ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 5, Issue 4 (Oct. - Dec. 2017)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2017)

Vishing Attacks on Mobile Platform in Nairobi County Kenya

[I]Elijah M. Maseno, [II]Patrick Ogao, [III]Samwel Matende
[I,II,III]Faculty of Computing and Information Management, KCA University, Kenya

Abstract
Voice phishing (vishing) is a type of phishing attack where social engineers manipulate individuals during phone conversation into divulging sensitive information. Through mobile phone users are able to carry out all bank services like cash withdraw, transfer and deposit, mobile phones offer payment services and through mobile phone, one is able to process loans. Mobile users in Kenya are a target to criminals (social engineers). Social engineers are criminals whose main aim is to manipulate individuals in giving out sensitive information regarding their bank accounts through phone conversation. They prefer this form of attack because they can easily complicate the call routes, making it hard for the investigator to locate them. Research shows that most of these attacks are never reported to the relevant authorities because most victim blame themselves for their naivety. Unlike email phishing, which is classified, as tradition way of attack mobile phone vishing is a modern way of attack, and very little has been reported in this area. The current study therefore aimed at exploring the key contributing factors of vishing attacks. The study employed a cross sectional survey research design. The sample size was comprised of 20 respondents, who were selected using random sampling. Data was collected using a structured questionnaire for mobile phone users and interview guide for the key informants in Kenya. Qualitative data was analyzed using content analysis while quantitative data was analyzed by use of SPSS. The study findings revealed that the main contributing factors in vishing attacks are psychological factors, technical factors and information sensitivity. Based on these three main factors mitigation measures were proposed.

Keywords
Vishing, Social Engineering, Mobile, Psychological factors, Information sensitivity factors, technical factors.

I. Introduction

Among various form of emerging electronic financial crimes, voice phishing is known to cause the most significant degree of damage [1].

Communication Authority of Kenya " fourth quarter sector statistics report for the financial year 2015/2016 shows that the number of mobile money transfer subscriptions stood at 26.3 million while the number of mobile money transfer agents was recorded at 158,727 [2]. The total number of transactions during the quarter was registered at 375.8 million with an equivalent of Ksh. 957.0 billion transacted amongst the users [2].

Long are gone days when mobile phones were only used for calling, In Kenya most of money transactions are carried through mobile phones. According to [3] with the present dynamic technological developments, electronic information has grown in significance, businesses now conduct most of their day-to-day business undertakings electronically and this has drastically changed the level of information security threat. According to [4] Kenya is at the global forefront of mobile money services as an alternative to traditional banking. These innovations are seen as new payment channels for online services that facilitate easier access to money. These new channels have opened new alternative targets for cyber criminals. Cyber criminals now have shifted their attacks from banks to financial services providers to access bank systems. Most of the Banks in Kenya are in the proses of trying to offer all of their services on mobile platforms. Customers are able to deposit, withdraw, pay and even process loans through their phones.

A study by [4] found that social engineering was the second top cyber security issue in Kenya in 2015 after data exfiltration. Several cases have been reported where individuals have been manipulated to give out sensitive information like subscriber identification module (SIM) pin or Money transfer pin, which has led to fraudulent transaction. Even with the increase of Vishing attacks on mobile platforms in Kenya, there is no extensive research that has been conducted, particularly to Kenyan mobile platforms to provide solution thus threatening the integrity of mobile transactions. Kenyans need to be informed on this type of attack and how well to protect themselves and hence this study.

II. Related Studies

According to [4] [5] "Cybercriminals have their eyes on the M-Pesa (in Kenya) platform. Users therefore need to exercise great caution and use common sense in the event of potentially fraudulent transactions. Over the years, since mobile money transactions services such as M-Pesa gained ground, criminals have always devised ways of gaining access to individual's accounts". Vishing is the commonly used method to launch attacks on mobile platforms in Kenya.

Vishing can be defined as form phishing attack where social engineers manipulate individuals during phone conversation into divulging sensitive information which can be used against themselves.[6][7].

The situational context and characteristics of voice phishing have not been sufficiently understood, and there is a lack of the theoretical background needed for establishing suitable countermeasures [6]. Through script analysis, they were able to come up with the sequential steps used in vishing attack. This was a major step in understanding the operation of vishing attacks. The crime script analysis showed that voice phishing crimes could be divided into the preparation, recruiting telemarketers, script composition, making phone calls, having conversations, deposit and withdrawal, and money transfer stages. They further categorized the process into three according to [8] who argued that it was appropriate to categorize the process of committing an offense into three steps of pre-crime (that is, offense planning), criminal event (that is, offense strategies) and post-offense (that is, aftermath). These stages are the following:

Pre-crime stage: According to their study, this stage comprised of the following phases:

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Preparation
In their research [6] noted that vishing criminals work as a team, each individual having a role to play. The roles are divided to Information Technology (IT), telemarketing, script, bank accounts, money withdrawals, money transfers and mobile phones. The sections are given specific tusks to perform towards the goal. When a potential target answers the call it is the work of IT section to direct the calls to a consulting agent through an Automatic Calling Program. The telemarketing section consists of social engineers who can speak fluent language of the victim. Diverse scenarios and situational responses are created and developed by the script section. The victims are lured to deposit cash in false bank accounts which are opened by the bank account section. The money withdraw section sends money to the transfer section. The transfer section delivers the money using illegal remittance system. False identities on phones a created by the mobile section [6].

Recruiting telemarketers
The first phase involve recruitment of telemarketers. Telemarketers who speak fluent language of the victim without any accent are selected to avoid any slightest indication of being a foreigner which could plant a seed of doubt to the victims mind. Much is invested in the recruiting of telemarketers due to the fact that they are the ones to adopt the developed script.
Study indicates that many Asians adopt the role of telemarketer due to the fact that the benefits outweigh the risks [6].

Script composition
In this stage different scripts are prepared so that telemarketers are able to make apposite responses in different situations. Detailed script is developed, and in accordance to the agency that the telemarketer is supposed to represent scenarios are developed [6].

Criminal event stage: consists of the following phases
Making the phone calls
An automatic calling program is used by the IT section to generate random calls that are transferred to a telemarketer when a victim picks the phone. To complicate the investigation process for locating the caller, complex dispatch routes are used to present international call as a domestic call. In addition, to evade capture by law enforcement complex reception routes are used by the voice phishing organizations. The voice phishing organizations take advantage of the complicated system that makes it difficult, both technologically and legally through registering as international telephone businesses or Internet phone businesses, [6].

Conversations
The telemarketers adopt different legitimate entities as per the created scripts, this include but not limited to the bank officer, the prosecutor's office, security officer, school teacher and public agencies [6].

Post-offense stage

Deposit and withdrawal
To prevent investigators from tracing the money transactions, victims are requested to deposit money in a bank account opened under a false name, the details of the false bank account is shared to the telemarketing team by the money withdrawal team. The withdrawal team pulls out the money deposited by the victims after the information regarding the feck account has been shared. It is difficult to apprehend the managers of the money withdrawal team even if when the individuals running errands for the organization are caught because they phones which are under false identities [6].

Money transfer
This is the last phase of vishing, money is transferred to the country where the vishing organization is located by the bank team [6]. As it can be noted above these are well organized criminals with all resources needed to hack human beings. The government and the citizens need to be informed on this process in order to be able to defend themselves on such.
In their research, [7] developed a social engineering attack detection model (SEADM) based on two main perspective of social engineering: psychological perspective and information sensitivity. The model was designed to be used in a call center environment. SEADM was further extended [9] to be able to detect social engineering attacks that use bidirectional communication, unidirectional communication or indirect communication.
In their study [10] found that the main entities in social engineering attacks were people, security strategy and technology. The research done by [11] categories the defense mechanism into technical and training techniques. If we can be able to achieve this, we can easily mitigate vishing in our networks.

A. Conceptual framework
The research adopted the conceptual model of the major aspects of social engineering-based attack by [10] as it meets all the objectives of the study as shown in Figure1.

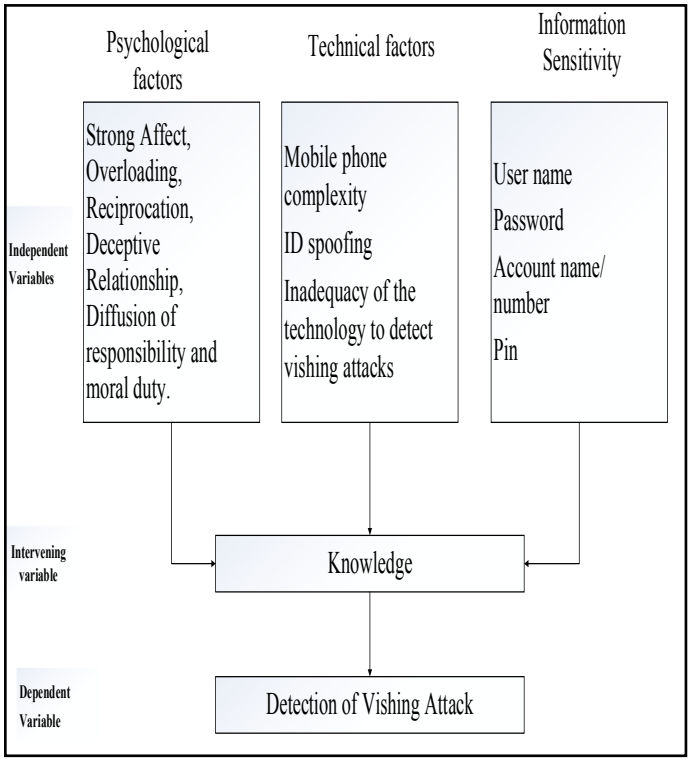

Fig 1: Conceptual framework

III. Methodology

1. Research Design
This study used the survey research design, which was cross-sectional because it was carried at one point in time. According [12], survey research seeks to obtain information that describes

existing phenomena by asking individuals about their perceptions, attitudes, behavior or values. For this study, it enabled the researcher to seek information from mobile users and IT managers on their knowledge on vishing attacks.

This research focused on mobile phone users to ensure the availability and genuineness of information concerning vishing attacs in Kenya. Study by [13] points out that an optimum sample is one that has the ability to fulfill the requirements of efficiency, representativeness, reliability and flexibility.

The objective populace for this study includes Mobile phone users, IT experts, and service providers in Nairobi County. Thus, the researcher approximates a population of 200 respondents.

2. Sampling design and sample size

According to [14], a good population sample lies within 10% to 30% of entire population. In defining, the sampling procedures this research study employed stratified random sampling. Taking an approximate population of 200 respondents, the sample size will be 10/100*200= 20. Therefore, from this formula twenty respondents who are Kenyan citizens (20) were selected as respondents for this study. Proportionate sampling of the respondents with the two major networks that is Safaricom and Airtel was done, with ten (10) respondents being sampled from each. Random sampling of the respondents was done with the researcher having to count every 20^{th} person who visited the customer care center for the various networks. It has been proposed [15] that less than 20 participants in a qualitative study helps a researcher build and maintain a close relationship and thus improve the "open" and "frank" exchange of information. This can help mitigate some of the bias and validity threats inherent in qualitative research. In quantitative research sampling, the size of the sample is determined by the optimum number necessary to enable valid inferences to be made about the population. The larger the sample size, the smaller the chance of a random sampling error, but since the sampling error is inversely proportional to the square root of the sample size, there is usually little to be gained from studying very large samples. The optimum sample size depends upon the parameters of the phenomenon under study, for example, the rarity of the event or the expected size of differences in outcome between the intervention and control groups [16].

Based on the above studies, and the nature of this research that mobile platforms use standard metrics across the world, sixteen respondents were good enough to produce better results since from the fourteen respondents the sample size had reached saturation or redundancy. This study therefore, focused on only twenty (20) respondents. However, sixteen respondents were reached. These are the respondents the researcher got relevant data that was used to show the impact of vishing on mobile users.

In addition, the researcher purposively selected bank mangers of various banks, which included Equity bank, Barclays bank, Cooperative bank, National bank, Family bank, Stanbic Bank and Kenya Commercial bank. Who served as key informants to the study providing in-depth information on cases handled in the banks as a result to vishing.

3. Data collection tools and procedure

Data from the respondents was collected by use of a self-administered questionnaire since it guaranteed anonymity and confidentiality. Study done by [13] stipulates that use of the questionnaire is one of the major ways to elicit self-reports on people's opinions, attitudes, beliefs and values. For the administration of respondent questionnaire, the researcher visited Safaricom and Airtel customer care centers within Nairobi County. The researcher approached the clients getting in to be served and engaged them by creating a rapport between the researcher and respondent explaining the purpose of the study. Respondents' consent to participate in the study was sought who upon consenting would sign the consent form and a questionnaire was then handed over for them to fill.

The researcher conducted a total of seven key informant interviews using a semi structured interview schedule. This was done to gather in depth information from the researcher ICT managers of various banks, which included Equity bank, Barclays bank, Cooperative bank, National bank, Family bank, Stanbic Bank and Kenya Commercial bank. Who provided in-depth information on cases handled in the banks as a result to vishing. The interviews were done face to face through direct personal investigation; hence the researcher collected information personally by writing.

4. Piloting of the tool

Before commencing the study, pre-testing of the study instruments was conducted. The aim of pre-testing was to assist in determining accuracy, clarity and suitability of the research instruments and to check their validity and reliability [14]. The pre-testing study was conducted among respondents who had visited Thika Safaricom customer care centre involving a total of five respondents who had a high propbability that they could not be duplicated in the main study. Adjustments were made in order to make to make the research instruments more appropriate before the actual field work begun. The responses derived from the pretest were used by the researcher to refine the questionnaire by rephrasing and editing thus ensuring that the questions conveyed the same meaning to all respondents. The pretest enabled the researcher to test the appropriateness of the study tool by ensuring that items tested what they were intended to (validity) and that they consistently measured the variables in the study (reliability). It also helped to estimate the length of time for the administration of instruments.

5. Data Analysis and Presentation

This study generated both qualitative and quantitative data. Quantitative data collected was analysed using the Statistical Package for Social Sciences (SPSS). Descriptive statistics of frequencies and percentages were used to describe and summarize data. Data presentation was done through tables. Information generated was also statistically analysed so as to elaborate on factors that contribute to vishing attacks. Qualitative data from the Key informants was presented in narrative form, highlighting respondents' voices to compliment some of the quantitative findings.

IV. Results and Discussion

A. Socio-Demographic characteristics of respondents

To capture general information, the researcher sought to establish the gender, age, education level and the position of the respondents. In regard to gender 31.25% of the respondents were female and 68.75% of the respondents were male, this is due to the fact that technology field is male dominated field. Majority of the respondents 62.6% were aged between 30 to 40 years.

The researcher sought to establish the education level of the respondents. The analysis demonstrated that respondents with postgraduate studies recorded the highest percentage of 50%, this covered those who had masters and doctorate. The 25% represents those who are University graduates, holding a degree, 12.5%

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

represents those with college certificates and 12.5% represent those with high school certificates. In addition 62.6% of the respondents were employed.

B. Vishing attacks

The study sought to find out how many people had been victims of social engineering attacks. Majority of the respondents 87.5% had been victims of social engineering attack with 50% experiencing social engineering attacks to a great extent, 25 % to a very great extent and only 12.5% of the respondents had not experienced social engineering attack to a great extent.

C. Exposure to vishing attacks due to technical factors- Mobile complexity

The researcher sought to establish technical factors due to mobile complexity that exposes mobile phone users to vishing attacks in the country. Majority of the respondents 56.3% reported that their phones had some complexity, 25% too much complexity; hence, the complexity on the use of their mobile phone was making them prone to vishing attacks. These findings are similar to [17] who noted that future of digital systems will be complex, and complexity is the worst enemy of security since the more the complex the system is the harder the user to understand it.

D. Exposure to vishing attacks due to human factors

Findings reveal that half the respondents 50% and 37.5% attested that human factors had a significant and critical potential to course security incidences on their mobile platforms. Social engineers prefer to hack human beings rather than system with security measures in place. This findings were similar to [7] who agreed that people lack knowledge on vishing engineering making them more vulnerable. This was supported by the IT managers interviewed who agreed that human factors were potentially critical in causing vishing attacks to customer's mobile phone.

This was attested by one of the respondents who said

"I received a call from my equitel line informing me they are calling me on behalf of the bank to notify that my account is being swindled and they wish to help me secure it. I out rightly panicked and was ready to follow all the instructions they gave to help secure my account. Which we did step by step without any question. Interestingly, the caller did not ask me for the pin. Right after the conversation with caller and hanging up, I started to think through the entire incidence. I did call the bank which confirmed my worst fears that I had just been conned... it was so depressing of how easily I could fall to such a scam ....and yes just to confirm that human factors make us prone to vishing attacks."

Respondent 13

E. Exposure to vishing attacks due to mobile banking services

The researcher sought to establish how many respondent were registered to mobile banking services, which exposed them to attacks. The analysis showed that 100% of the respondents were registered to M-pesa mobile money service hence the highest targeted mobile money service by attackers, 62.5% of the respondents were registered to Equitel mobile money service, 31.25% of the respondents were registered to Airtel money services and 25% to Branch mobile money service.

F. Establishing consequences of vishing attacks

The researcher sought to establish the most experienced loss by mobile users. The analysis showed that 100% of the respondents believed that the financial loss and loss of data were the greatest consequences of vishing attacks. This was followed by leakage of personal information 62.5%. These findings were similar to [10] that the major loss incurred after a successful vishing attack is available. This was supported by IT managers interviewed who attested receiving a lot of claims of money lost by their clients after encountering a vishing attack.

G. Knowledge of vishing attacks

The research sought to find out if people were knowledgeable about the various strategies used by social engineers. The researcher found that none of the respondent had some or much knowledge on vishing and smshing. 50% of the respondent had very little knowledge and 50% little knowledge on vishing attacks. 62.5% of the respondent had little knowledge on smshing attacks and 37.5% had very little knowledge on smshing attacks. This finding was similar to [7] who found that lack of knowledge is the key contributing factor to the increase of social engineering attacks.

H. Establish attack methods used by Social engineers

The researcher sought to establish the commonly used form of attack by social engineers. The researcher found that the mostly commonly used form of attack was vishing with 75% indicating to have experienced vishing attacks to a very great extent, 12.5% to a great extent and 12.5% to a small extent. These findings are similar to [6], who noted that most of the social engineer prefer vishing attack due to the fact that they can easily sense the emotions of the victim through the voice.

I. Establishing defense mechanisms used by mobile users

The researcher sought to establish the mechanism used by mobile users in defending themselves against vishing attacks. The researcher found that most of the users used content based defence mechanism to defend themselves, 75% to a very great extent, 6.3% to a great extent and 3% to a small extent. This finding is similar to [18] who found that individual preferred to use content base mechanism in defending against social engineering attacks due to its simplest.

J. Mitigation measures

Various methods have been proposed by different researchers to mitigate social engineering attacks. SEADM by [9] to assist the users in making informed decision during attacks. Awareness training was recommended widely as key in detection of social engineering attacks. In addition to this, the researchers propose the following measures based on the analyzed data.

1. Mobile users should understand their mobile phone in depth, that is application on their mobile phones
2. Mobile users should be aware of the psychological triggers exploited by the attackers.
3. Mobile users should not disclose or be forced to use their personal information during mobile conversation.
4. Mobile users should report any security incidence to the necessary authority.
5. The government and mobile money services providers should come up with a portal were victims can share their incidences anonymously. It was noted most of the victim fail to report or share their incidences because they feel naïve and blame themselves.
6. The government and mobile money service providers should publish any reported incidence in order to inform citizens.

7. Mobile users can use available software to protect themselves that is an ant spoofing software.
8. Communication Authority should seek to create awareness on the various forms of social engineering attacks that exist through radio and television to increase knowledge level on social engineering.
9. Communication Authority should seek to create training programs on social engineering attacks
10. The Ministry of Information and Communication Technology together with other stakeholders should embark on developing a policy on social engineering attack.
11. The Ministry of Internal Security should also develop a policy that seeks to deal with individuals engaging in social engineering attacks as it amounts to criminal activity.

V. Conclusion

The researcher sought to establish the main entities of vishnig attacks on a mobile platform and mitigation measures of vishing attacks. Through data analysis on the information gathered from the questionnaires and key informants it come out that the key entities of vishing attacks on mobile platforms were psychological factors, technical factors and information sensitivity factors. In addition to the three entities, finding showed that lack of knowledge contributed to successful vishing attacks. Majority of the respondents were not aware of the various strategies used by social engineers to get information from people, majority did not even know how to defend themselves from vishing attacks. The three main entities of vishing attacks and lack of knowledge informed the proposed mitigation measures.

This research was able to show the impact of vishing attacks in Kenya, which was a key contribution to the existing body of knowledge.

The major limitation was the selection of respondents, the respondents were mobile users with IT background and IT experts in Kenya. A research in future should be conducted to capture the input of non IT respondent which may be different.

VI. Future work

Through data analysis of the information gathered the researcher was able to identify the main contributing factors in vishing attacks, this key entities of vishing attacks can be used in creating a conceptual model for vishing attacks. The conceptual model will be used as tool to aid in detection of vishing attacks. More studies should be done in future to investigate the underlying theory on the three entities of vishing attacks.

VII. Acknowledgments

The authors the interviewees for their contribution.

References

[1]. Kim, S.E. and Yang, Y.J. (2008) the evolution of tele-financial fraud: An analysis of offender victim interaction structures and respondence to 'voice phishing'. Korean Journal of Public Safety and Criminal Justice 32(1): 103–149.

[2]. CAK. (2016). quarterly sector statistics report fouth quarter for the financial year 2015-2016 (april-june 2016). Nairobi.

[3]. Mulwa, D. K. (2012). A survey of insider information security threats management in commercial Banks in Kenya. Nairobi: University of Nairobi.

[4]. Kigen, P. M., Kimani, C., Mwangi, M., Shiyayo, B., Ndegwa, D., Kaimba, B., & Shitanda, S. (2015). Kenya Cyber Security Report 2015. Nairobi.

[5]. Muthengi F. M., 2015. On combating current and emerging cybercrimes in Kenya. International Journal of Education and Research, Vol. 3 No. 11 November 2015.

[6]. K. Choia, J. Leeb and Y.ChunbLijun, (2015) Voice phishing fraud and its modus operandi. Korea.

[7]. Bezuidenhout, M., Mouton, F., & Venter, H. (August, 2010). "Social Engineering Attack Detection Model:SEADM," in Information Security for South Africa. IEEE, (pp. 1-8). Johannesburg, South Africa.

[8]. Clarke, R.V. and Cornish, D.B. (1985) Modeling offenders' decisions: A framework for policy and research. In: M. Tonry and N. Morris (eds.) Crime and Justice: An Annual Review of Research. Chicago, IL: University of Chicago Press 6, pp. 147–185

[9]. Mouton, F., Leenen, L., & Venter, H. S. (04 Feb. 2016). Social Engineering Attack Detection Model: SEADMv2. 2015 International Conference on Cyberworlds (p. 223). Pretoria, South Africa: CPS.

[10]. L. Janczewski and L. Fu (2010) Social Engineering Based-Attack: Model and New Zealand Perspective. Proceeding of the International Multiconference on Computer Science and Information Technology pp. 847-853.

[11]. Alnajim, A. and Munro,M. "An evaluation of users' tips effectiveness for Phishing websites detection," in Digital Information Management, 2008. ICDIM 2008. Third International Conference on, 2008, pp. 63-68.

[12]. Robson, C. (2011).Real World Research: A Resource for Users of Social Research

[13]. Kothari, C.R. 2004. Research methodology: Methods and techniques. New Age International (P) Ltd, Publishers.

[14]. Mugenda,O.M. and Mugenda, A.G.(2012). Research Methods Dictionary. Nairobi: ARTS Press.

[15]. Crouch, M., & McKenzie, H. (2006). The logic of small samples in interview-based qualitative research. Social Science Information, 45(4), 18. doi: 10.1177/0539018406069584

[16]. Marshall, M. N. (1996). Sampling for qualitative research. Family practice, 13(6), 522-526.

[17]. Dunham, K. (2009) "Chapter 6 - Phishing, SMishing, and Vishing," in Mobile Malware Attacks and Defense, D. Ken, Ed., ed Boston: Syngress, 2009, pp. 125-196.

Author's Profile

Mr. Elijah Mwandata Maseno, a Masters Student in field of Data Communications and networking, KCA University, Kenya. He received his Diploma in Telecommunication Engineering in 2011 from Defence Forces Technical College, in Kenya, Bachelor of Computer Information Systems in 2015 from Kenya Methodist University, Kenya. He is a Lecturer at the Department of Information Communication Technology at Defence Forces Technical College, Kenya. His research interests include among others Data communication and Networking, Social Engineering and Cyber Security. E-mail: masenoelijah@gmail.com