason is, internet anxiety affects phishing susceptibility is that anxious people may feel bothered by unresolved issues suggested by the email, and thus have the compulsive need to reply or check the spear-phishing email. While other personality traits did not show significant results, it is still possible that in a different environment, different personality traits may show a stronger correlation with phishing susceptibility due to the difference in culture and background.

Having a better understanding of who is more susceptible to cyber-attacks, such as spear-phishing attacks, can be an important factor in designing a training module for an organization. Knowing which type of people are more susceptible can save many resources in terms of training time and cost when trying to raise security awareness in an organization. While this study does suggest that embedded training lowers the success rate of spear-phishing attacks, however there is no justification to believe that message framing can affect training efficiency.

VII. Conclusion

Primary Personality traits may hold the key to better understanding what makes some people more susceptible to spear-phishing than others. This research shows that certain personality traits can contribute to higher susceptibility to spear-phishing emails. A real-life spear-phishing experiment was implemented to measure the correlation between spear-phishing susceptibility and personality traits. The results show that Internet anxiety increases the person susceptibility to spear-phishing. An embedded training was provided to participants through the phishing emails, and through two rounds of emails. The embedded training lowered the overall click rate; however, there is no evidence to support the notion that message framing affects training effectiveness. While the small sample size in this study can provide some limitations), the results show promising results on the effect of personality traits on phishing susceptibility. Future research can aim to test the hypotheses on a larger sample size, and over a longer period of time.

VIII. Future Research Directions

The primary limitation of this study is the sample size. The sample size for this study was 107 participants, which is relatively small to the population of UKM. The main reason for that is the restriction because of the Covid-19 pandemic and time constraints of this study. The distribution of personality traits survey was limited to online forms, and physical distribution was not possible. Other factors that contributed to this small sample size include that participants had to answer a survey for them to take part in the spear-phishing study; while a monetary incentive was formed to encourage participants to fill out the survey, thus unable to determine its effectiveness. Because the invitation emails to do the survey was sent by faculty's staff, lecturers and IT centers, the total number of recipients was not disclosed for privacy reasons. Furthermore, a list of emails for all students contributes to the privacy concerns as well. Furthermore, because this study relies on people getting phished, this results in an even smaller sample size for each group. Previous studies had a click rate of around 40% (similar to study); this means that the final sample size will be even smaller when testing the training module's effectiveness. Another factor that can be improved is the personality traits questionnaire; this study uses existing instruments to measure the various traits. Designing more tailored questions that can relate better to internet behavior can show promising results.

Our study can lead to multiple paths down the road. Future researchers can examine if the findings persist over larger sample size. A sample size that includes all students in the university can lead to more accurate results and can eliminate any anomalies due to small sample size. If the survey had a low response rate, a larger sample size to start with will result in a sufficient number of participants answering the survey. Moreover, using a personality trait instrument that is designed with internet behavior and habits can lead to a better measurement of some traits. Lastly, the effectiveness of embedded training and message framing can be measured better when observed over an extended period of time. This also requires repetition of training, Future research can implement this study in multiple phases and multiple phishing rounds over an extended period of time, and larger break time between each phishing round to eliminate any priming effect other improvements can be implemented, for example, interactive embedded training that requires user's interaction can be included to make sure that participants have read and understood the training.

Acknowledgment

This study was supported by the Fundamental Research Grant Scheme (FRGS/1/2021/ICT02/UKM/02/1) from Ministry of Higher Education, Malaysia.

References

[1] Phishing.org, Phishing | History of Phishing, [Online]. Available: https://www.phishing.org/history-of-phishing.

[2] Symantec, ISTR Internet Security Threat Report 2019 Volume 24., 2019.

[3] Anti-Phishing Working Group, "Phishing Activity Trends Report 3 Quarter.," no. November, pp. 1–12, 2020.

[4] ProofPoint, State of the Phish., 2020.

[5] Verizon, 2020 Data Breach Investigations Report., 2020.

[6] S. Anawar, D.L. Kunasegaran, M.Z. Mas'Ud, and N.A. Zakaria, "Analysis of phishing susceptibility in a workplace: A big-five personality perspectives.," Journal of Engineering Science and Technology. vol. 14, no. 5, pp. 2865–2882, 2019.

[7] M. Butavicius, K. Parsons, M. Pattinson, A. Mccormac, D. Calic, et al., "Understanding Susceptibility to Phishing Emails: Assessing the Impact of Individual Differences and Culture.," Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017). vol. 2016, no. Haisa, pp. 12–22, 2017.

[8] B. Cusack and K. Adedokun, "The impact of personality traits on user's susceptibility to social engineering attacks,." Proceedings of the 16th Australian Information Security Management Conference. pp. 83–89, 2018, 10.25958/5c528ffa66693.

[9] E.D. Frauenstein and S. Flowerday, "Susceptibility to phishing on social network sites: A personality information processing model.," Computers and Security. vol. 94, p. 101862, 2020, 10.1016/j.cose.2020.101862.

[10] H. Siadati, S. Palka, A. Siegel, and D. McCoy, "Measuring the effectiveness of embedded phishing exercises.," 10th USENIX Workshop on Cyber Security Experimentation and Test, CSET 2017, co-located with USENIX Security 2017. p. 2017.

[11] A. Xiong, R.W. Proctor, W. Yang, and N. Li, "Embedding Training Within Warnings Improves Skills of Identifying Phishing Webpages.," Human Factors. vol. 61, no. 4, pp. 577–595, 2019, 10.1177/0018720818810942.

[12] A.J. Burns, M.E. Johnson, and D.D. Caputo, "Spear phishing in a barrel: Insights from a targeted phishing campaign.," Journal of Organizational Computing and Electronic Commerce. vol. 29, no. 1, pp. 24–39, 2019, 10.1080/10919392.2019.1552745.

[13] D.D. Caputo, S.L. Pfleeger, J.D. Freeman, and M.E. Johnson, "Going spear phishing: Exploring embedded training and awareness.," IEEE Security and Privacy. vol. 12, no. 1, pp. 28–38, 2014, 10.1109/MSP.2013.106.

[14] G.D. Moody, D.F. Galletta, and B.K. Dunn, "Which phish get caught An exploratory study of individuals′ susceptibility to phishing.," European Journal of Information Systems. vol. 26, no. 6, pp. 564–584, 2017, 10.1057/s41303-017-0058-x.

[15] T. Halevi, N. Memon, J. Lewis, P. Kumaraguru, S. Arora, et al., "Cultural and psychological factors in cyber-security.," ACM International Conference Proceeding Series. no. November 2017, pp. 318–324, 2016, 10.1145/3011141.3011165.

[16] N.A. Bakar, M. Mohd, and R. Sulaiman, "Information leakage preventive training.," Proceedings of the 2017 6th International Conference on Electrical Engineering and Informatics: Sustainable

Society Through Digital Innovation, ICEEI 2017. vol. 2017-Novem, pp. 1–6, 2018, 10.1109/ICEEI.2017.8312403.

[17] M. Elsadig Adam and O. Yousif, “Awareness of Social Engineering Among IIUM Students.,” World of Computer Science and Information Technology Journal (WCSIT). vol. 1, no. 9, pp. 409–413, 2011.

[18] A. Diaz, A.T. Sherman, and A. Joshi, “Phishing in an academic community: A study of user susceptibility and behavior,” (2018), 10.1080/01611194.2019.1623343.

[19] J.A. Litman and C.D. Spielberger, “Measuring epistemic curiosity and its diversive and specific components.,” Journal of Personality Assessment. vol. 80, no. 1, pp. 75–86, 2003, 10.1207/S15327752JPA8001_16.

[20] N. Nicholson, E. Soane, M. Fenton-O’Creevy, and P. Willman, “Personality and domain-specific risk taking.,” Journal of Risk Research. vol. 8, no. 2, pp. 157–176, 2005, 10.1080/1366987032000123856.

[21] Ahmad Fadhil Naswir, Lailatul Qadri Zakaria and Saidah Saad, “Determining the Best Email and Human Behavior Features on Phishing Email Classification” International Journal of Advanced Computer Science and Applications (IJACSA), 13(8), 2022. http://dx.doi.org/10.14569/IJACSA.2022.0130821

[22] T. Halevi, J. Lewis, and N. Memon, “Phishing, Personality Traits and Facebook.,” p. 2013.

[23] S. Sheng, M. Holbrook, P. Kumaraguru, L.F. Cranor, and J. Downs, “Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions.,” Conference on Human Factors in Computing Systems - Proceedings. vol. 1, pp. 373–382, 2010, 10.1145/1753326.1753383.

[24] R. Broadhurst, K. Skinner, N. Sifniotis, and B. Matamoros-Macias, “Cybercrime Risks in a University Student Community.,” SSRN Electronic Journal. p. 2018, 10.2139/ssrn.3176319.

[25] Z. Benenson, F. Gassmann, and R. Landwirth, “Unpacking spear phishing susceptibility.,” Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). vol. 10323 LNCS, pp. 610–627, 2017, 10.1007/978-3-319-70278-0_39.

[26] World Health Organization, “Pandemic fatigue: reinvigorating the public to prevent COVID-19.,” no. November, p. 2020.

[27] F. Sahul Hamid, G.J. Rangel, F. M. Taib, and R. Thurasamy, “The Relationship between Risk Propensity, Risk Perception and Risk-Taking Behaviour in an Emerging Market.,” International Journal of Banking and Finance. p. 2013, 10.32890/ijbf2013.10.1.8471.

[28] T.D. Datar, K.A. Cole, and M.K. Rogers, “Awareness of scam e-mails: An exploratory research study.,” In: Proceedings of the Conference on Digital Forensics, Security and Law (2014).

[29] B.B. Anderson, A. Vance, C.B. Kirwan, D. Eargle, and J.L. Jenkins, “How users perceive and respond to security messages: A NeuroIS research agenda and empirical study.,” European Journal of Information Systems. vol. 25, no. 4, pp. 364–390, 2016, 10.1057/ejis.2015.21.

[30] Eftimie, Sergiu, Radu Moinescu, and Ciprian Răcuciu. "Spear-Phishing Susceptibility Stemming From Personality Traits." IEEE Access. 10 (2022): 73548-73561.

[31] Yang, Rundong, Kangfeng Zheng, Bin Wu, Di Li, Zhe Wang, and Xiujuan Wang. "Predicting user susceptibility to phishing based on multidimensional features." Computational Intelligence and Neuroscience 2022 (2022).

[32] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman and M. A. Ibrahim, "Social Engineering Attacks Prevention: A Systematic Literature Review," in IEEE Access, vol. 10, pp. 39325-39343, 2022, doi: 10.1109/ACCESS.2022.3162594.

[33] R. Abdillah, Z. Shukur, M. Mohd and T. M. Z. Murah, "Phishing Classification Techniques: A Systematic Literature Review," in IEEE Access, vol. 10, pp. 41574-41591, 2022, doi: 10.1109/ACCESS.2022.3166474.