https://doi.org/10.56279/orseaj.special.3

Efficacy of Measures used by Mobile Companies in Preventing Social Engineering in Tanzania: A Customer's Perspective from Selected Companies in Dar es Salaam

Juma James Masele[1] **and Godfrey Wilfred Lekule**[2]

Abstract

While a number of measures, are introduced by mobile companies, to prevent social engineering, the problem is still ongoing. The study research question was, "What is the efficacy level of the measures used by mobile companies in preventing social engineering in Tanzania". The study specifically sought to determine, the influence of users' awareness generation, direct message blockages, hackers tracking, and hackers' blockage on social engineering prevention in Tanzania. The study was conducted in Dar es Salaam with 100 mobile service customers using a five-point Likert scale questionnaire. Data were analyzed through regression analysis. Results showed all four variables significantly influenced social engineering prevention ($p < 0.05$). The study emphasizes the need for mobile companies to enhance user awareness, secure communication channels, and maintain updated systems to reduce vulnerabilities. Policy recommendations include enforcing multi-factor authentication, developing clear reporting protocols, and promoting social engineering prevention research. Theoretically, the study extends the Interpersonal Deception Theory and Protection Motivation Theory by framing Social Engineering Prevention as a layered approach integrating human and technological strategies. The model explained 36.4% of the variance, suggesting further exploration of additional influencing factors.

Keywords: Efficacy of measures; mobile companies; social engineering prevention; social engineering; Customer's perspective

Introduction

Worldwide, social engineering has been one of sources of distortion of service quality offered by telecommunication companies as it makes customers less secured with their confidential information and also well-being of their money, they store in the mobile money facilities/services (Qadri, 2023; Hatfield, 2019). There are a number of enablers for social engineering already documented, such as increasing use of smart phones to perform multiple activities including mobile money services, internet access, direct and quick communications, networking and others (Tanzania Telecommunication Market Report 2020-2025). In Tanzania, the growing telecommunication sector with several companies operating in the market including Tanzania Telecommunications Corporation (TTCL), Vodacom Tanzania, Airtel Tanzania, Tigo Tanzania, Halotel Tanzania, and Zantel Tanzania (TCRA, 2023) makes mobile phone applications, including interpersonal communication, mobile banking, access to internet easier and the like less costly.

[1] University of Dar es Salaam Business School, Tanzania
Email: masele@udsm.ac.tz
[2] Honora Tanzania PLC (Yas Tanzania)

While such increasing use is welcome, social engineering has turned to be bothersome to businesses, customers and regulatory authorities to a great scale. Reports on users being manipulated by some criminally minded people claiming to be operators of the service providers while subjecting the users into fraud, thefts and several other discrepancies are numerous (Bankelele, 2017; UN, 2025). This has been and is still a common practice which has caused many users of services to suffer negatively with information breach and their money being stolen. The social engineering consequences are enormous including causing disgruntled customers, lost revenue in sales and, inability to perform critical internal transactions, and facing legal consequences. It is from this point; social engineering becomes a matter of both legal and policy as well as research interest.

Literature cites on a number of measures that have been implemented to prevent social engineering. According to Bankelele (2017), service providers have resorted to various means to eradicate the situation including awareness generation to the users, direct message blockages, hacker's blockages and hackers tracking. The cited measures (by Conklin et al., 2015; Kamndaya, 2016) include enactment of cybercrime laws, and awareness generation campaigns by various actors such as law enforcement organs, mobile companies, telecommunication regulators and others through mobile phone short message and use of various media (Conklin et al., 2015; Kamndaya, 2016). Treglia & Delia (2017) asserts that messages to inform users on the means and ways employed towards the practices including automatic blockage of some text messages that facilitate social engineering through mobile networks are commonly used. According to Qadri (2023) other means are tracking and blocking the identified hackers and their means of communication in order capture and take criminals into justice for further legal proceedings (Mas, 2017). Yet, with all such efforts, still social engineering persists. According to TCRA (2023) there were a total of 23,328 fraudulent cases in the country by 2023 (TCRA, 2023). Fraudulent practices reported by mobile network operators in the country amounted to 38% from Tigo, 33% from Airtel, 17% from Vodacom, 7% TTCL and 5% from Halotel which gives a total of 23,328 cases from all over the country. In Dar es Salaam region alone the number of fraudulent practices amounted to 703 from Tigo out of 8,606 from all regions, 1,594 from Airtel out of 7,817 reported practices from all regions, 758 from Vodacom out of 4038 reported attempts from all regions, 56 for TTCL out of 1,699 reported practices from all regions, 162 from Halotel out of 1,167 attempts reported from all regions, which also makes a total of 3,273 attempts (TCRA, 2023). Consequently, social engineering continues to be one of setbacks in the mobile companies' operations and prosperity.

The situation under such poor perception on security and safety in performing transactions constitutes negative impression on service quality offered by service providers due to uncertainty in assurance, reliability and responsiveness in services provided (Mwela et al, 2022). This to some extent affects market share generation and competitive advantage in the service providers' business. Consequently, the problem has drawn attention of not only the telecommunication companies and responsible regulatory authorizes, but also academia and researchers in the area. Yet, to the best of researchers' knowledge there were missing studies on this area. This fostered for the need to conduct this study to address the situation. While there are already existing some studies in the country, and developing countries at large (such as Matola, 2018; Siria, 2017; & Hamad, 2016; Pallangyo, 2022), no concrete study was on efficacy of the strategies. Pallangyo (2022) focus was more on the cyber security challenges in mobile

money transactions. The research question on, "*What is the efficacy level of the measures used by mobile companies in preventing social engineering in Tanzania"* remain unanswered, signifying for a need for conducting this study in the area in order to fill this gap. Therefore, the study was formulated to assess customers' perspective on the efficacy of measures used by mobile companies in preventing social engineering in Tanzania. The study seeks to determine, the influence of users' awareness generation, direct message blockages, hackers tracking, and hackers' blockage on social engineering prevention in Tanzania. The study significance is inclined into three folds: to add to existing stock of knowledge; policy implication, and managerial contribution.

Theoretical review

The study is guided by two theories, the Interpersonal Deception Theory (IDT) and Protection motivation theory (PMT). The IDT as invented by Burgoon and Buller in 1996, is the theory on communication which explains how people and or individuals handle deception while engaging in face-to-face communication through physical and non-physical by electronic means (Burgoon et al, 2008). The IDT view deception falling into three types: falsification (untrue statements), concealment (hiding the truth), and equivocation (avoiding direct answers). According to IDT, deception as a dynamic and interactive process is facilitated by the relationship and interaction level between the sender and the receiver participating in the entire communication process (Bond & DePaulo, 2006; Laura, 2007). This theory has been applied in several other studies including the study by Masip & Herrero (2015) on the mechanisms through which law enforcement agents, particularly police officers, detect deception. The IDT is used by this study to understand how social engineers strategically manipulate communication, and how security professionals identify deceptive behaviors by analyzing both verbal (e.g. direct calls) and nonverbal (e.g. text message) cues that may reveal a social engineer's attempts to elicit false beliefs and obtain information. In that case, hackers might use any chances to deceive individual customers given the room that customers lack awareness or knowledge on social engineering practices and hence hackers may intentionally give wrong information or ask for private information from customers (to deceive customers) for their personal interests and uses to get access of their accounts and other related materials they need. Yet, while this theory is powerful in explaining interpersonal deception, it fails short to explain how individuals respond to social engineering threats. It was from this point of view this study employed the Protection motivation theory (PMT) to supplement the IDT.

Protection motivation theory (PMT) as established by R.W. Rogers in 1975 and updated in 1983 explain individuals' responses to a potential threat. The PMT maintains that; people protect themselves based on two factors: threat appraisal and coping appraisal, with severity of the situation determining how one responds to the situation (Rogers, 1975). The PMT is a widely-used framework to understand responses to stimulate that ascertain individuals of a potential threat. These stimuli include fear messages that encourage individuals to take precautions or protective measures or to abstain from activities that might harm themselves or others (Boer & Mashamba, 2005). This theory falls within the expectancy-value theories that hypothesize attitudes or beliefs which lead to subsequent behaviors (Floyd, et al., 2000). The theory is connected to the study on the ground that; since social engineering practices creates harm not only to the mobile companies but also to their customers, so the theory emphasizes on these individual customers to take some precautions or abstain from any environments that seem to develop harm to them. Likewise, for the mobile companies in connectivity may use some

protective measures (such as users' awareness generation, direct message blockages, hackers tracking, and hackers' blockage) to prevent social engineering (harm) to prevent themselves and their customers from social engineering harms.

Empirical literature review

Users' awareness generation in relation to social engineering prevention

The assumption is that users' awareness positively influences social engineering prevention in mobile companies in Tanzania. In this case, literature indicate that the companies play vital role in generating massive information prior to awareness raising to the customers and users of the services through text messages from the companies, police force and the TCRA as regulator (Bankelele, 2017). According to report by the Government Cyber Security strategy of 2022/2027, knowledge and awareness campaigns among users of electronic devices and the society at large, has a positive influence in preventing social engineering threat in the country. Studies (Salahdine, & Kaabouch, 2019; Syafitri et al., 2022) further argue that a key mechanism for combating social engineering is educating potential victims—namely customers—to raise their awareness of these techniques and how to identify them, thereby linking user awareness to social engineering prevention..Yet, these findings were from abroad, whose context is different from that of Tanzania. Tanzania has distinct social norms, trust relationships, communal values that influence how customers respond to social engineering tactics. Besides, Tanzania is highly dependent on mobile money services (e.g., M-Pesa, Tigo Pesa, Airtel Money) for daily transactions (Richard & Mandari, 2017; Anania & Kimario, 2024).) an intensity that exposes users to social engineering. From that note, the hypothesis is stated as follows.

H_1: Users awareness generation positively facilitates social engineering prevention in mobile companies in Tanzania.

Direct message blockages in relation to social engineering prevention

Existing literature asserts that direct message blockages influence social engineering prevention (Mas, 2017; Nturibi, 2018; Bleiman & Rege, 2020). That, texts that are commonly used to deceive users as customers and perform social engineering are deliberately blocked'. It may also involve use of some best practices including installation of some strong filtering systems that are capable of detecting fraud messages and moving them to a junk mailbox or blocking them entirely to prevent social engineering rooms (Bleiman & Rege, 2020). While the strategies are assumed to be effective it is necessary to be inquired further in the context of Tanzania, given the continuance of social engineering problems being reported. Hence, the hypothesis is stated as follows.

H_2: Direct message blockages positively influence social engineering prevention in mobile companies in Tanzania.

Hackers tracking in relation to social engineering prevention

Existent of mechanism for tracking/detecting, managing and responding to incidents of hackers in cyberspace plays as a means to prevent social engineering (Tanzania Government Cyber Security Strategy, 2022). According to Hatfield (2019), in order to identify hackers, one need to first make a track via telephone or directly from a service provider's site as a way to prevent the mobile phone user from social engineering loopholes. The strategies are assumed to halt social engineering which is necessary to be inquired more. It is assumed that the strategies given by

mobile companies are effective enough to foster tracking of the hackers for the purpose of capturing them and take them to justice (Qadri, 2023). This study furthers the assumption, that hackers tracking is the predicting variable consist of positive influence on social engineering prevention in Tanzania telecommunication companies. Therefore, the hypothesis is stated in the manner that;

H_3: Hackers tracking positively influence social engineering prevention in mobile companies in Tanzania.

Hackers' blockage in relation to social engineering prevention

The assumption is that blockages of hackers as the independent variable positively influence social engineering prevention in the mobile companies in Tanzania. The situation is perceived that way because several measures identified by users as anti-hacking strategies are first employed to block communications and avoid further risks of social engineering and persistent cybercrime (Yasin et al., 2019). Other measures are then taken to apprehend the offenders and bring them to justice (Yasin et al., 2019). Installation of anti-phishing software, spam filter, Antivirus solutions to be used to bock unauthorised users/hackers from gaining access into systems or electronic devices can positively help prevent social engineering, this has been deemed effective in halting social engineering (Lohani, 2019). While millions of scam emails are sent by hackers every day, efforts are made to minimize social engineering, through detecting and blocking by different technical solutions. A good example is phishing attacks which are among the most successful attack methods in social engineering-based attacks (Pfeffel *et al*., 2019). This is important for further verification to be realized through the inquiry. Therefore, the hypothesis is stated as follows. *H4: Hackers' blockages positively influence social engineering prevention in mobile companies in Tanzania.*

Study conceptual model

This study conceptualised as per Figure 1, that user awareness generation, direct message blockages, hackers tracking, and hackers' blockage influence social engineering prevention. It if from this conceptual model, hypotheses H1, H2, H3, and H4 are formed.

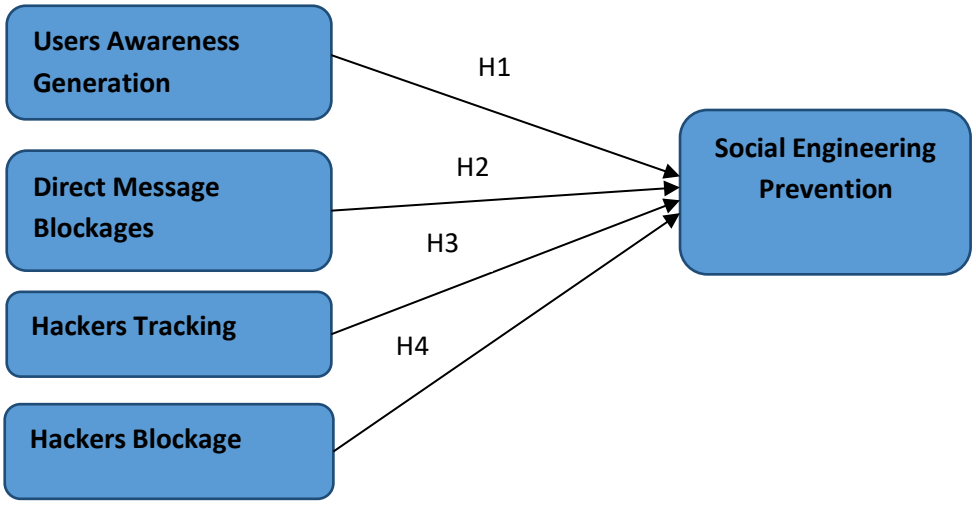

Figure 1: Conceptual model

Table 1: Operationalization of the study variables

Measures	Indicator statements	Citations
User's awareness generation	• I am aware of the potential warning signs that may indicate a social engineering attempt	Salahdine, & Kaabouch, (2019); Kumar et al. (2015); Conklin et al., 2015;
	• I understand the importance of safeguarding sensitive information to prevent social engineering attacks.	
	• I am confident in reporting suspicious communications or activities that may be related to social engineering.	
	• I actively participate in social engineering awareness training and educational programs.	
	• I understand the impact of social engineering attacks on individuals and company.	
	• I believe that continuous education and awareness efforts are crucial in combating social engineering threats.	
Direct message blockages	• Mobile companies have implemented measures to block suspicious or potentially harmful direct messages.	Mas, 2017; Nturibi, 2018; Bleiman & Rege, 2020.
	• The direct messages blockage implemented by mobile operators is clear and easy to understand.	
	• The direct messages blockage provides adequate information and notifications to keep me informed about potential risks.	
	• The direct messages blockage helps me identify and avoid suspicious or potentially harmful messages.	
	• I believe that the direct messages blockage instructs and triggers me to take precautionary actions on opening fraudulent msg or links.	
Hackers Tracking	• I am familiar with common tracking methods used by mobile companies to track hackers and stop them from committing social engineering attack	Qadri (2023); Hatfield (2019); Khan et al., 2020). Nturibi, (2018); Kamndaya, 2016)
	• I believe that tracking hackers' activities could enhance the prevention of social engineering attacks.	
	• I feel more secure knowing that your mobile company actively tracks and reports suspicious or malicious activities by hackers targeting its network.	
	• I would likely trust a mobile company that transparently communicates its efforts in tracking and preventing hacking activities to enhance customer security.	
	• Generally, hacker tracking is essential for effective social engineering prevention.	
Hackers blockages	• I understand the importance of hacker's blockages in safeguarding sensitive information and data.	Yasin et al., 2019), Lohani (2019); Pfeffel et al., (2019)
	• I am confident that the hacker's blockages implemented by our mobile phone service provider are effective in preventing social engineering attacks.	
	• I feel reassured knowing that our mobile phone service provider has robust measures to protect against hacking	

	attempts and social engineering.	
	• I am familiar with the various types of hacker's blockages and security protocols used to prevent social engineering attacks.	
Social engineering prevention	• I don't open emails and attachments from suspicious sources	Bleiman & Rege (2020); Bankelele (2017); Kamndaya, 2016); Treglia & Delia (2017).
	• I normally use multifactor authentication to ensure my account is protected in the event of system compromise.	
	• I am cautious about responding to calls and SMSs from unfamiliar or suspicious sources.	
	• I am always worried of tempting mobile phone related offers regardless of how enticing they may be.	
	• I can identify potential social engineering attempts in messages, or phone calls.	
	• I always keep my antivirus/antimalware software updated.	
	• I actively follow security guidelines and best practices to prevent social engineering.	

Methodology

This study adopted a cross- sectional explanatory research design in order to be able to explain the relationship between independent and dependent variable under study. The study was conducted in Dar es Salaam region. Dar es Salaam was selected not only because it is the most populated multicultural city in the country with a population of 5,383,728 (The United Republic of Tanzania, 2022), but also due to the fact that 18.4% of all active mobile subscriptions are in Dar es Salaam (TCRA, 2023). This subscription rate makes the region with the largest number of mobile users, about 3 times more mobile subscriptions as compared to Mwanza (with around 6.6% of total subscriptions) which ranks second in terms of regions with highest mobile subscriptions (TCRA, 2023). The study sample comprised 100 respondents. The sample size was determined using the formula proposed by Tabachnick and Fidell (2007), expressed as $N \geq 50 + 8m$, where N represents the number of subjects and m the number of predictors. Given that the study included four independent variables, the minimum required sample size was 82 respondents. The actual sample size of 100 respondents therefore met and exceeded this recommended threshold. .The study unit of analysis being individual mobile customers. A five point Likert scale questionnaire was used. Data collected was analyzed using regression analysis. The model for analysis was used as:

$$Y = \alpha + \beta 1X1 + \beta 2X2 + \beta 3X3 + \beta 4X4 + \mu,$$

Where:

Y = Social Engineering prevention
X1 = Users awareness generation
X2 = Direct massage blockages
X3 = Hacker's tracking
X4 = Hacker's blockage
$\beta_{(1-4)}$ = Beta coefficients (i.e., the slopes for independent variables)
μ = Stochastic error term
α = Y – intercept

Both validity and reliability was ensured by conducting pilot study to a sample of 20 respondents to remove any ambiguity and testing Cronbach's alpha internal consistence reliability. Data from the pilot study were subsequently included in the final sample analysed. The reliability test results as presented in Table 1, indicated in respective bracket show that user awareness generation with 0.712, direct message blockages (0.871), hackers tracking (0.944) and hacker's blockages (0.768) and social engineering prevention (0.792).

Table 2: Cronbach's Alpha Test

Study Variables	Cronbach Alpha Values
User's awareness generation	0.712
Direct message blockages	0.871
Hackers tracking	0.944
Hacker's blockages	0.768
Social engineering prevention	0.792

Demographic Profile of the Respondents

The findings presented in Table 2, from 100 customers of the mobile company's, 51 (51%) were males and 49% were females. These results indicate that number of men respondent were very close to that of female using mobile services to this study. Age wise, respondents were grouped into four age groups. Findings indicate that, customers aged between 20 to 35 were the majority comprising 49% followed by age between 36 to 45 who comprised 34%. The rest were below 12%. Table 3 details . Education wise, majority of respondents (57%) of respondents had bachelor degree, followed by 21% holding diploma level, while 14% had master degree, and those with primary education had 1% for primary education. This indicates that majority of the respondents had good understanding of research-based issue given their level of education.

Table 3: Demographic information

Demographic variable	Category	Frequency	%
Gender	Male	51	51.0
	Female	49	49.0
	Total	**100**	**100**
Age	20-35	49	49.0
	36-45	34	34.0
	46-55	11	11.0
	55-65	6	6.0
	Total	**100**	**100**
Education level	Primary Education	1	1.0
	Secondary Education	7	7.0
	First Degree	57	57.0
	Master's Degree	14	14.0
	Other (diploma)	21	21.0
	Total	**100**	**100.0**

Source: *Field Data (2023*

Regression Analysis

The results presented in Table 4, indicate that correlation R was equal to 0.603, meaning that the variables had strong positive correlation. It also implies that the variables have a high-strength, consistent linear relationship, where a change in one variable reliably indicates a large, predictable change in the other. It further indicates that, the regression results showing each predictor variable's contribution is given by user's awareness generation, p=0.000 ($p<0.05$; β=.391) direct message blockages p=0.000 ($p<0.05$; β= .283) hackers tracking p=.003 ($p<0.05$; β= .230), and hacker's blockages p=.020 ($p<0.05$; β=.214). This result implies that all predictor variables are significant at $p<0.05$. The results further indicate that all the predictor variables, hacker's blockages, hackers tracking, user's awareness generation, direct message blockages, were able to explain social engineering prevention by 36.4%. This is because the coefficient of determination, R^2 was equal to 0. 364, meaning that, the predictor variables were able to explain social engineering by only 36.4%, leaving 63.4% unexplained.

Multiple Regressions Results

Table: 3 Coefficients Table and Hypotheses Decision

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.	Hypothesis	Decision (at 0.05 level)
		B	Std. Error	Beta				
1	(Constant)	17.183	3.508		4.898	.000		
	User's awareness generation	.391	.105	.318	3.723	.000	H1	Accepted
	Direct message blockages	.283	.074	.328	3.798	.000	H2	Accepted
	Hackers tracking	.230	.076	.251	3.011	.003	H3	Accepted
	Hacker's blockages	.214	.090	.208	2.374	.020	H4	Accepted
R square= .364, R= .603; Adj R square= .337 Durbin Watson= .970. ANOVA, F=13.597								

***Dependent variable- Social engineering prevention**

Source*: Field Data (2023).*

Discussion of study findings

The results have shown a significant positive influence of user awareness generation on social engineering prevention with a beta value of 0.391 and p-value = 0.000. This indicates that user awareness generation has influence on social engineering prevention, hence the hypothesis is confirmed. These results are supported by the study of Samani & McFarland, (2015) who emphasized on awareness program combined with other measures as being one of the best tools for fighting social engineering attacks. The findings are in line with Aldawood & Skinner (2018) who establishes that there is a link between awareness of social engineering with protective security practices; with the aim to make customers to stay on the front line in

preventing themselves against social engineering threats. Salahdine, & Kaabouch, (2019) adds that, comprehensive fraud awareness and prevention programs which aim at informing customers how they can validate a phone call or SMS, to be able to identify phishing are also best means to influence social engineering prevention. It is from this point Nicholson *et al*., (2017) suggested on establishing training programs through social medias, TV programs, radio adverts, newspapers, SMS and all other means that can reach customers, to provide data security awareness to users to ensure their understanding of all forms of cybersecurity risks and threats and social engineering. This argument is in line with Kumar *et al*., (2015) who suggests that Education, Training and Awareness (ETA) is the primary measure to prevent the social engineering attacks. Training changes attitude, instills new knowledge and skills on doing certain course of action. It helps to upgrade the safe handling behavior of information, notifying the potential attacks and creating confidence to handle during the attacks amongst customers and service providers.

The findings have indicated that direct message blockages have positive influence on social engineering prevention since its computed scores are β= 0.283, t-value of 3.798 and p-value of 0.000. These results are consistence with Shaukat *et al*., (2020) study on learning techniques for cyber security in the last decade. In their findings, Shaukat et al. (2020), emphasized on a need to block texts, stop spam, and protect against other scam messages but also get some strong security software to block or defend against spam, malware, and other online threats. Khan et al. (2020) emphasize on importance of being aware and suspicious of any email or SMS that creates an environment of emergencies including stating some story that requires to be responded urgently. Such kinds of information need to be blocked immediately to prevent rooms for social engineering (Khan *et al*., 2020). Nturibi, (2018) further recommends for proactively combating of information security complacency like Block SMS header and Caller ID spoofing which to a better extent can help in preventing social engineering. Installing some endpoint security software like Anti-virus on user devices that can help in identifying and blocking obvious phishing messages, or any message that has a connection with malicious websites or IPS (Anderson, 2020).

This study result shows that social engineering prevention is significantly and positively influenced by hacker's tracking measure at β=0.230, t value= 3.011 and p=0.000. The study hypothesis is not rejected. The study findings are in line with the position of Khraisat *et al*., (2019) who alerts organizations to ensure regular updates of their software and systems with latest patches and security fixes to enable the process of tracking hackers run better and smoothly. The findings are also in line with Zhang et al. (2019) who urges on the need to conduct monitoring, detection and assessments by simulated phishing campaigns and social engineering tests, which will help identifying vulnerabilities and areas for improvement. This makes hackers tracking process easier and hence prevention of social engineering (Zhang *et al*., 2019). There are some initiatives in Tanzania including provision by the government through Tanzania Government Cyber Security Strategy (2022) of a resolution of administering a framework for improving social engineering prevention and to keep speed with the evolving social engineering risk ground in order to detect/track illegal actors in cyberspace. Yet, organizations are urged by Anderson (2020) to conduct frequent strong online audit trail to track system activity so as to detect and identify the occurrence of any security breach, the mechanism and extent of the breach for further action.

The result has revealed a significant and positive influence of hackers' blockage on social engineering prevention with a β=0.214, t-value = 2.374 and p= 0.000. This implies that hacker's blockages as a measure have influence on social engineering prevention. The hypothesis H4, was therefore accepted. The study findings are supported by Khan & Salah, (2018) who emphasize on the relationship between hacker's blockages on systems software security reviews and prevention of software. It gives suggestion on the use of "firewall" and "blockchain technology" to secure devices from unauthorized users. The software is designed to create a barrier against outside world or to block any unauthorized user from gaining access to your network hence, hackers can also be blocked as means for preventing social engineering (Khan & Salah, 2018). Lohan, (2019) findings align with this study by indicating that, in order to easily detect and prevent social engineering attacks, techniques such as use of anti-phishing tools for blacklisting and blocking phishing websites to give hackers' blockage are important. However, changing passwords or using complicated passwords to restrict unauthorized users from gaining access or easy logging into user account or devise, installation of smart software like antiviruses are also called for, to block all kinds of attacks through packet filtering thus improving social engineering prevention measures (Kumar *et al*., 2020).

Conclusion, Implications and Recommendations

This study has revealed significant and positive influence of user's awareness generation, direct message blockages, hacker's tracking, and hacker's blockages on social engineering prevention in mobile companies in Tanzania. The solidification of this finding within Tanzania context implies that the findings are consistent with the position of other researchers who attempted to link the variables in other parts of the world. Yet, this study adds to the understanding of contexts with distinct social norms, trust relationships, and communal values—such as Tanzania—that influence customers' responses to social engineering tactics. Moreover, Tanzanian users' high dependence on mobile money services for daily transactions hence intensifying their exposure to social engineering, adds an important dimension to the study phenomenon. This study has a number of implications theoretically, practically and policy wise. Practical implications are that customers need to be familiarized on criminal online behaviour and tips for identifying phishing attempts. Customer and company's interactions need to be done over secure communication channels, e.g. encrypted email, chat, and phone lines. On top of that, mobile companies/vendors need to keeping all application systems, and software up to date to minimize vulnerabilities, but also designing for improved means for direct message blocking, hackers tracking, and hackers' blockage.

As declared in the Tanzania Government Cyber–Security Strategy, (2022) that there are some challenges related to policy, laws and regulations including lack of a comprehensive legal framework for cooperation with external partners in cyber security issues and a high level of electronic devices illiteracy, including cyber security-related issues in the society. Hence the policy makers can look on how better the policy can be amended or reviewed taking into consideration the revealed findings of this study. Besides, reinforcement of the long-awaited Cybercrime Act of 2015 need to be enhanced in order to protect user's financial loss, and other fraud attempts related to social engineering. It may include enforcing technical controls such as use of multi-factor authentication, putting in place clear protocols for reporting suspicious activity without fear of reprisal, and incentives provision to encourages social engineering prevention research and development. Theoretically, the study combining IDT and PMT attributes adds explanatory power scope of the Interpersonal Deception Theory (IDT) and

Protection Motivation Theory (PMT). The study thus theorizes that since Social Engineering Prevention (SEP) involves human and technology-centric strategies, then SEP need to be an integrated approach that calls for continuous user education and psychological principles.

References

Aldawood, H. & Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A Literature Review in Proceedings of the IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), Wollongong, Australia; pp. 62–68.

Anania, J.C. & & Kimario, J. L. (2024). Influence of Technology-Related Factors on The Use of Mobile Money Services in Tanzania: The Moderating Role of Financial Literacy. *16th ORSEA Conference Proceedings Nov. 2024*

Bankelele, M. (2017). Banking, Finance, Technology, and Investments: Agency Banking in Kenya in 2017.

Bleiman, R., & Rege, A. (2020). An examination in social engineering: The Sus-ceptibility of Disclosing Private Security Information in College Students, *in Proceedings. 15th International Conference Cyber Warfare Security.* (ICCWS), pp. 47–56.

Boer, H. & Mashamba, M. T. (2005). Psychosocial correlates of HIV protection motivation among black adolescents in Venda, South Africa. AIDS Education and Prevention. 17(6), 590–602.

Bond, C. F. & DePaulo, B. M. (2006). Accuracy of deception Judgments. Personality and Social Psychology Review. 10 (3), 214–234.

Burgoon, J. K., Blair, J. & Strom, R. (2008). Cognitive biases and nonverbal cue availability in detecting Deception. *Human Communication Research*. *34* (4), 572–599.

Conklin, W., White, G., Cothren, C.; Davis, R. & Wasiams, D. (2015). Principles of Computer Security, Fourth Edition (Official Comptia Guide). New York: McGraw-Hill Education.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. Journal of Applied Social Psychology, 30(2), 407–429.

Hatfield, J. (2019). Virtuous human hacking: The ethics of social engineering in penetration-testing. *Computers & Security.* 83, 354–366.

Kamndaya, S. (2016). Vodacom to issue TSh500 billion shares. The Citizen (Tanzania). Dar es Salaam.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. https://doi.org/10.1016/j.future.2017.11.022.

Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2020). A survey on security and privacy of 5G technologies: potential solutions, recent advancements, and future directions. *IEEE Communications Surveys and Tutorials/IEEE Communications Surveys and Tutorials*, Review 22(1), 196–248. https://doi.org/10.1109/comst.2019.2933899

Kumar, A., Chaudhary, M. & Kumar, N. (2015). Social Engineering Threats and Awareness: A Survey. European Journal of Advances in Engineering and Technology, 2(11), 15-19.

Kumar, K., Raman, A. C., Gupta, C., & Pillai, R. G. (2020). The recent trends in malware evolution, detection and analysis for Android devices. *Journal of Engineering Science and Technology Review*, *13*(4), 240–248. https://doi.org/10.25103/jestr.134.25.

Laura, G. (2007). Close Encounters: Communication in Relationships (2nd ed.). Los Angeles, CA: Sage.

Lohani, S. (2019). Social Engineering: Hacking into Humans. International Journal of Advanced Studies of Scientific Research. 4(1), 385-393.

Mas, I. (2017). Why are Banks so scarce in Developing Countries? Critical review: *A Journal of Politics and Society,* 23(1–2), 135–145.

Masip, J., & Herrero, C. (2015). Police detection of deception: Beliefs about behavioral cues to deception are strong even though contextual evidence is more useful. *Journal of Communication*, 65(1), 125-145.

Mwela, J., Kisawike, B., & Colnerius Simba, C. (2022). Customer Perception of Service Quality in the Tanzanian Telecommunication Sector. *Global Scientific Journal*: Volume 10, Issue 10, Online: ISSN 2320-9186

Nicholson, J., Coventry, L.& Briggs, P. (2017). Assessing social salience as a means to improve phish detection. In Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS), Santa Clara, CA, USA.

Nturibi, B. M. (2018). A Mobile Money Social Engineering Framework for Detecting voice & sms phishing attacks - *A Case Study Of M-Pesa*. United States International University – Africa

Pallangyo, H. (2022). Cyber Security Challenges, its Emerging Trends on Latest Information and Communication Technology and Cyber Crime in Mobile Money Transaction Services. *Tanzania Journal of Engineering and Technology/Tanzania Journal of Engeering and Technology*, *41*(2), 189–204. https://doi.org/10.52339/tjet.v41i2.792

Pfeffel, K., Ulsamer, P., & Müller, N. (2019). Where the user does look when reading phishing mails - An eye-tracking study. In Proceedings of the International Conference on Human-Computer Interaction (HCII), Orlando, FL, USA, 26–31

Qadri, N. (2023). *Critical Factors that Affect the Adoption of Mobile Payment Services in Developed and Developing Countries* [Uppsala University Department of Informatics and Media]. https://uu.diva-portal.org/smash/get/diva2:1800492/FULLTEXT01.pdf.

Richard, E. & Mandari, E. (2017). Factors influencing usage of mobile banking services: The case of Ilala district in Tanzania.Operations Research Society of Eastern Africa (ORSEA) Journal, 7(1), 42-54.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*. *91*(1), 93–114.

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: a survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Samani, R., & McFarland, C. (2015). "Hacking the Human Operating System: The Role of Social Engineering within Cybersecurity." http://www.mcafee.com/au/resources/reports/rp-hackinghuman-os.pdf

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. IEEE Access, 8, 222310–222354. https://doi.org/10.1109/access.2020.3041951

Syafitri, W., Shukur, Z., Mokhtar, U., Sulaiman, R., & Ibrahim, M. A. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review Journal of IEEE Access. V.10. pp1-1. DOI 10 1109/ACCESS.2022.3162594.

Tanzania Communications Regulatory Authority, TCRA (2023). Communications Statistics Quarter ending 30th September 2023. Tanzania Communications Regulatory Authority.https://www.tcra.go.tz/uploads/text-editor/files/TCRA%20Communications%20Statistics%202023%20-2024-Q1_1698210303.pdf

Tanzania Government Cybersecurity strategy (2022). https://www.utumishi.go.tz/uploads/documents/sw-1688121496

The United Republic of Tanzania. (2022). Administrative Units Population Distribution Report. Ministry of Finance and Planning National Bureau of Statistics Tanzania & Presidents' Office - Finance and Planning Office of the Chief Government Statistician Zanzibar. https://sensa.nbs.go.tz/publication/volume1a.pdf.

Treglia, J.& Delia, M. (2017). Cyber Security Inoculation. Presented at NYS Cyber Security Conference, Empire State Plaza Convention Center, Albany, NY.

Yasin. A, Fatima, R., Liu, L., & Wang, J. (2019). Contemplating social engineering studies and attack scenarios: A review study. *Security and Privacy*, 2 (4), 1–14.

Zhang, C., Patras, P., & Haddadi, H. (2019). Deep learning in mobile and wireless Networking: a survey. *IEEE Communications Surveys and Tutorials/IEEE Communications Surveys and Tutorials*, *21*(3), 2224–2287. https://doi.org/10.1109/comst.2019.2904897