2018

The impact of personality traits on user's susceptibility to social engineering attacks

Brian Cusack

Kemi Adedokun

DOI: 10.25958/5c528ffa66693

Cusack, B., & Adedokun, K. (2018). The impact of personality traits on user's susceptibility to social engineering attacks. In *proceedings of the 16th Australian Information Security Management Conference* (pp. 83-89). Perth, Australia: Edith Cowan University

THE IMPACT OF PERSONALITY TRAITS ON USER'S SUSCEPTIBILITY TO SOCIAL ENGINEERING ATTACKS

Brian Cusack, Kemi Adedokun
Cyber Forensic Research Center, Auckland University of Technology, New Zealand
brian.cusack@aut.ac.nz, kemi.adedokun@aut.ac.nz

Abstract

Phishing attacks and other social manipulation attacks are an everyday occurrence for most workers in their email boxes. Others experience social engineering tricks to take and divert payments on legitimate electronic commerce transactions. This exploratory pilot study aims to examine the impact of user's personality on the likelihood of user's susceptibility to social engineering attacks. Five expert interviews were conducted to investigate what traits makes some individuals more or sometimes less susceptible to social engineering attack than others. The personality traits were obtained using the big five personality model for correlation with interview data. The result suggests that users with high scores in agreeableness and extroversion traits are likely to be more susceptible to social engineering attack than others. These results are a useful start for further research into the impact of different tricks on different personality types.

Keywords
Social engineering, Tricks, Personality Type, Vulnerability, Countermeasures

INTRODUCTION

Social engineering (SE) is a term generally used to describe the act of manipulating people to access information. It is the process of deceiving people to inadvertently perform an action that can cause harm or increase the probability of causing future harm (Stewart & Dawson, 2018, p. 188). Hadnagy in his view on social engineering, described it as "the art or better yet, science, of skilfully manoeuvring human beings to take action in some aspect of their lives" (Hadnagy, 2010, p. 10). Krombholz et al. described it as the process of manipulating users to compromise the information system (Krombholz, Hobel, Huber, & Weippl, 2015, p. 114). SE is a unique form of cyberattack which involves hacking humans through technology and the art of psychology of human behaviour to gain unauthorized access into an information system (Campbell, 2018, p. 1). While hackers target loop holes in technology, social engineers manipulate humans to access information that cannot be easily accessed. Social engineers exploit human feelings and thoughts through fear, curiosity, greed and sympathy (Alexander, 2016). They capitalize on the psychology of people's expect and tendency to help others (Jones, 2004, p. 3). SE attacks come in various forms ranging from telephone calls and email requesting personal information from what appears to be a legitimate source or text message (Parrish Jr, Bailey, & Courtney, 2009, p. 286). There are two main types of SE attacks, the targeted and target of opportunity (Bullée, Montoya, Pieters, Junger & Hartel, 2018). A targeted attack is the one in which the attacker is very specific in terms of the victim while a target of opportunity attack is the one in which the attacker distributes to a lot of people hoping to get response from as many victims as possible. SE usually involves two stages, the location, and the psychological method used. The location is where the attack takes place. This could be online, at work place or over the telephone. The second phase involves using different psychological methods to manipulate a victim. It includes exploitation of asserted authority, people's commitments and strong relationships. The exploitation can come in form of manipulating people's tendency to help, reciprocation, liking and similarity (Jones, 2004, p. 4). Irrespective of the method used, the goal of a social engineer is to gain access to desired information by manipulating the victim without the victim's awareness.

Information is of great importance to governments and organizations. There has been a rise in information security violations with attempts to get sensitive information by illegal access. Organizations invest a lot in technical solutions to prevent information theft. However, technical solutions have proven to be insufficient as users are often the weakest link in an information system (Mouton, Malan, Leenen, & Venter, 2014, p. 28). The human link is believed to be the weakest link in an information security system (Mitnick, Simon, & Wozniak, 2006, p. 12; Mouton, Leenen, Malan, & Venter, 2014, p. 186). Humans often react to emotions which makes them more vulnerable than machines (Mouton, et al., 2014, p. 267). Mouton also noted that an organization's biggest threat is not technical protection but the people working in the organization. Attackers find it easier to gain unauthorized access through people rather than penetrating the security system (Mouton, Leenen, et al., 2014, p. 267). Several organizations tend to use training solutions and raising awareness through warnings about social engineering attacks. These methods have generally been proven to be ineffective (Junger, Montoya, & Overink, 2017, p. 75).

This is likely because most training around social engineering are based on detecting electronic threats such as the phishing attack and avoiding malware downloads which can be easy to manage. However, the human-based social engineering attack which has been neglected poses more threats to the organization (Hadnagy, 2010). In this paper we report exploratory pilot study research into personality type as an antecedent for human behaviour and adopt the research question "What individual's personality traits is more susceptibility to social engineering attacks?" The following propositions were developed from the literature reviewed.

P1: Each personality trait of the big five model are susceptible to different types of social engineering attack.

P2: A user's personality trait will increase the user's susceptibility to social engineering attack.

BACKGROUND LITERATURE

Orgill et al. investigated user's susceptibility to SE attacks by posing as a computer support engineer from the organization asking for personal information such as username and passwords with the disguise of performing vulnerability auditing on the network. It was discovered that 80% of the people gave their username and 60% provided their password (Orgill, Romney, Bailey, & Orgill, 2004, p. 179). Also, the result showed that isolated users were easier to manipulate than those in groups. Furthermore, the effect of peer pressure and authority had significant influence on the likelihood of user's susceptibility to SE.

Bakshi et al. conducted an e-mail based social engineering attack study to raise awareness and assess the threat of social engineering attacks on IT systems (Bakhshi, Papadaki, & Furnell, 2009, p. 54). An experimental website was created and email with embedded link to website was sent out to employees. The result indicated that about 23 percent of the employees followed the link. A similar study by Jagatic et al. focused on phishing on social networks. The research was done on university students and the result indicated that the students were highly susceptible to fishing attack. Also, they found that females were more susceptible to phishing attacks than males (Salgado, J & Tauriz, 2014; Jagatic, Johnson, Jakobsson, Jakobsson, & Menczer, F., 2007).

The result of these studies shows how vulnerable an organization can be to social engineering attacks. One of the ways to deal with social engineering attacks is to understand why individuals fall for this attack and then to provide training as a countermeasure. A successful SE attack can be determined by the extent to which the victim is able to resist manipulation or be able to detect the attack (Uebelacker & Quiel, 2014, p. 25). One of the ways of understanding what qualities makes people more susceptible to SE attacks more than others is in using behavioural or personality models. Personality models help to understand what makes people think and respond the way they do. Personality from a psychological perspective is defined as a state when a person's thoughts, feelings and behavioural patterns are relatively stable (Uebelacker & Quiel, 2014, p. 25). Understanding the relationship between individuals and information security is particularly useful in forecasting an individual's ability to maintain information security standards and policies (Shropshire, Warkentin, Johnston, & Schmidt, 2006, p. 3435). There are multiple approaches to personality dimensions. Several models have been developed to identify different types of personality traits such as the Five Factor Model (the Big five). The Big five is one of the most widely used theoretical models and has received more attention than other options in the literature (Matz, Chan, & Kosinski, 2016, p. 36; Salgado & Tauriz, 2014, p. 3). The big five is coherent and scientific as it defines personalities along a continuum rather that in categories or types. It gives room for different types of behaviour in different circumstance. The big five tests determine personality traits using Openness to experience, Conscientiousness, Extraversion, Agreeableness, and Neuroticism referred to as OCEAN (Roccas, Sagiv, Schwartz, & Knafo, 2002, p. 792). Table 1 briefly describes the big five traits.

Table 1. Characteristics of Big five personality traits (Adapted from Matz et al., 2016, p. 42; Stidham, Summers, & Shuffler, 2018, p. 2147)

Traits	**Facets of high score**	**Facets of low score**
Openness to experience	Intellectual, imaginative, outgoing. Seeks novelty	Practical, conventional, skeptical, rational
Conscientiousness	Organized, self-directed, thorough, dependable, but controlling	Disorganized, careless, can be prone to addiction

Extraversion	Outgoing, enthusiastic, active; seeks novelty	Aloof, quiet, independent; cautious, withdrawn
Agreeableness	Trusting, straightforwardness, empathetic, compliant, affable	Uncooperative, hostile; unempathetic
Neuroticism	Prone to stress, anxious, self-consciousness, moody, impulsivity	Emotionally stable, calm and secured.

TEST SET UP

A researcher's perspective and assumptions of what constitutes truth and knowledge constructs the way we see ourselves, other people and the society around us. These views and beliefs are referred to as a paradigm (Cypress, 2017). Schwandt defined paradigm as a shared world view that represents the beliefs and values in a discipline and that guides how problems are solved. A paradigm can help clarify research questions and help in research design. This research will employ a qualitative non-experimental method to answer the research question. The methods fit context-based research that will provide insight into and allow capturing other people's perspective of real-life situations. A qualitative research approach is best suited for a study that serves the purpose of description, interpretation, verification, and evaluation of behaviour (Peshkin, 1993). Also, qualitative research generally seeks to answer the what, how and why question rather than how much or how many (Cypress, 2017). This best suits this study where a constructivism approach has been chosen with the underlying view that there is no single reality to be found, and knowledge is gained interactively (Chilisa & Kawulich, 2012, p. 9).

Data is collected through a purposive, semi-structured, expert interview. Interview methods give voice to people, which allows them to freely present their life situations in their own words, and provide personal interaction between the researchers and their subjects (Kvale, 2006, p. 481). Also, interview research methods are more powerful tools for obtaining narrative data that allows researchers to investigate people's views in greater depth compared to questionnaires and surveys. In particular, expert interview is concerned about the participant's knowledge and experiences as a result of their actions, roles, responsibilities or obligations within a specific organization or institution (Littig & Vienna, 2013). Expert interviews are more efficient and concentrated way of gathering quick quality data than using observation and surveys (Bogner, Littig, & Wolfgang, 2009, p. 3). An expert in this sense is a person with insight in aggregated or specific knowledge (Albladi & Weir, 2018). Also an important consideration in qualitative research is determining the sample size. The determination of qualitative sample size is challenging one that is based on different study designs and contextual considerations (Turner-Bowker et al., 2018, p. 842). Contrary to a quantitative research approach where the sample size can be calculated using statistical techniques, qualitative sample size is calculated by the number of participants that will be needed to attain saturation (Glaser, Strauss, & Strutzel, 1968, p. 61). The concept of saturation emerges when no more data are being found. In this study the number five was chosen from participants who had experienced on social engineering attack, and hence were classed knowledgeable of the phenomena and hence a quicker saturation point was reached for the pilot study. The thematic analysis was conducted using the NVIVO software.

RESULTS

The interview and trait data was thematically analysed in NIVO and is presented in the following two tables. Table 2 presents an overview of the factors identified by participants that made them susceptible to SE attacks based on their experience as a victim. Table 3 shows their personality traits.

The findings present some contradictions to the previous findings reported, for example, McCormac et al., 2017; Shropshire et al., 2006, p. 3446, regarding which personality trait is more prone to SE attack. Participant one believed the attack was successful because of a trusting relationship, love, or humour as a motivating factor. These findings are indications of extraversion and agreeableness traits which agrees with the participants personality result. Participant two believed it was desperation of finding a job and trust in other people's feedback that made the SE attack successful. These traits are indications of conscientiousness and agreeableness. However, the participant's personality test result does not indicate that. The third participant believed it was the fear of being locked out of personal account and not having access to money as well as lack of training and proper education as at that time that made the SE attack successful. These traits are indications of agreeableness and neuroticism. The participant believes in compliance and being loyal as well as fearful of losing personal money. This does not totally agree with the personality result. The fourth participant believed it was pressure from authority, the ease and comfort as well as cost savings that made the SE attack successful. These are indications of agreeableness and

conscientiousness. This is also contrary to the result from the participant's personality test. The last participants indicated that money, curiosity and trusting positive feedback from others that led to the successful SE attack. These traits are indications of openness, extroversion and agreeableness which are in line with participant's result. From this study and the scenarios examined, the findings indicate that personality traits can determine the likelihood of SE attack and users with some type of personality are more susceptible than others. While people with high score in *agreeableness* and *extroversion* trait are likely to be more susceptible to SE attack, the likelihood of a successful SE attack is not only dependent on the personality trait, it depends on the user's circumstance and the attack technique of the attacker. Though some types of personality traits have the tendency to be easily manipulated, if the attacker does not motivate them, the chances of a successful attack is low. Also, the result indicated that people that are more trusting will likely be more susceptible because once your trust level increases, your guard falls. Overall, it is believed that SE attack is usually a targeted attack, and people who score high in *agreeableness* and *extroversion* are likely to fall victims more than other personality traits.

Table 2. Participant's view of what made them susceptible to SE attack

Participants	Attacker's technique	Curiosity	Desperation	Ease and comfort	Fear	Humor	Lack of education and training	Money	Personality	Positive feedback from others	Pressure from authority	Sense of urgency	Time, chance & technique	Trusting relationship
P1	✓	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✓	✓
P2	✗	✗	✓	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✓
P3	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✗	✓	✗	✗
P4	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✓	✓	✓	✓
P5	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✓	✗

In answer to Proposition 1: One of the participants suggested that lack of training and education is the main factor enhancing user's susceptibility to social engineering attacks. It was believed that if users understand the traits to look out for irrespective of the technique used, the likelihood of susceptibility to SE attack will be reduced. Two of the participants believed it's the user's motivating factor that matters irrespective of technique that is been used if the user is not motivated the trick will not work on them. Two other participants supported that it's a synergy of the user's motivating factor, attacker's technique and chance. All the participants believed that personality is one of the reasons why people fall victim of social engineering attack. Considering social engineering attack is a targeted attack which means the social engineers knows the class of people they want which are likely to fall victim. This brings in personality profile. Drawing from the data analysis, it was stated that the factors which serves as the motivation can vary from time to time depending on the user's situation, however, the user's personality is expected to be relatively constant. As this study is focused on examining the personality trait that is more susceptible to SE attack the personality test followed the interviews. After the participants each explained the scenarios where they've been a victim of a social engineering attack and why they think things made them susceptible. Then they were asked to take the big five personality test.

Table 3. Participant's big five personality test (P=Participant; #= thematic occurrence)

Participants	Openness	Conscientiousness	Extraversion	Agreeableness	Neuroticism
P1	**93** (Enjoy novel experiences, see	**98** (Well-organized and reliable)	**92** (Extremely outgoing social and energetic)	**88** (Trusting, good-natured,	**9** (Remains calm even in

	things in new ways)			courteous, & supportive)	tense situations)
P2	**84** (Enjoy novel experiences, see things in new ways)	**98** (Well-organized and reliable)	**56** (Neither social or reserved)	**51** (Neither extremely trusting, forgiving or irritable)	33 (Generally relaxed)
P3	**28** (Somewhat conventional)	**80** (Well-organized and reliable)	**63** (relatively social and enjoy the company of others)	**54** (Trusting, good-natured, courteous, & supportive)	**21** (Generally relaxed)
P4	**59** (don't seek out new experiences)	**92** (Well-organized and reliable)	**30** (shy away from social situations)	**24** (Less trusting, express irritation with others)	**32** (Generally relaxed)
P5	**80** (Enjoy novel experiences, see things in new ways)	**93** (Well-organized and reliable)	**85** (Extremely outgoing social and energetic)	**82** (Neither extremely forgiving or irritable)	**29** (Generally relaxed)

In answer to Proposition 2: while the incident rate of social engineering attacks continues to increase, the need to understand what makes people vulnerable to this attack is imperative. Social engineers build their attack scenarios based on personality profiles. Several attempts have been made to prevent these attacks with the use of technical solutions and raising awareness through warnings about social engineering attacks. However, these methods have generally been proven to be ineffective (Junger et al., 2017, p. 75). This purpose of this study was therefore to examine what personality trait makes users more susceptible to SE attack. These data were gathered from experiences of participants who understand how social engineering works and have once been a victim of a SE attack. Several user's motivating factors were identified and the personality traits with the likelihood of increased susceptibility determined. The result is intended to contribute to the body of knowledge by informing individuals and organizations the kind of personality trait that are more prone to SE attacks, this in turn provides a basis for identifying possible SE techniques and initiating effective solutions through the decision making of user's who are more susceptible to social engineering attack.

CONCLUSION

The field of social engineering clearly needs further research especially in identifying the user's susceptibility and to aid effective countermeasures. As the social engineering techniques become more sophisticated and the incident rate increases, it is important to provide effective measures. One of the potential measures is in examining a user's susceptibility. When the users are aware of their SE vulnerability, organizations will be able to measure their risk to social engineering and employ effective measures to counter these attacks according to the distinct identified user's weakness. Several studies have focused on testing the rate of the user's susceptibility through phishing techniques. However, most of these studies have not focused on what attributes makes the user act the way they act. While there is literature focusing on the relationship between the user's personality traits and their susceptibility rate to SE attack, there is a discrepancy in existing literature on what individual personality traits make users susceptible to attack. The results reported in this paper suggest that users with high scores in agreeableness and extroversion traits are likely to be more susceptible to social engineering attack than others. We also identified moderating variables that included emotional state, the environment and motivations. These results are a useful start for further research into the impact of different social engineering attacks on different personality types. This has been an exploratory pilot study that has located the variables and focus for a quantitative exploration of the issue.

REFERENCES

Albladi, S. M., & Weir, G. R. S. (2018). "User characteristics that influence judgment of social engineering attacks in social networks". *Human-centric Computing and Information Sciences*, 8(1). https://doi.org/10.1186/s13673-018-0128-7

Alexander, M. (2016). "Methods for understanding and reducing social engineering attacks". SANS Institute.

Bakhshi, T., Papadaki, M., & Furnell, S. (2009). "Social engineering: assessing vulnerabilities in practice". *Information Management & Computer Security*, 17(1), 53-63.

Bogner, A., Littig, B., & Wolfgang, M. (2009). "Introduction: Expert Interviews — An Introduction to a New Methodological Debate". (pp. 1-13). https://doi.org/https://doi.org/10.1057/9780230244276_1

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). "On the anatomy of social engineering attacks—A literature- based dissection of successful attacks". *Journal of investigative psychology and offender profiling*. 15(1), 20-45.

Campbell, C. C. (2018). "Solutions for counteracting human deception in social engineering attacks". *Information Technology & People*. 17.

Chilisa, B., & Kawulich, B. (2012). *Selecting a research approach: paradigm, methodology and methods. Doing Social Research*, A Global Context. London: McGraw Hill.

Cypress, B. S. (2017). "Rigor or reliability and validity in qualitative research: Perspectives, strategies, reconceptualization, and recommendations". *Dimensions of Critical Care Nursing*, 36(4), 253-263.

Glaser, B. G., Strauss, A. L., & Strutzel, E. (1968). "The discovery of grounded theory; strategies for qualitative research". *Nursing Research*, 17(4), 364.

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons, New York.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., Jakobsson, M., & Menczer, F. (2007). "Social Phishing". *ACM*, 50(10), 94-100. https://doi.org/10.1145/1290958.1290968

Jones, C. (2004). "Social Engineering: Understanding and Auditing". GSEC, SANS Institute.

Junger, M., Montoya, L., & Overink, F.-J. (2017). "Priming and warnings are not effective to prevent social engineering attacks". *Computers in Human Behaviour*, 66, 75-87.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). "Advanced social engineering attacks". *Journal of Information Security and Applications*, 22, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

Kvale, S. (2006). "Dominance through interviews and dialogues". *Qualitative Inquiry*, 12(3), 480-500.

Littig, B., & Vienna, I. (2013). Expert Interviews. Methodology and Practice. IHS Vienna, IASR lecture series, Vienna.

Matz, S., Chan, Y. W. F., & Kosinski, M. (2016). "Models of personality". In *Emotions and Personality in Personalized Services* (pp. 35-54): Springer.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). "Individual differences and information security awareness". *Computers in Human Behaviour*, 69, 151-156.

Mitnick, K. D., Simon, W. L., & Wozniak, S. (2006). *The Art of Deception: Controlling the Human Element of Security.* Paperback ISBN 0-471-23712-4.

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). "Social engineering attack framework". IEEE Symposium conducted at the meeting of the Information Security for South Africa (ISSA).

Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. (2004). "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems". ACM Symposium conducted at the meeting of the Proceedings of the 5th conference on Information technology education

Parrish Jr, J. L., Bailey, J. L., & Courtney, J. F. (2009). "A personality based model for determining susceptibility to phishing attacks". Little Rock: University of Arkansas, 285-296.

Peshkin, A. (1993). "The goodness of qualitative research". *Educational Researcher*, 22(2), 23-29.

Roccas, S., Sagiv, L., Schwartz, S. H., & Knafo, A. (2002). "The Big Five Personality Factors and Personal Values". *Personality and Social Psychology Bulletin*, 28(6), 789-801. https://doi.org/10.1177/0146167202289008

Salgado, J. F., & Tauriz, G. (2014). "The Five-Factor Model, forced-choice personality inventories and performance: A comprehensive meta-analysis of academic and occupational validity studies". *European Journal of Work and Organizational Psychology*, 23(1), 3-30.

Shropshire, J., Warkentin, M., Johnston, A., & Schmidt, M. (2006). "Personality and IT security: An application of the five-factor model". AMCIS 2006 Proceedings, 415.

Stewart, J., & Dawson, M. (2018). "How the modification of personality traits leave one vulnerable to manipulation in social engineering". *International Journal of Information Privacy, Security and Integrity*, 3(3), 187-208.

Turner-Bowker, D. M., Lamoureux, R. E., Stokes, J., Litcher-Kelly, L., Galipeau, N., Yaworsky, A., & Shields, A. L. (2018). "Informing a priori Sample Size Estimation in Qualitative Concept Elicitation Interview Studies for Clinical Outcome Assessment Instrument Development". *Value in Health*, 21(7), 839-842. https://doi.org/https://doi.org/10.1016/j.jval.2017.11.014

Uebelacker, S., & Quiel, S. (2014). "The Social Engineering Personality Framework". Presented at the meeting of the 2014 Workshop on Socio-Technical Aspects in Security and Trust, https://doi.org/10.1109/stast.2014.12