A Survey of Awareness of Social Engineering Attacks to Information Security Management Systems at Kibabii University

Mbuguah S M.[1]& Otibene T .O[2]

1-Kibabii University

Corresponding e-mail: smbugua@kibu.ac.ke&totibine@kibu.ac.ke

Abstract

Computer based system are socio-technical system in nature. The security of the system depends both on technical aspect and also social aspect. The social aspect refers to people in contact with system commonly referred to as wetware. To attack the system you may consider to target the technical or wetware. Social engineering is based on exploiting human traits that make human susceptible to these attacks. The aim of this paper was establish how aware the staff of Kibabii are of these attributes and how these attributes could be used by social engineers to penetrate Information Security Management systems at Kibabii University. A survey research was adopted with a questionnaire being developed using Google application, was administered online to all staff members of Kibabii University. A descriptive analysis was carried out on feedback. The finding is that to a large extent the sampled staff are aware of these traits but there need for awareness training to enhance the information security managementsystem of Kibabii University.

Key words:

1.0Background

The increased dependency on reliable data communication networks has created a need for ever increasing computer security. Many technological options exist for security in both hardware and software and these implementations pose formidable threats for hackers. However social engineering bypasses the electronic security measures and targets the weakest component of networks - the human users (Kvedar et al., 2010).

Susceptibility to social engineering attacks stems from a lack of formal security management as well as limited education regarding social engineering. Computersecurity organizations such as SANS are pushing for increased defenses against social engineering (Allen 2004), but until the general business community realizes the threat, very little will be done to implement policies to protect themselves compared to the efforts made to establish electronic safeguards against traditional hacking techniques. Kvedar et al.(2010) carried out some research with the aim of proving the viability of social engineering as a method of network attack, as well as display the need to increase education and implement measures to protect against it.

Computers are designed to provide an unconditional response to a valid instruction set. The same instruction set is used to create different layers of security privileges for different category of users. Social engineering supersedes the explicit nature of machines and focuses on human emotion and tendency. Wetware has been coined to represent the human attached to the computer. Wetware is just as vital to the computer's security as any hardware or software (Allen 2004). It is this wetware that social engineering exploits.

Computers can completely secure information to prevent unauthorized access. This could easily defeat the goal of having information from being readily accessible when needed by privileged users. The goal for a social engineer is to manipulate these authorized users to gain access to privileged information. Dolan

considers social engineering as the "management of human beings in accordance with their place and function in society" (Dolan 2004).
Social engineers prey on humans' desire to be helpful, tendency to trust people, fear of getting in trouble, and willingness to cut corners. They have found out that exploiting weakness in human nature is much easier than exploiting flaws in encrypted software. Instead of physically breaking into bank's safe, it is much easier if one can get the lock pin combination code from a bank worker (Mbuguah & Wabwoba 2015).

Allen avers that the four phases of social engineering are: information gathering, relationship development, execution, and exploitation (Allen 2004). During the first phase, information gathering, information about company is gathered with the aim of finding weakness that can be exploited and ways of avoiding arrest within the organization. The second phase, relationship development, rapport and trust are developed with contact person within the organization. The third phase is actual execution of the attack where the information is actually exchanged. Finally, the last phase is utilizing information.
Thornburgh (2004) says that an attack is successful only if the target feels compelled to give up the information in spite of their gut instinct. While Manske (2000) saysthat a successful attack bypasses anything that would be in place to ensure security, including firewalls, secure routers, email, and security guards. This causes unrest and beats the security of encryption.
Winkler and Dealy (1995) provide advice on how to secure a network against social engineering. The list includes not relying on common internal identifiers within an organization, implementing a call back procedure when disclosing protected information, implementing a security awareness program, identifying direct computer support analysts, creating a security alert system, and social engineering to test an organization's security. Dolan (2004) beef up the list by adding; password policies, vulnerability assessments, data classification, acceptable user policy, background checks, termination processes, incident response, physical security, and security awareness training.

Social engineering tactics include impersonation of an important user, third-party authorization, in person attacks, dumpster diving, and shoulder surfing. Dumpster diving involves sifting through a target's waste in search of critical information. However shredders should be used to shred any documents destined tothe dustbin. Shoulder surfing is a basic social engineering attack based on attempts tosteal passwords and login information by watching a user input the data. This especially true in automated teller machine (ATM) halls, where users do not take precaution to block any other users from seeing them keying their pin numbers. The result is that a lot of clients have lost their funds. One person lost some money from his MPESA account when he unknowingly let a young man know his pin number. The young man picked the phone and transferred money from the person account to his. However forensic audit helped track down the culprit (Mbuguah & Wabwoba 2015).
Attackers prefer to remain unidentifiable to protect themselves, some tell-tale signs of an individualattempting a social engineering attack include refusal to give contact information, rushing the process, name-dropping, intimidation, small mistakes, and requesting forbidden information or accesses.
Reverse social engineering tact involves creating a situation where the targeted individual actually seeks the attacker for assistance, which provides the attacker with the opportunity to establish trust (Dolan 2004). A common tendency in human nature is for one to feel indebted to their benefactors. Reverse social engineering preys on this tendency. Not only does the target trust the individual, but also feels indebted the attacker, and will share out information he may not otherwise share out to settle that debt.
In Kenya people have been conned by people pretending to be business men expecting a certain a transaction to go through (Mbuguah & Wabwoba 2015). After they have developed rapport with the victim they initially ask some money before gradually increasing the amount then finally logging off, leaving the victim high and dry. Another type of fraud executed by Kamiti maximum prisoners is to exploit the greed of their victim. They call the victim informing them that they have won some lottery. They require some

information from them, including their MPESA pin numbers. Only for the victim to realize that the conmen have cleared what money they had in their accounts. Once again audit trail by service provider Safaricom located the location of the scam to Kamiti and other prisons in Kenya.

2.0Related studies

One of key study was entitled Understanding Scam Victims: Seven Principles For Systems Security .The researchers tried to find out on thepsychology of scam victimsAl, L. E. (2009). Researchers then identified traits that make people vulnerable to scams. These traits were published in ACM vol 54 journal as shown in table 1.

Table 1: Scam Victims

Principle	Cialdini (1985-2009)	Lea et al, (2009)	Stajano-wilson (2009)
Distraction		~	X
Social compliance(Authority)	X	-	-
Herd (Social proof)	X		-
Dishonesty			X
Kindness	~		X
Need and greed (Visceral Triggers)	~	X	-
Scarcity (related Time)	X	-	~
Commitment and Consistency	X	-	
Reciprocation	X		~
~ -------Lists a related Principle Also lists this principle X First identified this principle			

Source (ACM Vol 54)

Wilson (2011) says that the finding support their thesis that systems involving people can be made secure only if designers understand and acknowledge the inherent vulnerabilities of the human factor. Their three main contributions were: First hand data not otherwise available in literature; Second they abstracted seven principles; Third they applied the concept to more a general system point of view.

They argued that behavioral patterns are not just opportunities for small scale hustlers but also of the human component of any complex system. They suggested that system security architect should acknowledge the existence of these vulnerabilities as unavoidable consequence of human nature and actively build safeguards to prevent their exploitation Wilson, F. S. (2011) However they did not attempt to model the relationship between the traits and system attackability(Mbuguah et al. 2013).

The identified human traits are dishonesty, social compliance, Kindness, Time pressure, Herd mentality, greed/need and distraction. Personality traits models do exist. Researchers have identified traits that make human beings susceptible to social engineering attacks and have extended this to system view. Researchers have also identified that the human being is the weakest link in system security (Mbuguah et al.2013)

Mbuguah et al (2013) did extend these concepts by not only modeling the traits as applied to software systems but also introduced some metrics that are theoretically and empirically sound. He also published algorithm for determination of these metrics.

This paper is then application of these concepts to Kibabii University in a bid to assess the level of awareness of social engineering attacks at Kibabii University.

3.0 Methodology

For this paper a survey methodology consisting of twenty questions was administered online to Kibabii University staff through their email addresses. The staff numbers members are three hundred and thirty (330) and respondents were thirty three (33) which constituted about 10% which is an appropriate sample size (Mugenda & Mugenda 2003). The questionnaire was set on Google application. Questions were set out

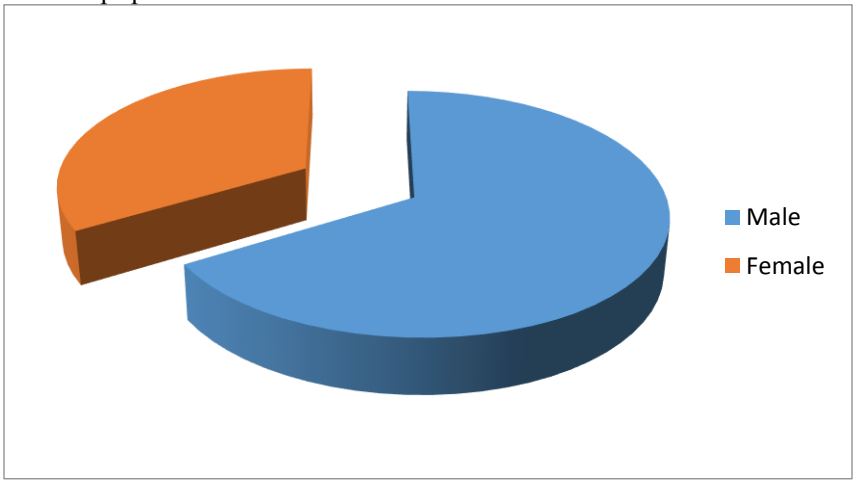
and the participant requested to respond by clicking on appropriate button. On completion participant pressed a submit button to relay the information back to the researchers. The application did compute the percentages for each response. Test retest was applied to seven attributes and average score computed. Hence descriptive analysis was done whose findings are represented below.

4.0 The results

The first five questions were general information and the trends

4.1 General information

a) Question one was on the gender composition of the respondents. The results were that of sample population 63.6 % were male while 36.4% were females.



b) Job Category

The distribution of the respondents as far job category was:
Administrative – 48.4%, Technical – 30.3% and Academic – 21.2 %

c) The question sought to find out whether the staff new who a social engineer was and only 60.6% could correct define a social engineer while 39.4 % could not.

d) Whether people seek the identification of strangers before serving them by requesting for ID or gate pass. 87.5% did while 12.5% did not.

e) This Question sought to find out whether they could allow a visitor mess up in their office whether the visitor had some identification document or not. 97% declared they could while 3% could take no action.

4.2 Seven Attributes

a) Social compliance-a tendency for people to obey authority or do as required of them by their superior or people in authority. The question was to find out whether the members of staff were aware that this trait exploited by conmen to take advantage us.

QUESTION	Strongly Agrees	Agree	Do not Know	disagree	Strongly
7	90.9	9.1	0	0	0
14	24.2	24.2	12.2	24.2	15.2
9	24.2	18.2	21.2	27.3	9.1

For this attributes the positives that strongly agrees and agree (100+ 48.4+ 42.4 = 190.8)
The average 190.8/3 = 63.6

The result indicates that 63.6 % are aware that social compliance can be exploited by con artist to penetrate systems. 36.4 % are not aware. This is higher percentage that can be easily exploited; hence the need of training to enhance the awareness.

b) Time pressure-a trait of a psychological urgency attributed to insufficient time for completing required tasks. The question wanted to find out whether the participants were aware that conmen to take advantage us by hurrying us.

QUESTION	Strongly Agrees	Agree	Do not Know	disagree	Strongly
8	78.8	21.2	0	0	0
13	30.3	51.5	6.1	9.1	3
15	42.2	33.3	6.1	9.1	9.1

This gives a total of 257.3 and an average of 85.8%.

This means that 85.8% of the staff members are of the effect of time pressure but 14.2% are not aware. There is need for training to reduce this gap.

c) Kindness- compassion. The trait of a person having a high level of agreeableness in a personality test, usually the person is warm, friendly, and tactful. Or having an optimistic view of human nature and getting along well with others. The trait can be used by conmen to take advantage of us.

QUESTION	Strongly Agrees	Agree	Do not Know	disagree	Strongly
11	81.8	15.2	0	3	0
16	27.3	42.4	6.1	18.2	6.1

The average for the positive or correct answer 83.3% and 16.7 % are not aware. There is need for training to breach this gap.

d) Greed/Need-Greed refers to a human trait of wanting more and more of something. While need is the want of something urgently and desperately. This trait can never be exploited by conmen breaking into information security systems.

QUESTION	Strongly Agrees	Agree	Do not Know	disagree	Strongly
12	63.6	33.3	3.1	0	0
17	42.4	30.3	0	9.1	18.2

The participant who responded positively were 84.8% and negatively 15.2%. There is need for awareness training.

e) Herd Mentality-the trait of a tendency for an individual to follow group thinking. To do something because most people are doing the same even though this may be against their better judgment. This trait could be negatively exploited by conmen to take advantage us.

QUESTION	Strongly Agrees	Agree	Do not Know	disagree	Strongly
10	21.2	48.5	12.1	15.2	3
18	51.5	33.3	3	12.1	0

The Positives responses were 77.25% and negative 22.75%. The aspect of herd mentality requires more training.

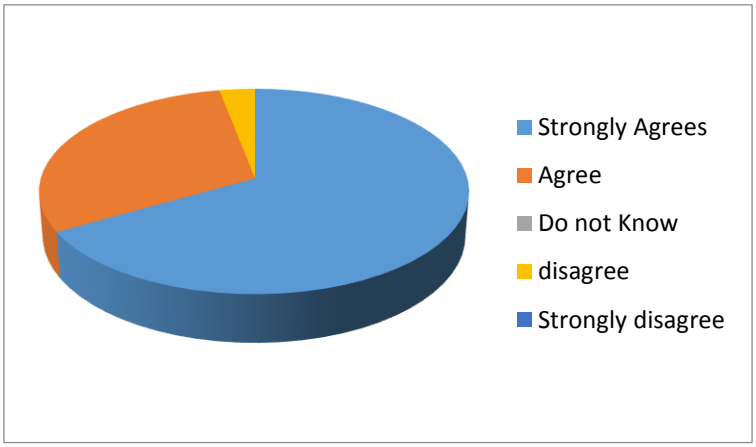
f) Distraction. The trait when a secondary task obstructs/slows the user from efficiently and effectively fulfilling the time-critical main task. This trait could be negatively exploited by conmen to take advantage of us.

QUESTION	Strongly Agrees	Agree	Do not Know	disagree	Strongly
6	90.9	9.1	0	0	0
19	36.4	51.5	3.0	3.0	6.1

The positive were at 81.85% and negative were at 18.15%. There is need for training to reduce this gap.

g) Dishonesty – the trait of being not truthful or cheating. This trait could be negatively exploited by conmen to take advantage of us in penetrating security barriers.

QUESTION	Strongly Agrees	Agree	Do not Know	disagree	Strongly disagree
20	66.7	30.3	0	3	0



People appear to appreciate that dishonesty can lead to social engineering attack. The positive respondent was at 97% while the negative was at 2%

5.0 Conclusion

We can conclude that in general the sampled staff are to a large extent aware of the human traits that can make one susceptible to social engineering attack. However there is still a significant mass that requires further awareness training to reduce the vulnerabilities of the Kibabii University system. Everybody should be fully aware of the ever changing scenario of attacks to make the system impenetrable.

The recommendation is further training for members of staff plus further monitoring including penetration testing

Reference

Al, L. E. (2009) Al, L. E. (2009). *The Psychology of Scams:Provoking and Commiting Errors Of ,Judgement.* London: University of Exeter School

Allen, M. 2004. Social Engineering: A means to violate a computer system from,http://securitytechnet.com/resource/security/hacking/1365.pdf.

Dolan, A. 2004. Social engineering. SANS Reading Room. Retrieved November , 2011from http://securitytechnet.com/resource/security/hacking/1365.pdf.

Kvedar D., Nettis M & Fulton S.P(2010). The Use of formal Engineering techniques to identity weaknesses during computer Vulnerability competition .*United, States Air force Academy*

Manske K.(2000). Amn Introduction to Social Engineering. Information Security Journal: A Global perspective 9:1-7

Mbuguah S.M. & Wabwoba F. Attackability Metrics Model for Secure Service oriented ,Architecture published by Lambert ISBN 978-3-659-66885-2

Mbuguah S.M. Mwangi, W. Song P.C, Muketha G.M .(2013) Social attackability metrics in the ,*International journal of information technology research ISSN-2223-4985* Volume 3 , No. 6

Mugenda, O. M. and Mugenda A.G (2003). *Research Methods.* Nairobi: ACTS.

Thornburgh T.(2004). Social Engineering: the Dark Art: *In the proceddingof the 1st. , conference on information curriculum development, GA, 133-135*

Wilson, F. S. (2011) Wilson, F. S. (2011). Understanding Scam Victims:Seven Principles For ,system ,Security. *Communication Of ACM, Vol 54,No3* .

Winkler I & Dealy B.(1995) Information Security Technology. Don't rely on it . A case, Study in Social engineering. *In Proceeding of the 5th USENIX/UNIX. Symposium, Salt Lake City Uta*