Personality Traits as Predictors for Social Engineering Vulnerability

Jake Imanaka[1], Michael-Brian Ogawa[1], and Martha E. Crosby[1]

[1] University of Hawai'i at Mānoa, Honolulu, HI 96822, USA
{jimanaka,ogawam,crosby}@hawaii.edu

Abstract: As security measures to protect against cyberattacks increase, hackers have begun to target the weakest link in the cybersecurity chain–people. Such attacks are categorized as Social Engineering and rely on the manipulation and deception of people rather than technical security flaws [4]. This study attempts to examine the relationship between people and their vulnerability to Social Engineering attacks by posing the following questions: (1) what relationship, if any, exists between personality traits and Social Engineering vulnerability, and (2) what relationship, if any, exists between personality traits and the speed at which an individual makes cybersecurity-related decisions. To answer these questions, 79 undergraduate students at the University of Hawaii were surveyed to measure their personality traits and cybersecurity awareness. The survey results indicated that there was no significant correlation between the measured personality traits and measured vulnerability. The relationship between different personality traits and the elapsed time to complete the survey was slightly more significant; however, it was still statistically insignificant overall.

Keywords: Social engineering, personality traits, computer security

1 Introduction

Now, more than ever, information systems are at risk of being breached due to the weakest link in cybersecurity–people [1]. Hackers equip themselves not only with advanced technologies to exploit our information systems but also with techniques to coerce individuals into willingly giving up their sensitive information–Social Engineering (SE). Social Engineering attacks bypass most security features implemented in information systems by targeting humans who own and use the systems directly. Once a Social Engineering attack is successful, and depending on the privilege level of the victim, a hacker can access sensitive information without throwing exploits, bypassing firewalls, or cracking a password [14]. Social Engineering's effectiveness and the relative ease at which it can be performed make it one of the most efficient and effective access vectors for a hacker.

1.1 Social Engineering Techniques

Social engineering techniques may use physical, social, technical, or socio-technical aspects to deceive their victim into divulging sensitive information [10]. Examples of classical SE techniques as described by Krombholz et. al. [10] are as follows:

- **Phishing:** An attack which can be performed over any electronic communication channel in which the attacker masquerades as a trusted individual. Phishing attacks can target large groups of people at the same time making them cost and time efficient. Sub-techniques include **spear-phishing**—where attackers target specific individuals rather than everyone, or **whaling**—where attackers target high-profile targets.
- **Shoulder surfing:** Technique where an attacker directly observes a victim to gain sensitive information. This could be performed by looking at a victim's screen or keyboard while they input their password.
- **Reverse social engineering**: Technique where an attacker establishes themselves as someone who can solve the victim's problems. The attacker will then create a situation where the victim may feel compelled to reach out to the attacker to ask for help.
- **Baiting**: An attacker leaves malware-infected storage mediums around so that potential victim's may pick them up, insert them into their computers, and infect themselves. These may take the form of USB sticks left in libraries or in classrooms.

1.2 Measuring Social Engineering Vulnerability

Prior studies have resulted in three main approaches in measuring Social Engineering vulnerability: Surveys, imitation studies, and lab experiments [11]. Each approach has inherent weaknesses and strengths. Surveys are simple to create and easy to distribute, but answers are self-reported by the subject and are thus vulnerable to the subject's biases. Individuals may feel embarrassed to admit they have fallen for a SE technique or fail to comprehend the severity of a situation due to the low-risk environment leading to inaccurate results. Imitation studies provide real-world situations where subjects can fully immerse themselves in the situations; however, they are difficult to proctor and time-consuming to create. Furthermore, the ethical dilemma of deceiving and testing subjects without their knowledge is also an issue. Lastly, lab experiments offer a controlled environment with well-defined boundaries, but subjects may become hyper-aware of the fact they are participating in a study which may also introduce bias.

1.3 Social Engineering and Personality

Personality traits and Social Engineering have been thought to be related due to how our personality may influence our susceptibility to persuasion and manipulation [14].

Existing studies suggest that individual personality traits may indicate higher susceptibility to SE and email phishing [2, 7, 8, 9]. However, results from these studies show conflicting conclusions as to which personality traits correspond with higher levels of SE vulnerability. For example, Cusak and Adedokun [9] found that agreeableness and extraversion were indicators SE vulnerability, Halevi et al. [7] concluded that individuals with high levels of neuroticism were more susceptible to phishing, and Alseadoon et al. [8] concluded that individuals with higher levels of openness, extraversion, and agreeableness were more susceptible to phishing. One study also suggests a "Social Engineering Personality Framework" based upon the Big Five personality traits [13].

1.4 Big Five Personality Traits

The Big Fiver Personality Traits are a taxonomy of personality traits distributed amongst 5 categories: extraversion, agreeableness, openness, conscientiousness, and neuroticism [6]. Characteristics of each trait are as follows:

- Extraversion: positive emotions, activity, sociability, assertiveness [6,14].
- Agreeableness: trust, compliance, modesty, and kindness [6.14].
- Openness: creativity, fantasy, and openness to different experiences 6,14].
- Conscientiousness: self-discipline, order, goal-directed behavior, and impulse control [6,14].
- Neuroticism: anxiety, self-consciousness, depression, and vulnerability [6,14].

1.5 Goals and Research Questions

The first step to combat and decrease the effectiveness of Social Engineering is to understand why people are vulnerable to it. As Social Engineering seeks to manipulate and deceive individuals, it is logical to ask questions of whether our personality and augmented cognition plays a role in our vulnerability to it. Therefore, the goal of this study is to better understand the relationship between our augmented cognition and our vulnerability to Social Engineering cyber attacks. Results and deliverables from this study may benefit future Social Engineering researchers and our overall security posture against Social Engineering attacks. To achieve these goals, this study aims to answer the following research questions (RQs):

1. What relationship, if any, exists between personality traits and Social Engineering vulnerability?
2. What relationship, if any, exists between personality traits and the speed at which an individual makes cybersecurity-related decisions?

2 Methods

To achieve the goals described by RQ1 and RQ2, a survey was designed and administered online through Google Forms to undergraduate students in low-level Computer Science classes at the University of Hawaii at Manoa. The survey consisted of two parts: a security survey and a personality survey. The survey results were then statistically analyzed to produce quantitative results about the relationship between personality traits and Social Engineering vulnerability and the time it takes to make cybersecurity decisions.

2.1 Security Survey Design

The security survey consisted of 22 scored questions designed to measure an individual's susceptibility and vulnerability to Social Engineering. This section of the survey consisted of 3 types of questions. The first question type was related to "situational awareness" and Social Engineering techniques. These questions began by presenting a cybersecurity situation and subjects would answer questions regarding how they felt about the situation and what they would do. Figure 1 depicts an example of a fake email presented in the security survey–a phishing email.

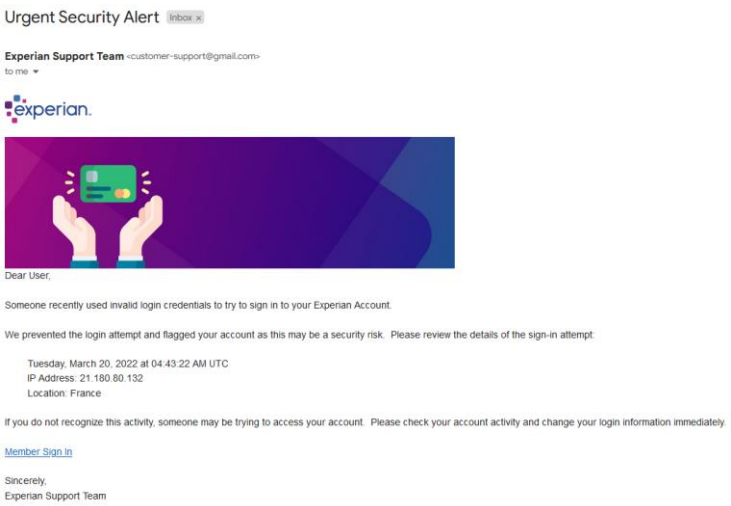

Fig. 1. Example Security Situational Question

The subject line, name of the sender, and the body of the email seem to be a normal security email; however, the sender's email address is "customer-support@gmail.com" which would not be the case if this email was truly from Experian. The subject would then be presented with statements such as "I would click the link" where they respond on a Likert scale. During this section of the survey, subjects were also asked to input their start time at before reviewing the question and their end time after completing each question. Time measurements were self-reported via a

stopwatch application, www.timertab.com. In total, the survey consisted of 4 “fake” situations and 2 controls. The second type of security question was the “general security” questions. These were simple questions about the subject's general security practices. An example general security question was “When downloading files, I make sure to verify the download source and file content before opening it” where they would again respond to a Likert-scale question. The third type of security question was the “short answer” questions. Short answer questions asked the subject for further explanations of their reasonings and thoughts on the situational and general security questions. These questions were intended to be used as additional qualitative data or for future research.

2.2 Personality Survey Design

The personality section of the survey used the publicly available Big-Five Personality Inventory [6]. The Big-Five Personality Test is a 44-item survey that asks subjects to respond to questions about their personality and behavior on a Likert scale between 1 and 5. An example question from the Big-Five Personality Inventory is “[I am] full of energy”.

The total score of a given survey was calculated by adding the numerical values of each answer. For the security survey, the answer “strongly disagree” corresponded to 1, “disagree” corresponded to 2, “neutral” corresponded to 3, “agree” corresponded to 4, and “strongly agree” corresponded to 5. For both the security and personality surveys, certain questions were marked for inverse scoring. For any inverse score question, the inverse of the subject’s answer would be added instead when tallying the final score. For example, if the subject answered with 5, 1 would be added to the score instead, if a subject answered with 4, 2 would be added. In addition to summing the answers, the time taken to analyze each situation and answer each section in the “situational security” section was also summed and used as a time total in the analysis.

Fifteen of 22 questions from the security survey were counted towards the final survey score due to restrictions of using some statistical analysis methods on Likert scale answers [14]. Due to these restrictions, only answers on a 5-point scale were counted; answers on a 2, 3, or 4-point scale were ignored in this analysis. This is a threat to validity is a limitation of the study. This will be discussed further in the Threats to Validity section.

3 Results

The survey was administered over one week and received 79 total responses. Figure 2 depicts the distribution of security scores, Figure 3 depicts the distribution of time totals, and Figure 4 depicts the distribution of the Big Five Personality Traits. Visually, the security scores, extraversion, and neuroticism follow relatively normal distributions, the security scores are positively skewed, and agreeableness, conscientiousness, and openness appear negatively skewed.

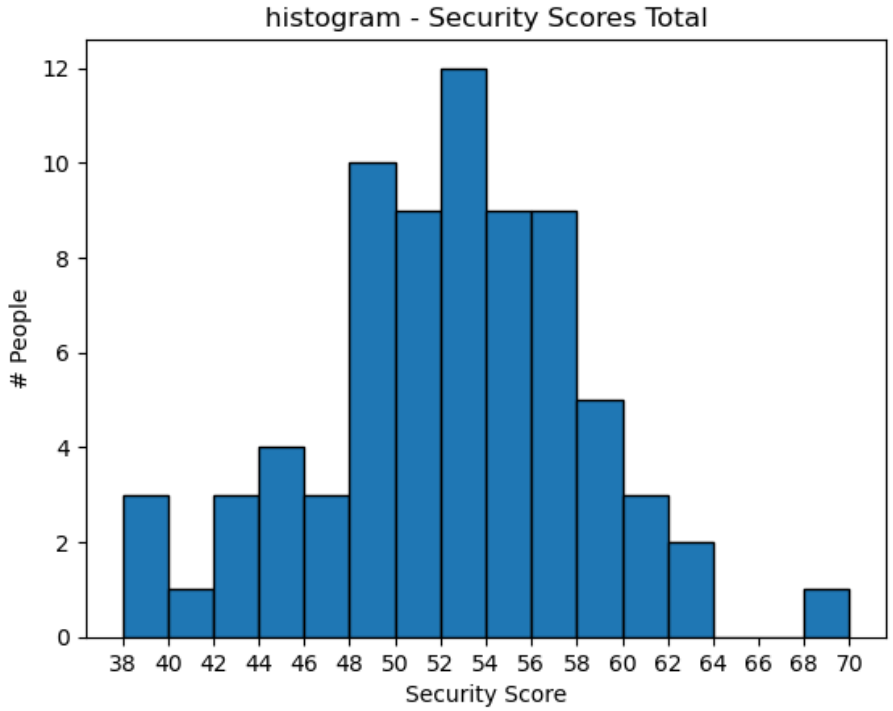

Fig. 2. Security Score Totals

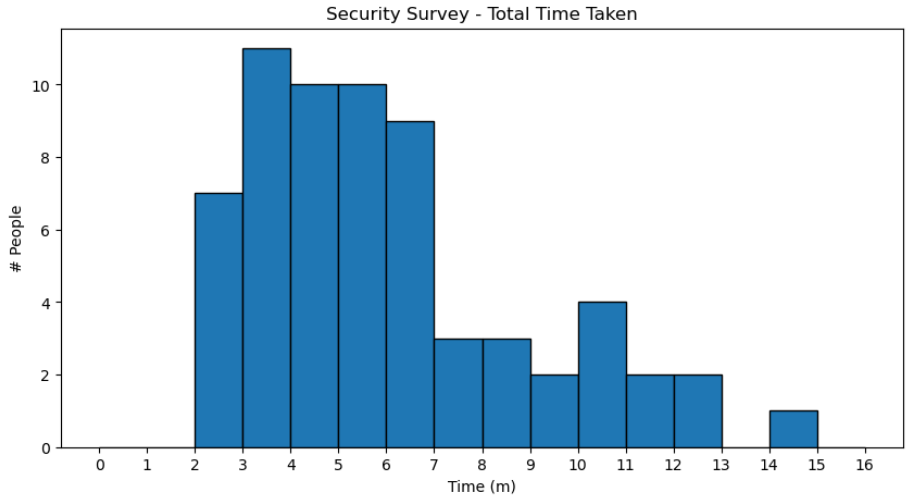

Fig 3. Time totals

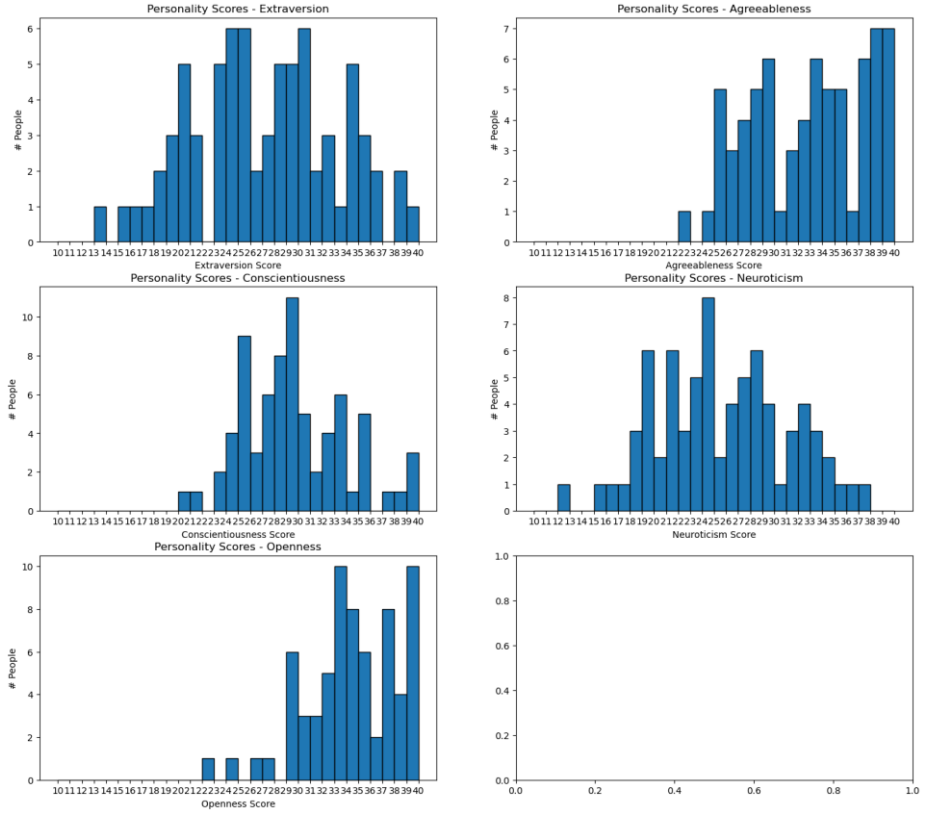

Fig 4. Big Five Personality Scores

3.1 Analysis

The goal of this analysis was to determine whether a statistically significant relationship existed between security/time scores and individual personality scores. To achieve this, subjects were split into 4 groups corresponding to the 4 quartiles of individual personality trait scores. Figure 5 illustrates these four group's security scores as they relate to the extraversion personality trait, and Figure 6 shows the same group's time totals as they relate to the extraversion personality trait. Each personality trait was analyzed independently of each other; thus the subject group distributions vary depending on the personality trait. The following analysis will only show examples of the extraversion personality trait due to space constraints; however, the rest of the graphs for the other personality traits can be found in the replication package [5].

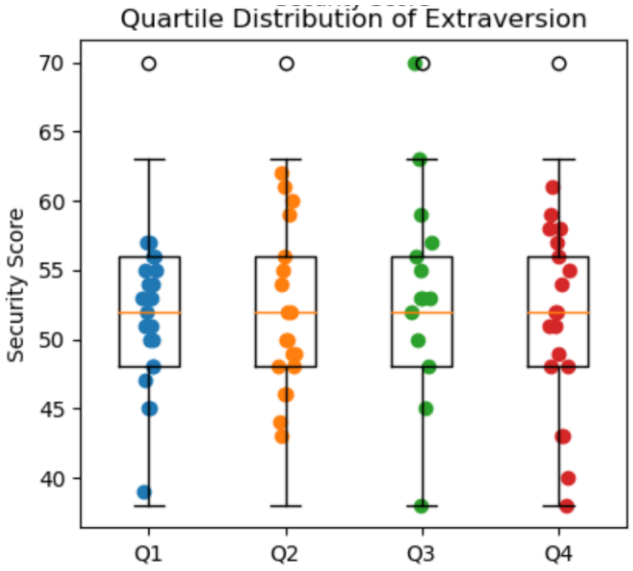

Fig. 5. Security Score vs. Extraversion Quartile Distribution

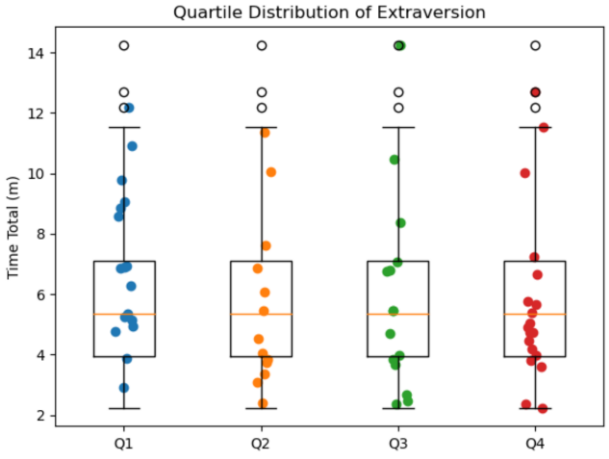

Fig. 6. Time Total vs. Extraversion Quartile Distribution

The security scores and time totals from quartiles 1 and 4 were then tested with the Mann-Whitney U Test and the Pearson Correlation Coefficient to determine whether a statistical difference existed between the two groups. The statistical test results of the two groups can be seen in Table 1 and Table 2. The results of the U-test and P-test show that there was no statistical difference and significance between security/time scores and each of the Big Five Personality Traits as all p scores were greater than 0.05.

Table 1. Security Score Vs. Personality Score Tests

Test	Extraversion	Agreeableness	Openness	Conscientiousness	Neuroticism
Mann Whitney U	u=218	u=249.5	u=178.5	u=196	u=186
	p=0.824	p=0.607	p=0.301	p=0.724	p=0.724
Pearson Correlation	r=0.0167	r=0.00988	r=-0.0146	r=0.0355	r=-0.0208
	p=0.874	p=0.835	p=0.806	p=0.956	p=0.756

Table 2. Time Vs. Personality Score Tests

Test	Extraversion	Agreeableness	Openness	Conscientiousness	Neuroticism
Mann Whitney U	u=107	u=215.5	u=133	u=191.5	u=176
	p=0.0871	p=0.0936	p=0.375	p=0.543	p=0.232
Pearson Correlation	r=-0.0203	r=-0.0266	r=-0.0314	r=0.00697	r=-0.0396
	p=0.888	p=0.933	p=0.901	p=0.764	p=0.861

4 Discussion and Augmented Cognition Applications

The analysis of the survey results show that no statistical difference exists between the security scores and time totals for high and low scorers of individual personality traits ($p>.05$). However, the Mann-Whitney U test highlighted a $p<.1$ for Extraversion and Agreeableness when compared to time. The data is trending towards a significant relationship between time and these factors.

Although no statistically significant relationships were found for both RQ1 and RQ2, the trend towards time spent and personality test scores (Extraversion and Agreeableness) should be further explored. The general conclusion is in contradiction to prior research on this topic [2, 4, 13] that each found at least one of the Big Five Personality Traits to have a significant relationship to Social Engineering vulnerability.

4.1 Threats to Validity

The largest threat to the validity of this study is the self-created security survey. Two aspects of the survey that may have contributed to the "no statistically significant relationship" findings are general survey design and the choice to use a survey over other security vulnerability-measuring methods. Various aspects of the survey could have been designed for additional accuracy and precision. First, was the choice to create questions with non-Likert scale responses. Performing statistical analysis methods used in this study on Likert scale questions requires all questions to be on the same Likert scale [12]. This caused 7 of the 22 security questions to be discarded which may have affected the individual security scores of the subjects. Second, the method to measure elapsed time while taking the survey was variable. Times were self-reported and used a third-party tool instead of automation or time-stamp collection. This was generally a limitation of the survey medium–Google Forms–but nevertheless introduced non-precise time measurements. This was seen in the survey responses themselves as user-input error was available for some in the time fields. In the future, a different survey

medium with automated time-stamp collection for individual question responses would decrease the error.

The choice to conduct a survey over a closed-lab experiment or a full immersion test may have also led to variations in level of Social Engineering vulnerability. As discussed in the Methods section, the self-reporting nature of surveys have different affordances and limitations compared to other mediums.

4.2 Future Work

There are many opportunities for future research including a deeper of analysis of additional personality traits and the refinement of instrumentation. Although the Big Five Personality Traits did not initially yield statistically significant results, there was a lead for Extraversion and Agreeableness when comparing time and personality traits. This research approach can be combined with additional personality factors such as locus of control (internal/external) to determine if these may further delineate differences between groups. It is surmised that additional factors such as these aligned with time, security score, and the interaction between time and security score may provide evidence of additional findings.

Many of the lessons learned and discussed in the Threats to Validity section can be implemented in future research on Social Engineering vulnerability. Implementing a closed-lab or full immersion study using more accurate measuring mediums would greatly improve the validity of the work and may help achieve the goal of improving our overall security posture. Overall, performing this study again would be beneficial. Other studies that focus on qualitative data rather than quantitative would also be intriguing as none of the qualitative data collected from this study was used in answering the research questions.

4.3 Conclusion

To help reduce the effectiveness of Social Engineering we must first ask what within ourselves makes us so vulnerable to it. One school of thought is that our cognition–more specifically the Big Five Personality Traits–can help measure one's vulnerability to Social Engineering attacks. However, this study highlighted the importance of exploring factors beyond the Big Five Personality Traits and such as locus on control and their interactions to attain fine-tuned results. The goal of this study was to determine whether our personality traits could be used in such a way, or not. Although this study showed that our personality traits were not significantly related to our Social Engineering vulnerability; it highlighted the potential for future research by expanding the factors and analysis methods. Future works in this field may take away the lessons learned from this study to illuminate new pathways for augmented cognition Social Engineering research.

5 Acknowledgements

This material is based upon work supported by the National Science Foundation (NSF) under Grant No. 1662487. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

References

1. Abraham, Sherly, and InduShobha Chengalur-Smith. "An Overview of Social Engineering Malware: Trends, Tactics, and Implications." *Technology in Society*, vol. 32, no. 3, 2010, pp. 183–196., https://doi.org/10.1016/j.techsoc.2010.07.001.
2. Albladi, Samar Muslah, and George R. Weir. "User Characteristics That Influence Judgment of Social Engineering Attacks in Social Networks." *Human-Centric Computing and Information Sciences*, vol. 8, no. 1, 2018, https://doi.org/10.1186/s13673-018-0128-7.
3. Chetioui, Kaouthar, et al. "Overview of Social Engineering Attacks on Social Networks." *Procedia Computer Science*, vol. 198, 2022, pp. 656–661., https://doi.org/10.1016/j.procs.2021.12.302.
4. Cusack, Brian, and Kemi Kemi . "The Impact of Personality Traits on User's Susceptibility to Social Engineering Attacks." *Australian Information Security Management Conference*, 2018, https://doi.org/10.25958/5c528ffa66693.
5. J. Imanaka, "Replication Package", https://github.com/jimanaka/personality-traits-as-predictors-for-social-engineering-vulnerability
6. John, O. P., & Srivastava, S. (1999). The Big-Five trait taxonomy: History, measurement, and theoretical perspectives. In L. A. Pervin & O. P. John (Eds.), Handbook of personality: Theory and research (Vol. 2, pp. 102–138). New York: Guilford Press
7. Halevi T, Lewis J, and Memon N (2013) Phishing, personality traits and Facebook. arXiv Prepr. arXiv1301.7643
8. I. Alseadoon, M. F. I. Othman, and T. Chan, "What Is the Influence of Users' Characteristics on Their Ability to Detect Phishing Emails?," *Lecture Notes in Electrical Engineering*, pp. 949–962, Nov. 2014, doi: https://doi.org/10.1007/978-3-319-07674-4_89.
9. K. Arif, and E. A. Janabi. "Social Engineering Attacks." *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, vol. 4, no. 6, June 2017.
10. K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *Journal of Information Security and Applications*, vol. 22, pp. 113–122, Jun. 2015, doi: https://doi.org/10.1016/j.jisa.2014.09.005.
11. P. Finn and M. Jakobsson, "Designing ethical phishing experiments," *IEEE Technology and Society Magazine*, vol. 26, no. 1, pp. 46–58, 2007, doi: https://doi.org/10.1109/mtas.2007.335565.
12. S. Gail M., and A. R. Artino. "Analyzing and Interpreting Data from Likert-Type Scales." *Journal of Graduate Medical Education*, vol. 5, no. 4, 2013, pp. 541–542., https://doi.org/10.4300/jgme-5-4-18.

13. U. Sven and S. Quiel. “The Social Engineering Personality Framework.” *2014 Workshop on Socio-Technical Aspects in Security and Trust*, 2014, https://doi.org/10.1109/stast.2014.12.
14. Z. Wang, H. Zhu, and L. Sun, “Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods,” *IEEE Access*, vol. 9, pp. 11895–11910, 2021, doi: https://doi.org/10.1109/access.2021.3051633.