EJTAS
ISSN 2786-7447
EUROPEAN JOURNAL OF THEORETICAL AND APPLIED SCIENCES
OPEN ACCESS
PEER REVIEWED

Evaluation of Measures Taken by Telecommunication Companies in Preventing Social Engineering Attacks in Tanzania

Goodluck Muzigura
Master Student, College of Business Education, Tanzania

Dr. Respickius Casmir
Lecturer, College of Business Education, Tanzania

Suggested Citation

Muzigura, G. & Casmir, R. (2023). Evaluation of Measures Taken by Telecommunication Companies in Preventing Social Engineering Attacks in Tanzania. *European Journal of Theoretical and Applied Sciences, 1*(4), 1248-1259.
DOI: 10.59324/ejtas.2023.1(4).114

Abstract:

This study aimed to evaluate the measures taken by telecommunication companies in preventing social engineering attacks in Tanzania. The study was guided by the deception theory, the researcher employed a descriptive research design and quantitative approach to conduct this study. Data was collected by using a questionnaire administered to the selected telecommunication companies in Tanzania. Furthermore, the obtained findings were as follows; most of the respondents who participated in this study are aware of social engineering and that they experienced social engineering. The study also revealed that there are common social engineering attacks experienced by the respondents such as business collaboration benefits, alleged wrong remittance of money, sim swaps, SMS phishing and fraudulent SMS from lost or stolen phones, password requisitions and links sharing. The findings of this study went further to reveal that social engineering has effects such as loss of sensitive data, financial loss, reputational damage, disruption of operations as well as legal and compliance issue. The general findings of this study show that most of the respondents said that there is a presence of security measures to prevent social engineering such as the provision of the awareness program, enabling the use of multifactor authentication, there is implementation of policies around social media usage, provision of regular software updates, regular review of security protocols, provision of well-known customer care services number. On the other hand, the study also revealed that telecommunication companies use the following ways to minimize social engineering attacks, provision of security awareness training for employees, implementing security policies and procedures, regularly reviewing and updating security protocols, detecting and responding to social engineering attacks, placing limits on the access each member has in the system, always require a username and password to be configured. On the strategies used to prevent social engineering, the finding of this study showed that telecommunication companies should ensure encrypting data, proper verification of emails or instructions sent to customers, ensure that even if hackers intercept communication they can't access information contained within, use of SSL certificates from trusted authorities, incorporating phishing and malicious detection solutions into security stack. This study concludes that telecommunications ensure routine reviews of security standards, daily notifications for customers and other system users, and the availability of a well-known customer care services number. Due to the difficulties that information system users face, businesses have been using a variety of protection techniques to avoid social engineering, from putting up multifactor authentication for users' accounts to teaching employees how to spot suspect activity. Hence it is recommended that it is necessary to deploy mechanisms like machine learning-based ways to defend against social engineering-based assaults since cybercriminals exploit human activities to breach security as well as using the security features on messages (filter unknown senders) and calls (silence unknown callers).

Keywords: *Telecommunication; social engineering; companies, Prevention.*

Introduction

Universally it is agreed that social engineering is a broad range of malicious activities accomplished through human interaction (Siddiqi et al., 2022). It uses psychological manipulation to trick users into making security mistakes or giving sensitive information (Pollock, 2022). Social engineering attacks happen in one or more persons, the perpetrator first investigates the intended victims to gather necessary background information such as points of entry and weak security protocol, needed to proceed with the attack (Salahdine & Kaabouch, 2019).

In developing countries, social engineering is an illegal activity that accounts for 98% of cyber-attacks. Social engineering is characterized by attackers coercing victims into divulging sensitive information by pretending to be a known person or legitimate entity (Jansen van Rensburg, 2021). Identity theft through phishing attacks is the most common form of social engineering. Over 70% of data breaches start with phishing or social engineering attacks (Mwagoti, 2016). Following the challenges facing the user of the information systems companies have been employing several prevention strategies to avoid social engineering, from setting up multifactor authentication for the user's accounts to training employers to identify suspicious behavior (Washo, 2021).

In Tanzania, the telecommunications sector has various companies operating in the market, one belonging to a public corporation and more than four multinationals (Abade, 2016). They include Tanzania Telecommunications Corporation (TTCL), Vodacom Tanzania, Airtel Tanzania, Tigo Tanzania, Halotel Tanzania, Zantel Tanzania, Smile, and others (URT, 2021). The companies perform well in the market and have facilitated the transformation of communication in Tanzania to the extent that it is highly advanced and able to compete and work with others all over the globe despite some challenges in its operations (Hamad, 2016).

The companies have attained significant market share and competitive advantage which is inevitable for the users to make use of the services (Sanders, 2018). This has mostly been facilitated by mobile money services, internet access, direct and quick communications, affordable mobile bundles, networking, and others (Aldawood & Skinner, 2020). Regardless of the gains, social engineering attacks have been persisting to a great scale to the extent that users are being manipulated by some claiming to be service providers' operators and subject the users to fraud, theft, and several other discrepancies (Syafitri et al., 2022). This has been and still is a common practice that has caused many users of the services as customers to suffer negatively by their money being stolen and sometimes information breaches (Syafitri et al., 2022).

Despite using various techniques to fight against social engineering attacks still, there is responsible for 98% of the attack. In 2020, 75% of the companies reported being victims of phishing (Juma, 2022). The average cost after a data breach is $150 per second. Also, there are approximately 43% of phishing emails impersonate large organizations and also there 60% of companies have reported data loss after a successful phishing attack and 18% of targeted users fall victim to social engineering (Pallangyo, 2022). Therefore, this study is conducted to evaluate measures taken by telecommunication companies in preventing social engineering attacks in Tanzania, A case of selected telecommunication companies. This study specifically addresses the following objectives, to identify the measures taken by telecommunication companies to prevent social engineering attacks, to determine the effects of social engineering attacks and to propose strategies for preventing social engineering attacks.

Literature Review

Conceptual Definitions

Mobile Companies

Mobile companies refer to corporate entities which may be public or private engaged in the provision of telecommunication services (Ryan, 2012). They are large companies either publicly or privately owned which may operate in the respective country of origin or as multinational companies operating beyond the country(s) of origin (O'Brien, 2012). As multinational companies may be private or publicly owned as well. This study uses the term mobile companies to mean entities engaged in the provision of telecommunication services and it includes companies such as Vodacom, Halotel, Tanzania Telecommunication Corporation (TTCL), Zantel, Airtel, and Tigo in Tanzania.

Social Engineering

Social engineering refers to the actions that consist of psychological manipulations of the people that aim to distort the information which is confidential to the concerned actor and or subject (Anderson, 2008). Social engineering entails the confidential trick that may lead to certain information gathering without the knowledge of the provider, fraud, hacking, and others that may have wrong or negative implications. This study uses the term social engineering to mean practices that use manipulations to distort information that is sought to be shared or already shared.

Theoretical Framework

Theory of Deception

This is the theory of communication that 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 theory was invented by Burgoon and Buller in 1996 and explains the behaviour and reactions that individuals or people take in the course of identifying deception in the course of information sharing in the communication process (Bond & DePaulo, 2006). The theory suggests that deception is facilitated by the relationship and interaction level between the sender and the receiver in the entire communication process (Guerrero, 2007). This is facilitated by the behaviour and the intention of the participants in communication as being the sender and the receiver. The theory is connected to the study on the ground that social engineering practices in mobile companies are comprising deception in communication between the sender and the receiver. In that case, the situation has been handled by the companies through hackers' blockades, hacker tracking, awareness generation to the customers, and message blockades. Regardless of that, the situation that persists requires further interventions through the inquiry.

Information Systems Success Model

This is the theory on information systems that seeks to determine the realization of the success of the information system in particular usage and application (DeLone& McLean, 1992). The theory describes the success of the relationship on the components that assures success in the information system performance (DeLone& McLean, 2002). The components include system quality, information quality, service quality, user satisfaction, system usage, and net system benefits. Once the components perform well automatically the system is deemed to be effective and efficient in fostering performance and positive results for that matter (DeLone& McLean, 2003). The theory is relevant to the study because social engineering practices in mobile companies imply limited performance on the success of the information systems related to mobile phone usage that is in use. Where information quality, service quality, system quality, user satisfaction, system usage, and net system benefits are poor and less functioning they may render not satisfy the customers and assure the realization of the expected goals and objectives. It is from this case, the study assesses the extent to which measures like message blockades, hackers tracking, hackers' blockades, and customer awareness influence social engineering prevention in Tanzania. Even though these measures have been instituted still the situation persists which fosters further interventions through the inquiry.

Empirical Literature Review

In the research conducted by Siddiqi et al., (2022) to study the psychology of social engineering–based cyber-attacks and existing countermeasures. Social engineering-based cyberattacks are extremely difficult to counter as they do not follow specific patterns or approaches for conducting an attack, making them highly effective, efficient, easy, and obscure approaches for compromising any organization. To counter such attacks, a better understanding of the attack tactics is highly essential. Hence, it provides an in-depth analysis of the approaches used to conduct social engineering-based cyberattacks. Similarly, Pollock, (2022), assessed the roles of environmental and devices type on the success of social engineering attacks. Specifically, it was surprising to learn that the non-distracting environment results for the Phishing IQ tests were overall lower than those of distracting environment, which is counter to what was envisioned. These Phishing IQ test results may be assumed to be because, during the distracting environment, the participants were monitored over Zoom to enable the distracting sound file.

Moreover, according to Albladi and Weir, (2020), it was predicted individual vulnerability to social engineering in social networks the popularity of social networking sites has attracted billions of users to engage and share their information on these networks. Social engineering is one of the most common types of threat that may face social network users. Training and increasing users' awareness of such threats is essential for maintaining continuous and safe use of social networking services. Moreover, according to Banire et al., (2021), investigated the experience of social engineering victims; Explanatory and user testing studies. The user testing study showed that the AI-based tool was accepted by all users irrespective of their occupation. The categories of users' occupations can be attributed to the level of SE awareness. Information security awareness should not be limited to organizational levels but extend to social media platforms as public information.

Also, according to Fuertes et al., (2022), who examined the impacts of social engineering attacks; The main findings are concentrated in companies, financial institutions, and even vehicle vulnerabilities, which have caused economic losses and a decrease in the image and reputation loss damage of individuals and companies. Most of the causes are related to human behaviour, such as innocence, unconsciousness, and lack of training or capacity. In the same way, Salahdine and Kaabouch, (2019), conducted research on the social engineering survey. Social engineering is one of the biggest challenges facing network security because it exploits the natural human tendency to trust. This paper provides an in-depth survey of social engineering attacks, their classifications, detection strategies, and prevention procedures. In the research conducted by Wilcox & Bhattacharya, (2019), countering social engineering through social media; an enterprise security perspective. Social engineering through social media confirms the crucial need for employees to be made aware of attack methods through a combination of policy development and employee education, alongside traditional technical countermeasures.

Also, it was discussed in the research conducted by Ye et al., (2020) that risk analysis framework for social engineering attacks based on user profiling. In this article, a risk analysis framework for social engineering attacks is proposed based on user profiling. The framework provides a pathway to quantitatively calculate the possibility of being compromised by social engineering attack and potential loss, to effectively complement current security assessment instruments. Meanwhile, the research conducted by Duarte, (2019) examined social engineering; the art of attacks, and the correct management of information systems security, this study approached social engineering by taking an introductory brief on its history, what is psychological manipulation and human weaknesses, what are the social engineering attacks, how they use authority and fear establishment, it is also approached how a social engineering attack is executed, providing value monetizing the scam, and identity exploration.

Conceptual Framework

A conceptual framework is an illustration that consists of the variables of the study that are described for testing to facilitate the information-gathering process. The variables include predicting ones as independent variables and the dependent variable which are shown in Figure 1 which is illustrated below.

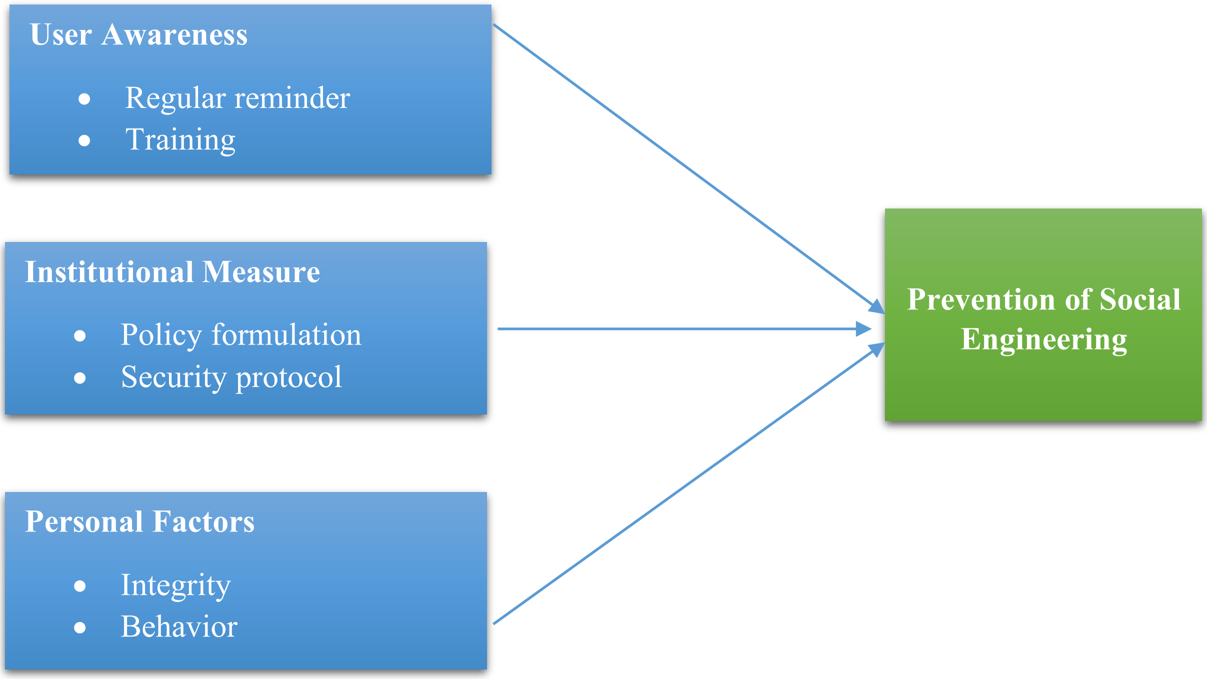

Figure 1. Conceptual Framework
Source: Researcher (2023)

Methodology

This study used a quantitative approach, because it helps in emphasizing objective measurements and statistical, mathematical or numerical analysis of data collected through polls, questionnaires as well as surveys, hence it helps in manipulating pre-existing statistical data using computational techniques(Taylor & Jackson, 2019). This study employed a descriptive research design because it ensures a complete description of the situation, making sure that there ensuring minimal bias in the collection of data and allowing data collection from a sizeable population economically. The study was conducted in two selected companies in Tanzania namely The Tanzania Telecommunication Company Limited (TTCL) and Airtel Tanzania in Dar es Salaam City. According to Tanzania Telecommunication Overview and Statistics (2021), TTCL maintains a total subscriber base of 305,000 who have affixed phone lines and 600 employees, while Airtel Tanzania has 529, 0000 who have affixed phone lines and 1300 employees. Therefore, the target population of this study is 860,000. While the sample size was 100 respondents who were used in gathering reliable information to fill the study gap. Since the study used primary data, a questionnaire was used to assure the information generation process. The collected information was analysed quantitatively through SPSS datasheet version 23.0 to generate relevant statistical tools to present primary data.

Results

Table 1 shows that 49.5% of the respondents were male similarly 49.5% of the respondents were female. The results depict equal participation of the male and female respondents in the data collection process. Hence the researcher successfully managed to avoid gender-biased research. On the Age of the respondents, Table 1 shows that 38.1% of the respondents were aged 22 – 35 years, 37.1% of the respondents were aged 36 – 45 years and 24.7% of the respondents were aged 46 – 55 years. The study shows that most of the respondents who participated in this study are older enough to understand the need of the researcher and hence were able to accord the researcher with relevant information for this study. On the level of education, the study revealed that 25.7% of the respondents has a certificate level of education, 37.1% of the respondents had a diploma level education, on the other hand, 24.7% of the respondents had a bachelor's degree, while only 12.4% of the respondents had the master degree. Therefore, it can be shown that most of the respondents in this study are educated though with varied levels but their level of education enables them to appreciate the intention of the researcher as well as provide a well-reasoned opinion concerning the problem being investigated. Table 1 also shows that respondents were from different categories such as 13.4% were from the management, 38.1% of the respondents were ICT officials, moreover 24.7% of the respondents were customers and 23.7% of the respondents were employees from different areas in the selected telecommunication companies.

Table 1. Demographic Characteristics

Character	Category	Frequency	Per cent
Sex	Male	48	49.5
	Female	48	49.5
Age	20 - 35	37	38.1
	36 - 45	36	37.1
	46 - 55	24	24.7
Level of Education	Certificate	25	25.7
	Diploma	36	37.1
	Degree	24	24.7
	Masters	12	12.4
Occupation	Management Official	13	13.4
	ICT official	37	38.1
	Customer	24	24.7
	Other Employees	23	23.7

Source: Field Data (2023)

Measures Taken by Telecommunication Companies to Prevent Social Engineering Attacks

The study intended to examine the measures which have been taken by telecommunication companies to prevent social engineering attacks on their customers. Thus, for this objective several questions were asked to the respondents to assess the awareness of the respondents about social engineering in the first instance, then the experience of the telecommunication companies towards social engineering.

Table 2. Awareness of Social Engineering

Response	Frequency	Per cent
Yes	84	84.0
No	16	16.0
Total	100	100.0

Source: Field Data (2023)

Table 2 presents results on the awareness of social engineering, whereby 84% of the respondents who participated in this study said that they are aware of social engineering attacks, while 16% of the respondents said no that they are not aware of social engineering. Thus, these results depict that most of the respondents who participated in this study are aware of social engineering.

Table 3. Presence of Security Measures to Prevent Social Engineering

	Frequency	Per cent
Yes	94	94.0
No	6	6.0
Total	100	100.0

Source: Field Data (2023)

Table 3 shows that 94.0% of the respondents agree that there is the presence of security measures to prevent social engineering. On the other hand, 6% of the respondents, said no that they are not sure if there are present security measures to prevent social engineering. Thus, the general findings of this study show that most of the respondents said that there is a presence of security measures to prevent social engineering.

Table 4. Measures Taken by Telecommunication Companies to Prevent Social Engineering Attacks

Responses	Frequency	Percent
Provision of an Awareness program	11	11.0
Multi-Factor Authentication	15	15.0
Increasing Spam Filtering Via Email Gateways	15	15.0
Implementation of Policies Around Social Media Usage	10	10.0
Provision of Regular Software updates	19	19.0
Regular Review of Security Protocols	10	10.0
Provision of daily Reminders	7	7.0
Provision of a well-known customer care services number	13	13.0
Total	100	100.0

Source: Field Data (2023)

Table 4 shows that one of the measures taken by telecommunication companies to the prevention of social engineering of provision of awareness programs as agreed by 11.0%, while 15% of the respondents contend that another measure taken by telecommunication companies prevent social engineering attacks on their user is used onMulti–Factor Authentication. Not only that but also 15% increased spam filtering via email gateways, also it was shown that 10% of the respondents agree that implementation of policies around social media usage is one of the mechanisms used to prevent social engineering attacks. The study further revealed that 19% of the respondents provide another mechanism used is the provision of regular software updates. Not only that but also there is a need to have regular review of security protocols as agreed by 10%. The study also revealed that 7% of the respondents provided that telecommunication companies provide a daily reminder, lastly, 13.0% opined that telecommunication companies have provided well – know customer care service numbers.

Table 5. The Most Common Social Engineering Attacks Experienced

Response	Frequency	Per cent
Business Collaboration Benefits	14	14.0
Alleged wrong remittance of money	22	22.0
SIM Swaps	22	22.0
SMS phishing and fraudulent SMS from lost or stolen phones.	18	18.0
Password requisitions	12	12.0
Links sharing	12	12.0
Total	100	100.0

Source: Field Data (2023)

Table 5 of the respondents provides that 14.0% of the respondents' business collaboration benefit, on the other hand, 22.0% of the respondents show alleged wrong remittance of money, the other 22.0% of the respondents provide that SIM Swaps are one of the most common social engineering attacks experienced. It was also shown that 18% of the respondents SMS phishing and fraudulent SMS from lost or stolen phones. Another social engineering attack experience was requisition attacks opined by 12% and lastly, 12% of the respondents said link sharing as one of the social engineering attacks.

Table 6. Effects of Social Engineering Attacks

Responses	Frequency	Per cent
Loss of Sensitive Data	30	30.0
Financial Loss	18	18.0
Reputational Damage	17	17.0
Disruption of Operations	18	18.0
Legal and Compliance Issues	17	17.0

Source: Field Data (2023)

Table 6 shows that 30% provided that one of social engineering is loss of sensitive data, in the same vein 18% of the respondents said that another effect is financial loss, 17% perceived reputational damage as one of the effects of social engineering, while 18% of the respondents agreed that disrupted operations while 17% of the respondents considered legal and compliance issues as one of the respondents. The general findings of this study show most of the respondents agree that social engineering leads to the loss of sensitive data.

Table 7. How Telecommunication Companies are Prepared to Minimize these Effects

Response	Frequency	Per cent
Provision of security awareness training for employees	18	18.0
Implementing security policies and procedures	17	17.0
Regularly reviewing and updating security protocols	13	13.0
Detecting and Responding to social engineering attacks	16	16.0
Placing limits on the access each member has in the system	17	17.0
Always require a username and password to be configured	19	19.0
Total	100	100.0

Source: Field Data (2023)

Table 7 also examined the extent to which telecommunication companies are prepared to minimize the effects of social engineering attacks, where 18% of the respondents said that telecommunication companies ensure the provision of security awareness training for employees. In the same vein, 17% of the respondents provided that telecommunication companies implement security policies and procedures, while 13% of the respondents considered regularly reviewing and updating security protocols. Not only that but also telecommunication companies are very prepared to detect and respond to social engineering attacks. On the other hand, 17% of the respondent's telecommunication companies considered placing limits on the access each member has in the information system, lastly, 19% of the respondents said that telecommunication companies normally require usernames and passwords to be configured when performing a transaction in the information system.

Table 8 Strategies Used by Telecommunication Companies Employ to Prevent and Protect its Users Against Social Engineering Attacks

Responses	Frequency	Per cent
Encrypting Data	22	22.0
Proper verification of emails or instructions sent to customers	16	16.0
Ensure that even if hackers intercept communication they can't access information contained within	22	22.0
Use of SSL Certificates from trusted authorities	20	20.0
Incorporating Phishing and malicious detection solutions into the security stack	20	20.0
Total	100	100.0

Source: Field Data (2023)

According to Table 8, it was established that 22% of the respondents opined that data encryption is used as the strategy that telecommunication employs to prevent and protect its users against social engineering attacks. In the same vein, 16% of the respondents considered proper verification of emails or instructions sent to customers. Moreover, 22% of the respondents opined that telecommunication companies use a procedure which ensures that even if hackers intercept communication they can't access information contained within. Furthermore, 20% of the respondents said that telecommunication companies ensure that they use SSL certificates from trusted authorities, while another 20% of the respondents opined that incorporating phishing and malicious detection solution into the security stack. From the general findings of this study, it can be established that most of the respondents who participated in this study opined that telecommunication has different strategies they use in ensuring the protection of its users against social engineering attacks.

Discussion

Therefore, it may be prohibited that social engineering is utilized and promoted in the majority of circumstances. Identity theft is one of the largest problems with social engineering, and it may be done without the user's consent. An attacker who is effective at social engineering can get authenticated access to the target's system. The attacker can penetrate the system, network, or data with their destructive actions once they have full access to the employee or individual, and they can even exfiltrate the data.

The study also revealed that through social engineering someone else's personal information can be obtained, accessed and used. One's private information may also be misused to harm others. Criminals are constantly seeking something and most of the time it's money. Businesses might lose hundreds to millions of dollars due to social engineering, and that's before recovery expenses are included. Time is money in any kind of company. If the attack is effective, a lot of time will be squandered trying to undo the harm done by social engineering. The productivity of the IT staff, all employees, and eventually the profitability of the company are frequently destroyed by this.

The findings of this study demonstrate that some of the measures employed to prevent social engineering by telecommunication companies included the provision of an awareness programme, multi-factor authentication, telecommunication also increased spam filtering via email gateway, not only but also telecommunication companies ensure the implementation of policies around social media usage, they ensure the provision of regular software updates, and so on.

On the other hand, telecommunications ensure routine reviews of security standards, daily notifications for customers and other system users, and the availability of a well-known customer care service number. Due to the difficulties that information system users face, businesses have been using a variety of protection techniques to avoid social engineering, from putting up multifactor authentication for users' accounts to teaching employees how to spot suspect activity. It is necessary to deploy mechanisms like machine learning-based ways to defend against social engineering-based assaults since cybercriminals exploit human activities to breach security.

Also, according to Wilcox & Bhattacharya, (2019), there is a worrying trend to rush these technologies into the workplace without initiating effective security strategies involving social media use. Social engineering through social media confirms the crucial need for employees to be made aware of attack methods through a combination of policy development and employee education, alongside traditional technical countermeasures. Ye et al., (2020), provided that existing security analysis instruments are difficult to quantify the social engineering attack risk, resulting in invalid defence guidance for social engineering attacks. In this article, a risk analysis framework for social engineering attacks is proposed based on user profiling.

Duarte, (2019) suggests that social engineering is a risk to security information and must be considered just as important as in technological areas. Also, this study approached social engineering by taking an introductory brief on its history, what is psychological manipulation and human weaknesses, what are social engineering attacks, and how they use authority and fear establishment, it also approached how a social engineering attack is executed, providing value monetizing the scam, and identity exploration, while Sekhar, (2021) provided that it is significant for both individuals and organizations to be aware of different social engineering attacks, follow & implement the prevention, detection and mitigation strategy for the possible. Similarly, the practice of safe information handling behaviour is crucial for every individual to fight against social engineering attacks. To prevent and mitigate the loss of an attack, the government and service providers must adopt a multi-dimensional approach of education, training and awareness program (ETA), proper incident response, effective implementation policy and standard practice for the public and its customers. Aldawood & Skinner, (2020), opines that for better implementation methods against social engineering, this qualitative study will attempt to provide measures against information security challenges faced by organizations. The analysis is then provided by the answers of interviewed experts in the field of cyber security and social engineering. The research herein focuses on the human element of cyber security threats, recognizing that hackers exploit the vulnerabilities and lack of awareness of staff.

Conclusions

From the general finding user awareness and message blockades are effective in the prevention of social engineering attacks, however, the researcher recommends that telecommunication companies must ensure that they employ more forensic techniques since technology tends to be improved and nourished in a timely. Based on the first research objective this study also revealed that direct massaging and user awareness generation are very important in the prevention of social engineering, however, the study recommends that telecommunication companies should remind their customers to be careful and avoid tempting offers and which are always false and also to practice authentication as well as confidentiality all the time.

In respect to the second objective the study also recommends to both telecommunication companies and customers that they should frequently use multifactor authentication on user accounts. And to call customer care numbers to confirm in case they are not sure of their decision or call the police to report to the police before being the victims of the hackers.

On the last objective, the study also recommends that users of information systems should use very strong passwords since hackers have tended of assuming passwords as one of the strategies for social engineering. Thus, having a weak password may lead to an easy attack on the information system leading to loss of information and data breaches.

More the study recommends to customers to have tended of thinking before clicking, this is because sometimes hackers use links which when you open them without reasonable care will lead to security breaches. Therefore, customers and users of information systems should ensure that they assess the safety and security of shared links before clicking them.

Area for Further Research

This study recommends that future research be conducted on the strategies used to enhance social engineering attacks in private institutions. This study will be useful because it draws attention to the users of the information system about different ways that hackers use to attack systems, hence being able to determine the proper ways to deal with the kinds of attacks which will be engineered in their systems.

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

Albladi, S. M., & Weir, G. R. S. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, *3*(1). https://doi.org/10.1186/s42400-020-00047-5

Aldawood, H., & Skinner, G. (2020). Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions. *IEEE Access*, *8*, 67321–67329. https://doi.org/10.1109/ACCESS.2020.2983280

Banire, B., Al Thani, D., & Yang, Y. (2021). Investigating the experience of social engineering victims: Exploratory and user testing study. *Electronics (Switzerland)*, *10*(21). https://doi.org/10.3390/electronics10212709

Duarte, N., Coelho, N., Guarda, T. (2021). Social Engineering: The Art of Attacks. In: Guarda, T., Portela, F., Santos, M.F. (eds) *Advanced Research in Technologies, Information, Innovation and Sustainability*. ARTIIS 2021. Communications in Computer and Information Science, vol 1485. Springer, Cham. https://doi.org/10.1007/978-3-030-90241-4_36

Fuertes, W., Arévalo, D., Castro, J. D., Ron, M., Estrada, C. A., Andrade, R., Peña, F. F., & Benavides, E. (2022). Impact of Social Engineering Attacks: A Literature Review. *Smart Innovation, Systems and Technologies*, *255*, 25–35. https://doi.org/10.1007/978-981-16-4884-7_3

Hamad Bakar, I. (2016). *Social Engineering Tactics Used In Mobile Money Theft In Tanzania.*

Jansen van Rensburg, S. K. (2021). End-User Perceptions on Information Security. *Journal of Global Information Management*, *29*(6), 1–16. https://doi.org/10.4018/jgim.293290

Juma, Y. H. (2022). Assessing the Mobile Money user's awareness on social engineering in Tanzania: Case of the Ministry of Information Tourism and Heritage Zanzibar. *International Journal of Novel Research in Engineering and Science*, *9*, 27–34. https://doi.org/10.5281/zenodo.7277453

Mwagoti, L. M., & of Nairobi, U. (n.d.). *Social Engineering in E-commerce Platforms in Kenya.* Retrieved from http://erepository.uonbi.ac.ke/bitstream/handle/11295/99767/Mwasambo_Social%20Engineering%20in%20E-commerce%20Platforms%20in%20Kenya.pdf?sequence=1

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, *41*(2), 189–204. https://doi.org/10.52339/tjet.v41i2.792

Pollock, T. (2022). Experimental Study to Assess the Role of Environment and Device Experimental Study to Assess the Role of Environment and Device Type on the Success of Social Engineering Attacks: The Case of Type on the Success of Social Engineering Attacks: The Case of Judgment Errors Judgment Errors. Retrieved from https://nsuworks.nova.edu/gscis_etd/1173/

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. In *Future Internet* (Vol. 11, Issue 4). MDPI AG. https://doi.org/10.3390/FI11040089

Sanders, C. A. (n.d.). *Social Engineering Knowledge Measured as a Security Countermeasure*. Master's thesis. College of Engineering and Computing.

Sekhar Bhusal, C. (2021). Systematic Review on Social Engineering: Hacking by Manipulating Humans. *Journal of Information Security*, *12*(01), 104–114. https://doi.org/10.4236/jis.2021.121005

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. In *Applied Sciences (Switzerland)* (Vol. 12, Issue 12). MDPI. https://doi.org/10.3390/app12126042

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022a). Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access*, *10*, 39325–39343. https://doi.org/10.1109/ACCESS.2022.3162594

Taylor, G. R., & Jackson, C. L. (2019). Quantitative Research Approach. In *Demystifying Research*. https://doi.org/10.1163/9789087903411_014

Washo, A. H. (2021). An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports*, *4*. https://doi.org/10.1016/j.chbr.2021.100126

Wilcox, H., & Bhattacharya, M. (2015). Countering Social Engineering Through Social Media: An Enterprise Security Perspective. In: Núñez, M., Nguyen, N., Camacho, D., Trawiński, B. (eds) *Computational Collective Intelligence. Lecture Notes in Computer Science*, 9330. Springer, Cham. https://doi.org/10.1007/978-3-319-24306-1_6

Ye, Z., Guo, Y., Ju, A., Wei, F., Zhang, R., & Ma, J. (2020). A risk analysis framework for social engineering attack based on user profiling. *Journal of Organizational and End User Computing*, *32*(3), 37–49. https://doi.org/10.4018/JOEUC.2020070104