Novelty Journals

ISSN 2394-7349

International Journal of Novel Research in Engineering and Science
Vol. 9, Issue 2, pp: (27-34), Month: September 2022 - February 2023, Available at: www.noveltyjournals.com

Assessing the Mobile Money user's awareness on social engineering in Tanzania: Case of the Ministry of Information Tourism and Heritage Zanzibar

Yussuf Haji Juma

Institute of Accountancy Arusha
P.O. Box 69007, Dar es Salaam.

DOI: https://doi.org/10.5281/zenodo.7277453
Published Date: 03-November-2022

Abstract: **Social engineering is one of the most common attacking threats to the Mobile Money users during money Transactions. With the increasing rate of mobile money use, it has directly increased the number of social engineering incidents in mobile money services. It is therefore important to come up with the guidelines that will help the society to be more aware and to reduce the mobile phone criminals. As of now, some customers and other Mobile money users like agents have already lost thousands of shillings due to social engineering attacks.**

This study assesses the mobile money user's perception on social engineering. The primary data were used and collected by a questionnaire method of 407 populations with the 203 sample size, analyzed by using the SPSS tool and it is a descriptive analysis. Few of the reason founded that lead in social engineering attacks are as lack of security awareness, PIN sharing, PIN requests and storing PINs in address books were recognized as major sources of vulnerability in mobile money theft. The study revealed that, mobile money users level of awareness on social engineering were good and is caused by the good perceptions of the Mobile Money users in the extents that many of them use their Mobile Money accounts in a safe environmentsin the consideration of knowledge, behavior and the security metrics.

The study recommends that mobile money service provider, government and the normal Mobile Money users each have to play the role on fighting against social engineering attacks, like service provider to make security awareness program to the Mobile Money users has to make sure that the security and privacy policy are surely practiced. Furthermore normal Mobile Money users are advised to acquire professional knowledge, get educational trainings and form strong collaboration to fight against cybercrimes in general and social engineering particularly.

Keywords: **Social engineering, Mobile Malware, Social engineering attack.**

1. INTRODUCTION

Social engineering is the art of manipulating people so they give up confidential information. In then Social engineers clearly perform information gathering from the Mobile Money users, by developing some form of relationship with them, exploit the element of trust resulting on obtaining sensitive information that could fall in the wrong hands if proper controls are not taken. In the world we have, the social engineers take the advantages of the people using that mobile platform in their way mobile money transaction in the fact that people will always be the weakest link. But then assumption is as the number of Mobile Money Service Providers increasing day to day then the chances of the social engineering incidences

occurring on that Mobile Money users are also high. Those Mobile money users being the main victims of the theft , Social engineers uses different ways to lure those users some of the users of mobile money may be by calling and speaking as someone's you know voice or acting as a close family member and asking for money for a certain issue need to be done urgently for example got an accident and need money for paying somewhere for something example port to transport luggage , also the call and tell the Mobile Money users win the drawer so they have to follow the instruction to get their money package, in then they take that opportunity to commit crime.

Mobile money refers to virtual or electronic money stored using subscriber' Identity Module Card (Financial Action Task Force, 2013). The card acts as a unique identifier of the user account. The electronic money may be converted to physical money through a network of agents. Traditionally, Mobile phones were used for making voice calls and messaging services. However, in recent years the use of mobile phones has increased to include traditional banking activities (Agwu& Carter, 2014). Mobile phone users are able to access and transact through their wallet accounts. As the result, mobile phones provide people with an opportunity to virtually access banking services with minimum conditions (Masamila,2014).

Due to the fact, the existence of mobile Money usage is on everywhere either in Urban or Rural areas, so therefore Social Engineering has to be said as pervasive and wide issues around the World. Although fraud issues in the day to day life is not commonly reported, and for then it's still an existing threat. The Mobile Money users can and continue losing their money. Fraudsters are always on the lookout for innovative ways on how to steal from the Mobile Money users in the usage of non-technical methods like social engineering. This kind of attack mainly takes advantage of the human element of security.

2. LITERATURE REVIEW

2.1 Empirical Literature Review

The rapid growth of mobile money services acceptance has resulted into increasing number of variety forms of types of fraud. Mobile attacks have rapidly grown recently and promise to be the future of phishing (Nagunwa, 2014). Among such potential key fraud and security attacks to Mobile Money Services include social engineering. Some of the types of mobile money social engineering attacks are mobile malware, smishing, vishing, mobile phone phishing, impersonation of company officials and theft of mobile device (Subex,2012).

According to United Nations Conference on Trade and Development (2012) mobile money is used to refer to money stored using the Subscriber Identity Module (SIM) in a mobile phone as an identifier as opposed to an account number in conventional banking. It is value issued by Mobile Network Operator (MNO) and is kept in a value account on the SIM within the mobile phone that is also used to transmit transfer or payment instructions, while corresponding cash value is safely held in a bank. The balance on the value account can be accessed via the mobile phone, which is also used to transmit instant transfer or payment instructions.

2.1.1 Mobile Money Services in Tanzania

Commencement of mobile money services in Tanzania started in April 2008 when Vodacom launched its mobile money transfer platform, known as M- PESA. In the same year Zantel introduced its mobile payment service called Z-PESA where was upgraded and re-launched in 2012 as EzyPesa. Later on the service was also adopted by other mobile network operators. Zain launched Zap (now Airtel Money) in 2009 ,TigoPesa followed in 2010 (di Castri and Gidvani, 2014) and Halo Pesa launched in early of2016.

2.1.2 Social Engineering Attack

As previously stated, social engineering is all about influencing people to become interested in giving out classified information, or doing wrong actions without their consent. It is like a trap of acquiring someone's trust and confidence; in consequence people are defrauded after attaining their trust and confidence. Social engineering relies predominately on establishing and exploiting trust (Spinapolice, 2011). By means of generating trust with organization's staff, the attacker is capable of achieving confidential information that he or she would not obtain otherwise. The main purpose of social engineering attack is to obtain understanding or permission to gain access to information system.

Mobile Malware: The increasing attractiveness of smart-phones use in the world has led to the advancement of mobile services such as mobile payments, mobile banking and mobile money remittance. This makes mobile phones prone to criminals. Different types of malwares have been developed by Fraudsters to capture data from smart-phones. Mobile Malwares are designed to steal personal data from the phone and then transmit them to the attacker.

Smishing: It is also known as SMS Phishing. Smishing is a social engineering technique used by criminals to send deceitful and misleading text messages (Short Message Service –SMS) to the victim's mobile phone. The sender's aim is trying to take sensitive information such as passwords, mobile money PINs or credit card details of the recipient.

Shoulder Surfing: Looking over the shoulder of an individual as he types in his access code, password and PIN on a keypad for the purpose of committing this to memory so as to reproduce it later on (Allen,2007).

Reverse Social Engineering: The main aim of reverse social engineering is to get information by having the victim ask the questions rather than the attacker. Normally, when employing this type of attack, the attacker will disguise the person of an authority figure within the organization. Utilizing this authority characteristic can yield a great deal of information to the social engineer based on the questions asked by the victim.

Dumpster Diving: This involves searching through garbage of an individual or organization thrown away in order to obtain potentially useful information that should have been disposed of more secured place.

Phishing: It is the most common computer based form of social engineering. Phishing attacks search for the victim meaning the attacker is not waiting for the victim to come to him. These attacks normally extract on the friendliness and scarcity of human traits. Phishing attacks are attempted via a message, phone call, email and in person (McQuade,2006).

Vishing: Vishing or Phone Phishing is a social engineering technique that fraudsters use the telephone to lure customers into providing personal details to phishers. Victims are contacted by means of telephone and asked to provide sensitive information. This technique involves using voice over IP (VoIP) to imitate a legitimate sound of employee of a company that the customer trusts (Hall, 2012;Nagunwa,2014).

Smishing: It is also known as SMS Phishing. Smishing is a social engineering technique used by criminals to send deceitful and misleading text messages (Short Message Service –SMS) to the victim's mobile phone. The sender's aim is trying to take sensitive information such as passwords, mobile money PINs or credit card details of the recipient.

2.2 THEORETICAL LITERATURE REVIEW

A theoretical framework is a collection of interrelated ideas based on theories. It is a reasoned set of prepositions, which are derived from and supported by data or evidence. It attempts to clarify why things are the way they are based on theories. It is a general set of assumptions about the nature of phenomena (Kombo and Tromp, 2006). This study was guided by Theory of Deception (ToD) and Principles of influence.

2.2.1 Principle of Influence

According to Cialdini and Guadagno (2005) influence refers to the change in one's attitudes, behaviour, or beliefs due to external pressure that is real or imagined. Besides, there are principles recommended by Mitnick (2013) in his book The Art of Deception – Controlling the Human Element of Security. These principles explain why social engineering works. The book mentions some of human behaviors that Cialdini and Guadagno talk about They give explanations of the reasons why people react as they do on influence. They define six basic principles that force the tendency of human being. The following are six principles that derive the individual's influence and their description taken from Mitnick(2013).

Social Proof: People have the tendency to comply, when doing so appears to be in line with what others are doing. The action of others is accepted as validation that the behaviour in question is the correct and appropriate action.

Reciprocation: Humans may automatically comply with a request when they have been given or promised something of value. When someone has done something for another person, the person feels an inclination to reciprocate. This strong tendency to reciprocate exists even in situations where the person giving the gift hasn't asked for it i.e. willing to repay kindness with kindness.

Social Proof: People have the tendency to comply, when doing so appears to be in line with what others are doing. The action of others is accepted as validation that the behaviour in question is the correct and appropriate action.

Liking: People have a tendency to comply when the person making a request has been able to establish himself as likeable, or as having similar interests, beliefs, and attitudes as the victim.

Authority: A person can be convinced to comply with a request if he or she believes the requester is a person in authority or a person who is authorized to make such a request.

2.2.2 Theory of Deception

According to Grazioli (2004) "the Theory of Deception describes the information processing involved in both deceiving and detecting deception. It states that individuals detect deception by noticing and interpreting anomalies in their environment in light of the goals and capability for action that they ascribe to others with whom they interact. The interpretation process is triggered when individuals notice inconsistencies between their experience and their expectations about their experience". The procedure by which customers can discover deception is clarified by this theory. According to ToD, detection is a cognitive process that consists investigating different cues such as body language, tones and words. The four factor model reveals that people are disposed by four behaviours when they are lying which are arousal, attempted control, felt emotions and cognitive effort (DePaulo et al.,2003; Zukerman and Driver,1985).

The first behaviour is due to the fact that people become extra aroused or nervous when they are telling lies rather than when they are speaking truth. The second is due to the reason that people do not want to be caught when they are lying. They hardly try to control their behaviours when lying, in consequence some parts of the body give away the hidden deception. The third behaviour, emotion, exposes the criminals because the deceptive character is the companion of negative pessimistic emotions such as guiltiness and possibility of being caught. The last behavior is a cognitive effort.

This necessitates a liar to go on with his/her story wherever he/she goes. The liar is required to tell the same story as has already said. He/she must possess big and good memory. This situation will force the liar to take more time when responding to questions because of thinking what has been said before. Therefore, investigators look for cues that will direct them to know and conclude whether the received message is a deceptive one or not.

2.3 CONCEPTUAL FRAMEWORK

It presents the discussion of the research variables provided in a summary through a figure as shown below

Perceptions, (Parsons et al.,2017)

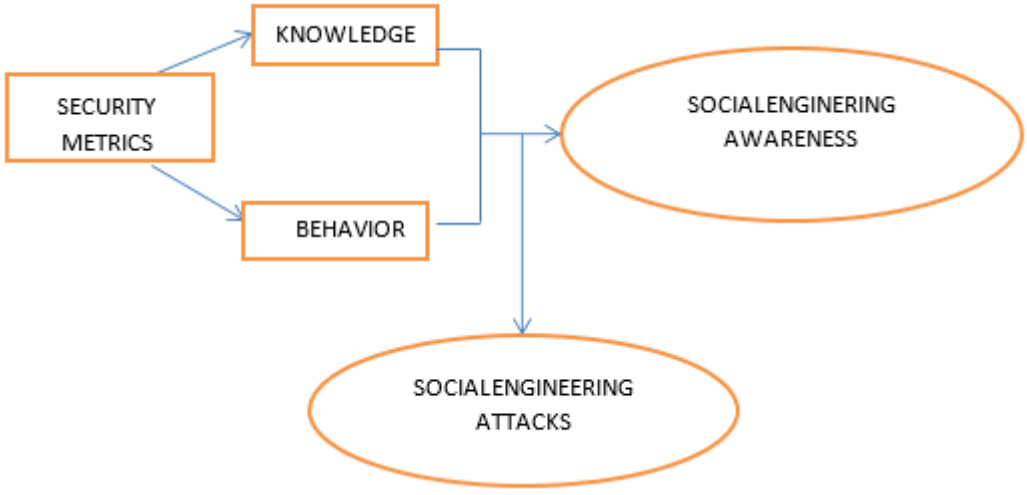


Figure 1: Conceptual Framework

International Journal of Novel Research in Engineering and Science
Vol. 9, Issue 2, pp: (27-34), Month: September 2022 - February 2023, Available at: www.noveltyjournals.com

3. METHODOLOGY

This chapter discusses the research design adopted, population targeted, the sample size of the research, the sampling techniques, data collection methods, data collection instruments, and data analysis techniques that were employed in the study.

Research design.

The quantitative approach was used in this study because of the specific objectives and the nature of the research problem.

Study Area.

The study was conducted in the United Republic of Tanzania, in Zanzibar Islands. It was specifically for the staffs of the Ministry of information Tourisms and Heritage.

Population

The Ministry of information Tourism and Heritage was chosen as a study area, and was consisting of 407 staffs.

Sample size

Yamane (1967), provides a simplified formula to calculate sample sizes. This formula was used to calculate the sample sizes of a known population. A 95% confidence level is assumed for a Yamane Equation.

$$n = \frac{N}{1 + N(e)^2}$$

Where

n is the sample size,

N is the population size, and

e is the level of precision and which is 0.05.

The total population of the study was 407. Then the number of the respondents calculated as

$$n = \frac{407}{1 + 407(0.05)^2} = 203 \text{ respondents}$$

The sample size of the study were 203 respondents.

Data Collection

This study used the questionnaire as a data collection instruments.

Data analysis

The data collection instrument were done with the use of Statistical Package for Social Sciences(SPSS), and it is descriptive analysis.

4. FINDINGS

This presents the general summary of the major findings as follows;

4.1 Mobile Money User's perception on social engineering.

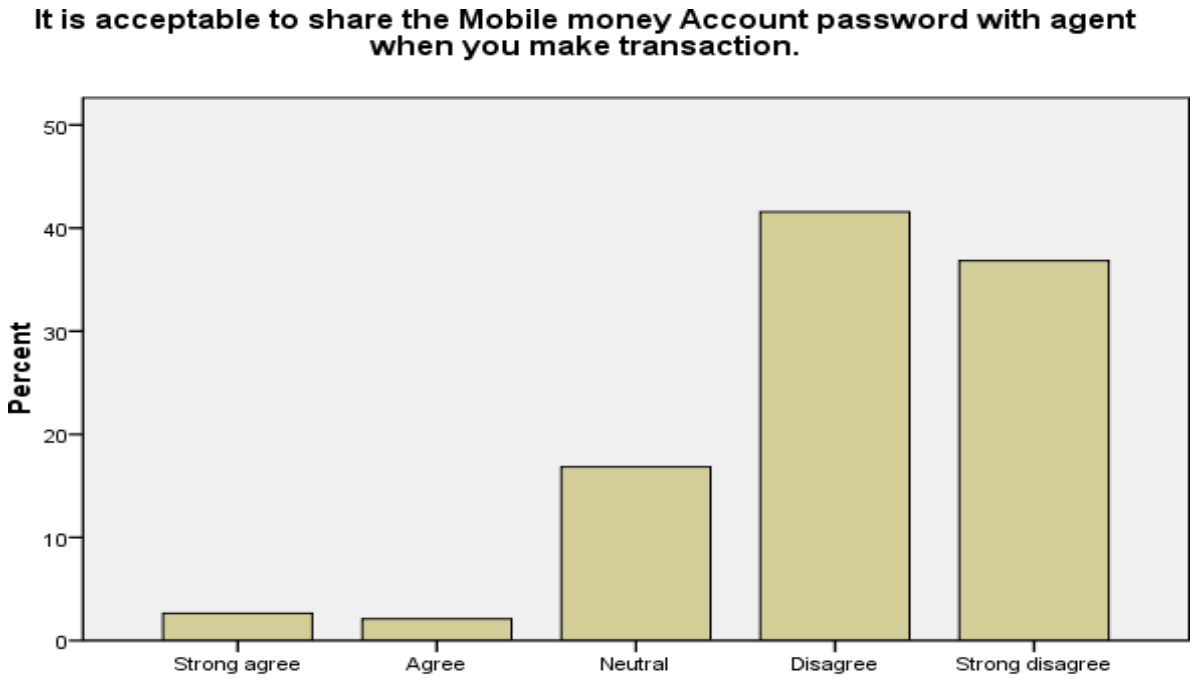
The findings on this study revealed that most of the respondents are higher in the manner that most of the respondents perceive well and aware on the proper usage of the Mobile Money service, generally in knowing well the mechanisms that social engineers normally use in attacking the Mobile Money accounts, and knowing some tips in the security perspectives of their Mobile Money accounts as well as the Mobile phones that having the SIM cards joined with the Mobile Money services. The findings is shown on the factors as:

Novelty Journals

ISSN 2394-7349

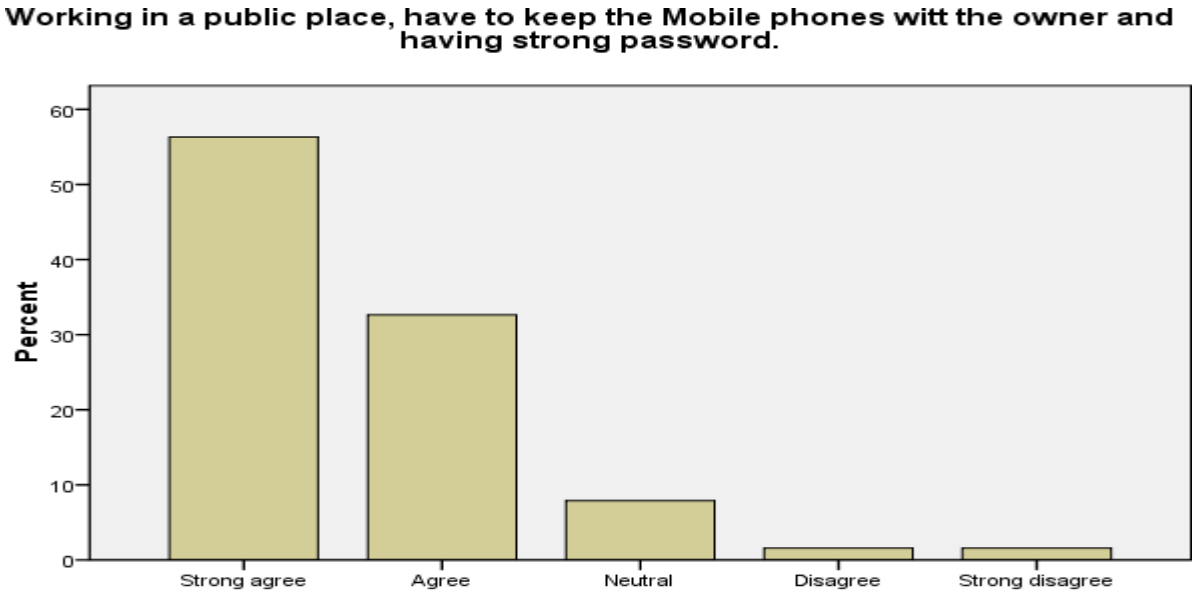
International Journal of Novel Research in Engineering and Science
Vol. 9, Issue 2, pp: (27-34), Month: September 2022 - February 2023, Available at: www.noveltyjournals.com

Knowledge



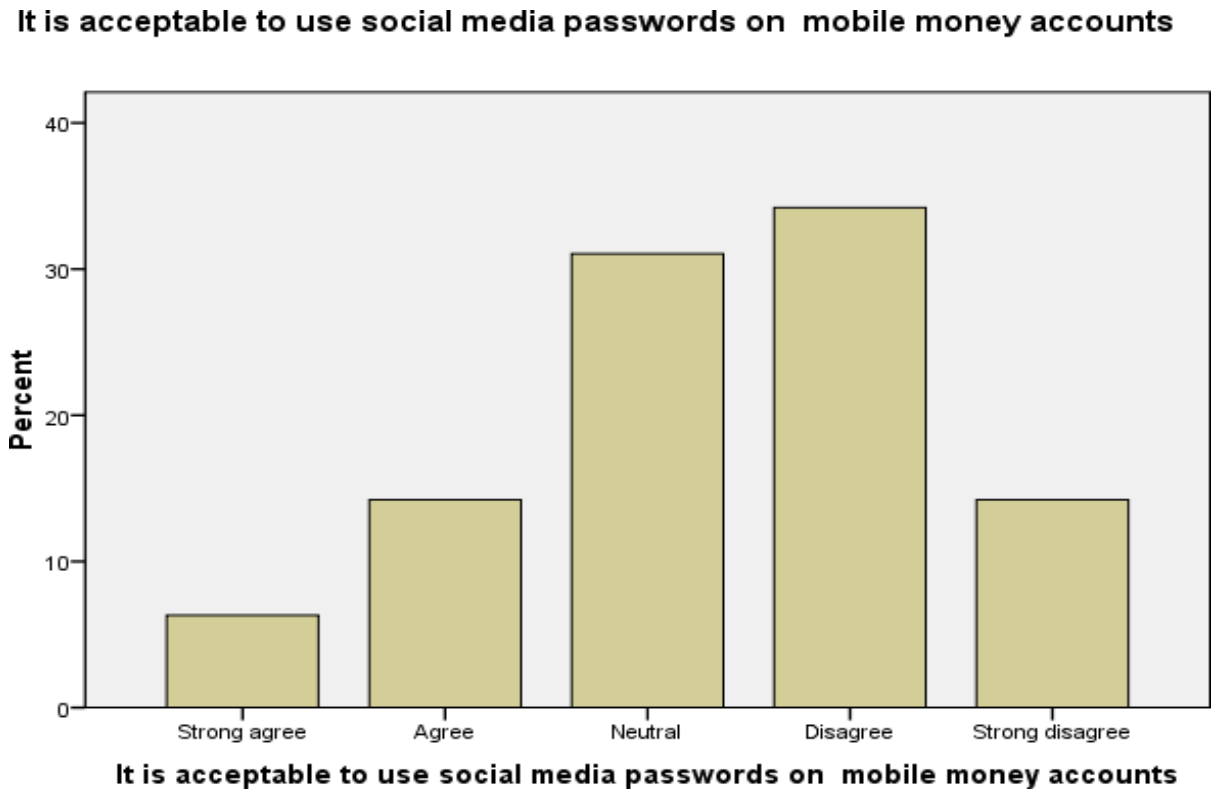
The findings of this study revealed that 41.6% disagreed on the statement that it is acceptable to share the Mobile money password with agents when make transaction, also 36.8% were strongly disagreed on the statement that it is acceptable to share the Mobile money password with agents when make transaction, also 36.8% of the respondents strongly disagreed that it is acceptable to share the Mobile money password with agents when make transaction, on the other hands 16.8% of the respondents remained neutral on the statement that it is acceptable to share the Mobile money password with agents when make transaction, 2.6% of the respondents strongly agreed that it is acceptable to share the Mobile money password with agents when make transaction, as well as 2.1% agreed that it is acceptable to share the Mobile money password with agents when make transaction.

Behaviour.



According to the findings of this study revealed that 56.3% of the respondents agreed that when working in a public place, I have to keep my Mobile phones with me and having strong password, also 32.6% of the respondents were strongly agreed that when working in a public place, I have to keep my Mobile phones with me and having strong password, on the other hand 7.9% of the respondents were remained neutral on the statement that when working in a public place, I have to keep my Mobile phones with me and having strong password 1.6% of the respondents disagreed that when working in a public place, I have to keep my Mobile phones with me and having strong password, as well as1.6% of the respondents strongly disagreed that when working in a public place, I have to keep my Mobile phones with me and having strong password.

Security Metrics.



According to the figure above 34.2% of the respondents disagree on the statement that it is acceptable to use social media passwords on mobile money accounts, similarly 31.1% of the respondents remained neutral on the statement that it is acceptable to use social media passwords on mobile money accounts, on the other hand 14.2% of the respondents strongly disagree on the statement that it is acceptable to use social media passwords on mobile money accounts, also 14.2% of the respondents agree that it is acceptable to use social media passwords on mobile money accounts, however 6.3% of the respondents strongly agree that it is acceptable to use social media passwords on mobile money accounts.

5. CONCLUSION AND RECOMMENDATION

This paper was mainly aimed in assessing the mobile money user's perception on social engineering.

Conclusively, the level of awareness on the social engineering among mobile money users in Tanzania from the findings shows that for about 65% of the respondents are well aware on social engineering together with the Mobile Money attacks in the consideration of the respondent's perception factors which are knowledge, behavior and the respondent's security metric issues.

The research project recommends the following based on the research findings, the following recommendations are here being made. They might be useful to the Mobile Money service providers, Mobile Money users and also the government institutions. It is therefore, they could be used to minimize social engineering attacks to the Mobile Money users in Tanzania and to make an environment good and secure for the Mobile Money transaction.

Recommendation for the Mobile Money service provider, Government and the Mobile Money Normal users.

Based on the findings of this research, Mobile Money accounts password sharing is one of the major causes of Social engineering attacks, so then the Mobile Money service providers have to make sure that, they make security awareness programs to their Mobile Money users, and to educate them well concerning with the techniques and ways that social engineers normally use in attacking the Mobile Money accounts and making sure that their Mobile Money users update themselves in making sure they are always secure and not making the chance for the social engineers to do social engineering attacks.

The government has to make sure that the security and privacy policy on the Mobile Money usage are surely practiced and to make sure that it is understood by all Mobile Money users in Tanzania. It is also recommended that for all government agencies like TCRA, Police Force, Cybercrime units of Tanzania and others have to establish strong collaboration between them in order to have smooth and safe Money transaction.

The Mobile Money users like normal customers and Agents are advised to make sure that for any transaction they make should confirm first and have to verify the identity of the receivers before transaction to be done, and also to have a strong password to their Mobile Money accounts and not stored in the books or phone memory, and also not to share to any one the Mobile money accounts PIN in order to be safe from social engineering frauds.

REFERENCES

[1] Afanu, E. K., and Mamattah, R. S. (2013), Mobile Money Security: AHolistic Approach. Lulea University of Technology.

[2] Agwu, E. & Adele-Louise, C. (2014). Mobile Phone Banking In Nigeria: Benefits, Problems and Prospects. International Journal of Business and Commerce, 50-70

[3] Davis, D &Venkatesh, V. (2000).A Theoretical Extension of the Technology Acceptance Model.In V. &. Davis, A Theoretical Extension of the Technology Acceptance Model (pp.186-204.).

[4] Hassan,A&Kamel, S. (2003). Assessing the Introduction of Electronic Banking in Egypt. USA: IdeaGrouping.

[5] Kothari, C. R. (2004) *Research Methodology: Methods & Techniques, New age International (P)Ltd.*

[6] Stergiou, D. (2013), *Social Engineering and Influence: A Study that Examines Kevin Mitnick's Attack through Robert Cialdini's Influence Principles.* Lulea University ofTechnology.

[7] Stallings, W. (2006), *Cryptography and Network Security: Principles and Practices*(5th ed.). New York: Pearson Education,Inc.

[8] Tanzania Communications Regulatory Authority.(2016). Quarterly Communication Statistics.Retrieved April 11, 2016, from http://www.tcra.go.tz/images /documents/telecom munication/CommStatMarch16.pdf

[9] TheUnitedRepublicofTanzania.(2015),TheelectronicTransactionAct,2015.Dar es Salaam: Parliament of the United Republic ofTanzania.

[10] Qin and J. K. Burgoon.An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering. IEEE Intelligence and Security Informatics, May: 152–159, 2007.

[11] Zuckerman, M., and Driver, R. E. (1985), Telling lies: Verbal and nonverbal correlates of deception. In A. W. Siegman and S. Feldstein (Eds.), *Multichannel integrations of nonverbal behavior* (pp. 129-147). NJ: Erlbaum, Hillsdale