Towards Securing Organizational Data against Social Engineering Attacks

Azaabi Cletus
Department of Mathematic/ICT
St.John Boscos College of Education, Navrongo, Ghana

Ussiph Najim, PhD
Department of computer science, Kwame Nkrumah University of Science and Tehnology, Kumasi, Ghana

ABSTRACT
The study was carried out mainly to investigate how data of organizations can be secured against Social Engineering (phishing) attack using a model. The phenomenon of social engineering is emerging as a major security threat to organizations' information systems accounting for about thirty (30) percent of all security breaches globally with its attendant negative impact. It exploits the vulnerabilities inherent in users of information systems using psycho-social skills to influence them to divulge confidential information that is usually used later to gain access to a targeted technology system. Thus to secure data against social engineering attacks, the defense should be modeled around the user who is often considered as the weakest link in the information security chain.

The paper used the Design Research method by proposing a model which was translated into web application system that identified vulnerable users to Socially Engineered attack by using their responses to a scam emails administered to them in phases. Purposive sampling was used to select customers of the community Bank where the study exercise (Simulated Phishing Attack) was conducted and evaluation of the efficiency of the model was carried out. Data was collected using log files and was analyzed using simple descriptive statistics and the results presented using frequency tables, bar charts and pie charts.

The result showed that, users are highly vulnerable to social engineering attacks, and this vulnerability can be reduced by adopting the CEMASEA training model since it can build the resistance of users or reduces vulnerability by 69.05%.

It was recommended that, for organizations to build social engineering resistance or immunity in particular and a sound security culture in general, Ethical Penetration Testing or Red Team Assessment should be adopted by all organizations periodically using a novel CLEMASEA model.

GENERAL TERMS
Information Systems Security, Social Engineering, Confidentiality, Integrity, Availability

Keywords
Penetration testing, Red Team Assessment, social engineering compliant user, Non Social Engineering Compliant user CLEMASEA model.

1.1 INTRODUCTION
The existence of small or large organizations depends largely on its information which of late is usually stored in Computer Systems. The information/data kept by organizations include but not limited to its trade secrets, confidential reports, product manuals, employee vital records, Product information, designs, plans, patents, source codes, drawings, Financial records, market needs research assessments and a company's own customer information , foreign/ local intelligence reports of states etc. As a valuable asset, data/ information need to be protected from unauthorized disclosure, access, and or modification. Because of the value of such information/data, it is susceptible to many attacks usually for the purpose of self-education, financial gain, and industrial espionage, economic and geo-political consideration (Nohlberg, 2007). Thus, a breach in an information system could be costly to the individual, organization or even a nation. Therefore, the need to ensure security mainly confidentiality, integrity and availability known as the CIA TRIAD must be ensured by all stakeholders in the information security chain (Pfleeger (2003)).

Ironically, Security Experts in the industry have over concentrated on the technical protection procedures i.e. firewall installations, anti-virus schemes, Intrusion Detection Systems (IDS), hardware and software upgrades, patches, and logical control procedures (traditional methods) with little or no attention to the security of the user who is often considered as the weakest link in the information security chain making it easy for cybercriminals to rather target the user since it is easy to manipulate the user than the technology (Björck, 2005, p. 237). Taking advantage of the human vulnerability in the firm or information security chain to gain confidential information usually to use it to attack an information technology system later is known as social engineering.

Social engineering is an attempt to convince people to reveal information that would result in illegally seeing, using or haven access to confidential information. (Mitnick et al, 2011). It is done using social, psychological, power of persuasion and influence to convince victims to divulge the needed information and uses techniques such as phishing, pharming, dumpster diving, reverse social engineering, telephone call, piggybacking, and others. The social engineering phenomenon as threat to Information Security has gained global notoriety due to the proliferation of the internet which makes it easy for attacks from remote location.

Kowalski,(1994) opined that security of organizations must be looked at holistically, Hence the SBC (Security By Consensus)model. The model embodies the technical, Socio-Technical and legal issues in ensuring holistic security in an organization. He suggest that the user or owner of the information system has the potential to create an environment that will make him/her a victim by his/her legitimate interaction with the system and thus needs to be secured as well.
Since the user is the target in this kind of attacks, any defense procedure to protect data /information against it should be modeled around the user taking into consideration the psycho-social factors that makes social engineering less cumbersome. This will ensure that the user becomes conscious about behavioral change both online and offline regarding the release of confidential information.

Chapman, (2010) opine that, behavior change of humans (users) usually follow four stages; Unconscious Incompetence, Conscious Incompetence, Conscious Competence and Unconscious Competence. So in trying to build security consciousness of users to information security or make them aware of the risk involved in their behavior online and offline regarding security, the individual needs to pass through these phases. At the Unconscious Incompetence (UI) Stage, the user will be exposed to the phenomenon or the threat that makes his or her to become aware that he/she is at a security risk regarding his/ her behavior in the organization or outside since any confidential information divulged into the wrong hands can have disastrous consequences.

The second stage is the Conscious Incompetence(CI) whereby the user now accept that he/she is incompetent to adequately performs securely and thus may begin to find ways to learn to acquire skills in handling the problem making him/her now Consciously Incompetent.

The third stage is the Conscious Competence (CC) level where the user has now acquired enough knowledge and experience but still not able to function well without difficulty. At this stage the user is security conscious but with difficulty.

The last and final stage is the Unconscious Competence (UC), at this stage the user has now imbibed all the rudiments of the act or skill or behavior change and act consciously without thinking since it has become part and parcel of the individual's behavior and which is the desired goal of every organization regarding security culture (S. H. Von Solms & Von Solms, 2008).

Thus a system to secure organizational data against socially engineered attacks must target the behavior of the user, be repetitive to enable the user acquire behavior change.
To achieve this, a model known as "Cletus Model Against Social Engineering Attacks" (CLEMASEA) was proposed, describing how social engineering works as shown in figure 1 below:

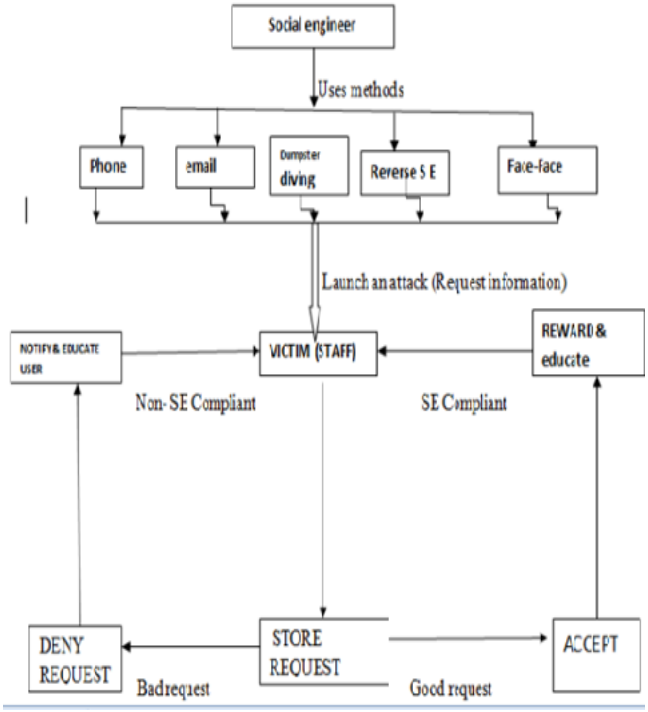

Figure 1. **CLEMASEA Model**

This was translated into a web application system which was used to conduct a simulated phishing attack on staff and customers of a Bank to ascertain the level of vulnerability of users to scam emails (phishing), the effect of training on such users' behavior and the overall efficiency of the model as a tool to secure organizational data/ information against socially engineered attacks.

2.1 METHODOLOGY

The choice of a research method depends largely on the problem under study. The main research methods available include qualitative, quantitative, mixed and the research and development paradigms such as design and constructive research (Reeves, 2000).

The Design Research Method was used for this paper. This method is a procedure for producing innovative constructions to solve real world problems and to make contribution to knowledge and theory (Lukka, 2003). Since the objective of the study was to produce a novel solution to both practically and theoretically relevant problem in society such as Social Engineering, the Design Method was deemed to be most appropriate. This is because the validity and reliability of this paradigm can be ascertained i.e whether it produces workable solutions to the identified problem. It also ensured the neutrality and criticality of the researcher while producing innovative constructs. To do that, a real world phishing attack needed to be conducted on users and the results analyzed. This was done by translating the model into a web application system with an automatic online training system attacked to a simulated socially engineered phishing attack on users of a bank.

2.2 DATA COLLECTION METHODS.

For the purpose of this paper, the log files method was used to gather the primary data as the system was required to automatically train and record the number of users and their behaviors and the secondary sources which included the review of journals, textbooks and others. The log files records the behavior of users in a platform and it is automatically collected at low cost. (Randolph, 2007). One good side of this method is that, the data collected need no encoding and beside the collection process is unobtrusive. One weakness is that the method could lead to the gathering of overwhelming data (Randolph, 2007). The data gathered from this exercise formed the main data for the evaluation of the system to ascertain the level of vulnerability of users to social engineering attacks and the efficiency of the model as a tool for building user immunity against security attacks.

2.3. SAMPLE METHODS

The universe of this study was all users of the internet specifically email. But due to the difficulty in getting all these users, Customers of a Community Bank and Branches was chosen with all staff and some customers as the target population, but a total of one thousand two hundred and fifty (1250) staff and customers were considered to respond to the scam email as the sample frame. This was done using purposive sampling which is one of the non-probabilistic sampling methods. The sample was purposively done because the researcher needed to group all the customers that had emails and are active users on the system. According to Palys (2003), Purposive sampling doesn't aim for formal representativeness. He contends that people and locations are intentionally chosen because they meet criterion for inclusion in the study. Consequently the sample was disaggregated into whether the customer had an email and was an active member on the system and such were chosen and that formed the bases for their inclusion in the study.

2.4 DATA ANALYSIS TECHNIQUES

The Designed Web Application System for the simulated email administration or phishing included a feature that recorded the entire user behaviors on the system and kept track of each activity. All active users were recorded; the Social Engineering Compliant staff (non- vulnerable users), the Non-Social Engineering Compliant (vulnerable users), and those who do not use the system or did not respond to the emails. These statistics column contained all the necessary data needed for analysis when the model was implemented. This analysis assisted the researcher to evaluate, whether the designed application was capable of solving the problem i.e. securing organization's data against social engineering attacks by looking at the behavior of users to the scam mails before an online training and after the training**.** Simple percentages, pie charts, and bar charts were used to present the data.

2.5 TRANSLATING THE MODEL INTO A WEB APPLICATION SYSTEM.

To be able to test the model and the web application system developed. The CLEMASEA (Cletus Model Against Social Engineering Attack) was proposed, as part of the study as shown in the figure 1 above**.**

This model was developed for preventing social engineering attacks (phishing) by building the immunity of users based on the Conscious Competence Learning Model (Chapman, 2010).

Many Authors concede that, user education, training, and awareness creation are the vital requirements to protecting users and organizations from falling prey to social-engineering attacks such as Phishing, face-face attacks, etc (Dodge et al,2007; Jagatic et al, 2007,Kumaraguru et al, 2009;Dodge et al., 2007; Kumaraguru et al., 2009; Mann,2008). On the bases of that, any activity to secure data against socially engineered attacks must involve any of these. The following explains how the model works:

A Social Engineer uses any of the social engineering methods to launch an attack on a victim i.e. staff/customer of the organization by requesting for sensitive information as shown in the figure below.
If the user is Security Conscious, he/she refuses to provide the requested information, that means the individual is Social Engineering Compliant(SEC)
The system generates refresher training for the user on social engineering as a threat to data security in the organization and personally.
Where a user is not social engineering compliant and thus provides all the requested information, that means the individual is Non Social Engineering Compliant (NSEC), the system generates a warning to the user indicating the risk of his/her actions. Thus, Subsequent notification/training of such to the individual will build the immunity of such a person to become unconsciously competent which is the expectation of all organizations (Von Solms &Von Solms, 2008).

In order to ascertain whether the model is effective in ensuring attacks using Social Engineering tactics such as phishing, the logic of the model or construct was translated into a Web Application System and used to evaluate on users in a real life situation in a Bank**.**

2.5.2 DESIGN OF THE WEB APPLICATION SYSTEM

To be able to test the model, it was developed or translated into a web application system and used to conduct a simulated phishing attack in a Bank.
An SQL database structure to store the behavior or user reactions was designed; administrative login interface that gives the administrator the opportunity to go into the system, a mass message interface to distribute the scam mails, and an email registration interface to register all email accounts of users were developed. A clone website of the selected organization was created in which victims were diverted into when they clicked on a link. This cloned website which looks exactly like the real website of the said Bank was enough to convince the victim that the scam message was coming from a legitimate source; their Bank. These formed the foundation for the administration of the simulated phishing attack.

Four different types of scam emails were created and distributed to the participants; one on Database Crash, one Lottery win, one on Bonus and the other one on accidental Loan deduction. All the users were divided into four groups where each group was given a particular scam message for the first week. In week 1, the 'LOTTERY WIN' scam was administered to group 1. Group 2 was given the 'DATABASE UPGRADE' scam, group 3 was given the 'LOAN

DEDUCTION' scam and finally group 4 was given the' BONUS' scam for that week as can be seen in figure 4.2.

In the second week of the exercise, the participants were given different scam messages as indicated in figure 4.2. Group 1 now received the 'BONUS' scam; group 2 was given the 'LOAN DEDUCTION' scam, group 3 this time was given the 'DATABASE UPDATE' scam while group 4 now received the 'LOTTERY WIN' scam.

The Database scam emails was asking customers to provide their account numbers, usernames and password the Bank update their records because of a database crash, Lottery Win scam requested the user to provide same details for the bank to process a visa of a USA lottery, that the bank entered on behalf of the customers, a third scam mail was the fact that the customer was selected by the bank to receive some bonus for customer loyalty to the Bank, and fourth one was an erroneous loan deduction from the customer account and the needed the details to confirm or otherwise as shown in the figure below. By comparing the results of the exercise in phase one and that of phase two, it was possible to identify the vulnerable users (Non-Socially Engineering Compliant) and non-vulnerable users (Social Engineering Compliant) and those who abstained from responding to the scam mails. The percentage of user behavior changes before and after the administration of the exercise in both phases were compared takas shown in figure 2.

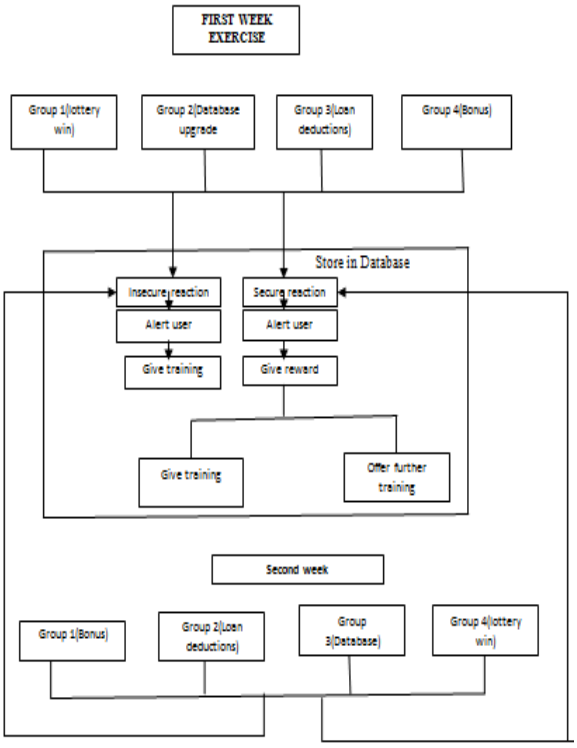

Figure 2. Administration of the exercise

3.1 RESULTS AND FINDINGS

The purpose of the study was how organizations can secure their data against social engineering attack. A model was proposed and was developed into a web application system to test the vulnerability of users in an organization against a named social engineering attack; phishing, and how this system can help organizations protect their data against social engineering (phishing) attack. The result of this exercise is presented below.

3.2 SOME USERS' RESPONSES TO THE PHISHING ATTACK EXERCISE

The researcher received three responses from the participants that gave an indication that they were aware of some security implications of a the BONUS scam, another user responded with the following email message: '*You have my details already that showed that I deserved a bonus, then what details again? 419 like you*".

Another user requested for my location and contact person so that he can bring the particulars in person and can appreciate the effort.

3.3 RESULTS FOR PHASE ONE

Table 1. Secure and insecure users in phase one

Users	Frequency	percentage
Secure users	**863**	**86.04**
Insecure users	**140**	**13.96**
Total	**1003**	**100**

In the first phase of the exercise, a total of 1003 representing 80.24% of the total sample checked their emails during phase one which means they were active users on the system. Out of this number, 863 of these users representing 86.04% reacted incorrectly or insecurely (fall prey) and were automatically trained by the Automatic Online Phishing Training module, while 140 of the users representing 13.96% acted securely. The entire secure users i.e. 13.96% were giving the online training as shown in table 1. The results are as shown pictorially on figure 3 below using a Bar chart..

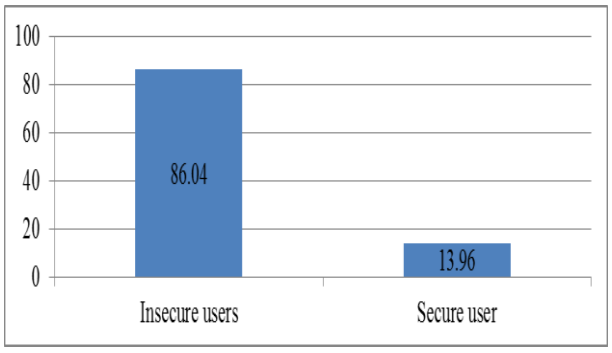

Figure 3: Bar chart showing insecure and secure users in phase one of the exercises

3.3.1 Results Per Attack Type In Phase One

From the pie chart shown, Bonus scam had 341 respondents representing 39.51% that reacted insecurely to that scam in the first week.

The lottery scam had 333 respondents representing 38.59% that also fell victims to the attack during the first

phase. The number of respondents in the Database upgrade was 139; representing 16.11% of the insecure users while that of the Loan deduction scam recorded only 50 respondents that represents 5.79% of the insecure users.

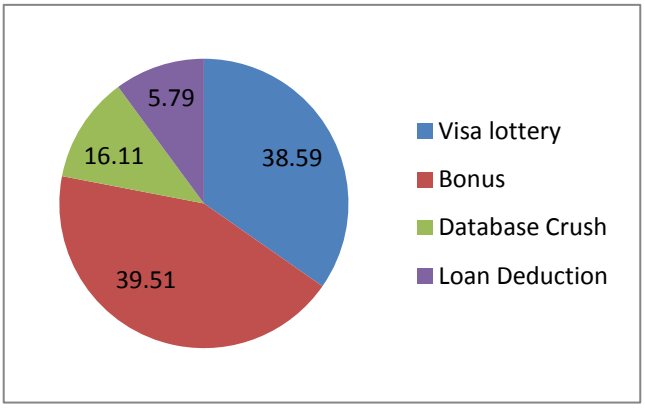

Figure 4. Pie chart showing attack type for phase one

.3.2 RESULTS FOR PHASE TWO

Table 2. Secure and insecure users in phase two

Users	Frequency	percentage
Secure users	**966**	**85.94**
Insecure users	**158**	**14.06**
Total	**1124**	**100**

In the second phase of the exercise, a total of 1,124 of the population were active on the system. Out of that, 966 of the subjects representing 85.94% reacted securely this time.158 respondents in this group representing 14.06 % acted insecurely this time as showing in table 2 and which is represented in a bar chart in figure 5.

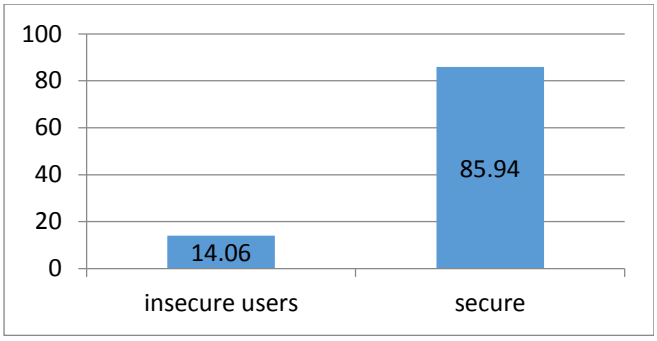

Figure 5: Bar chart showing secure and insecure users in phase two of the exercise

3.3. RESULTS PER ATTACK TYPE FOR PHASE TWO OF THE

The results of the exercise per the type of attack as was done in phase one was considered. Out of the total number of 1124 users, 966 users representing 80.24% acted securely whiles 158 users representing 14.06 acted insecurely. The results of the various attack type is represented as shown in the pie chart below.

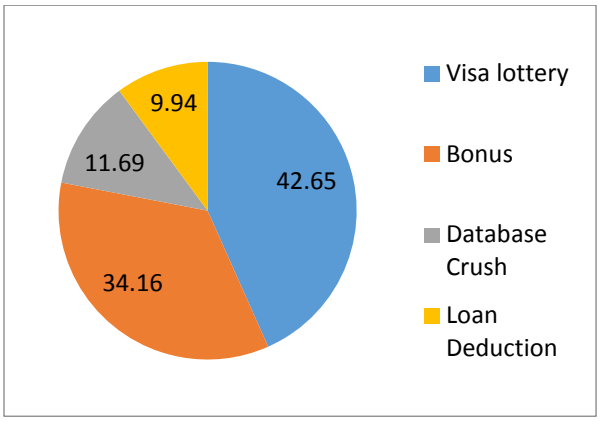

Figure 6: Pie chart showing attack type

From the pie chart showing above, 330 of the subjects representing 34.16 % of the total active users who reacted to the Bonus scam mail behaved securely. With the USA Visa Lottery, 412 respondents representing 42.65% acted securely to the attack during the next phase. The number of respondents in the Database upgrade this time was 113; representing 11.69% of the secure users while that of the Loan deduction scam recorded only 96 subjects that represents 9.94% of the secure users. Both secure and insecure users, incidentally, were trained.

4. DISCUSSIONS

The main topic of the study was securing organizational data against social engineering attacks using a model. To effectively carry out the study to meet the intended objectives, a model or construct was suggested depicting a socially engineered attack such as phishing. The suggested model was translated into a web application system as a way to test the efficiency of it as a tool against the phenomenon and identifying the vulnerability of users. Research abounds that, user education, training, and awareness creation are the vital requirements to protecting users and organizations from falling prey to social-engineering attacks (Dodge et al, 2007; Jagaticetal, 2007,Kumaraguru et al, 2009;Dodge et al., 2007; Jagatic et al., 2007; Kumaraguru rom et al., 2009; Mann,2008).

Results from the study showed that, in the studied organization, some level of knowledge of social engineering awareness is observed by some employees. This was demonstrated by some of the comments received from the subjects as indicated in the results section where chicky and insulting answers/questions were giving. The implication of this is that some users in organizations have some level of awareness of social engineering as a threat such as phishing. However, the number of such respondents was only three representing an insignificant percentage of the population under study. Consequently, organizations should not assume that all users are totally unaware of the security threat posed

by social engineers. But adequate training is required to maximize security against socially engineered attacks.

On ways organizations can secure their data against social engineering attacks (phishing), by looking at the first phase of the exercise, a total of 1003 users representing 80.24% of the total sample checked their emails which mean they were active users on the system. Out of this number, 863 of these users representing 86.04% reacted incorrectly or insecurely and were automatically trained by the online Training module attached, while 140 of the users representing 13.96% acted securely and also appropriately giving a refresher training accordingly.

In the second phase of the exercise, a total of 1,124 of the population were active on the system. Out of that, 966 of the subjects representing 85.94% reacted securely this time.158 respondents in this group representing 14.06 % acted insecurely.

A careful comparison from the analysis of the first and the second phase results of the exercise showed that the number of insecure users reduced by 69.05%. This means that, many users of information technology resources are not aware that the information they carry or work with within their computing systems are targets for cybercriminals. This make them (users) easily give out confidential information online about their company, personal private details when requested as in the researcher's scam emails. Thus, after been exposed to the scam emails in the first phase and training offered to vulnerable users in phase one of the exercises, majority of users learnt to be security conscious and in the second phase behaved securely. This confirms the Chapman Competence Learning module proposed in the literature review section of the study. Therefore, for organizations to ensure security against social engineering attacks, constant exposure of users to penetration testing or Red Team Assessment over a period of time will make users resistant to such schemes. This is a clear indication that the system can actually help protect organization's data by periodically exposing staff to simulated attack and offering training to them. It is worthy of note that, the efficiency and effectiveness of the system was about 69.05% as compared to a similar work by Jansson whose exercise efficiency was only about 46%.(Jansson& Von Solms, 2010).

Another way organizations can secure data against social engineering attacks as confirmed by many literatures is training, awareness creation and education. From the study, it's evident that, the use of a simulated system like CLEMASEA to be used as a tool to build the resistance of users is very necessary and subsequent deployment in organization can lead to users becoming unconsciously competent towards information security especially phishing attacks. These simulated fake attacks or penetration testing on users by exposing them to a variety of socially engineered attacks by using any of the vectors or methods employed by social engineers periodically with a training module attacked online or offline can build the resistant of the users to these attacks (Dodge et al., 2007; Hasle et al., 2005; Herold, 2010).

In conducting such simulated attacks, however, the level of enticement a mail carries has the potential to lure the users. This was confirmed in the study by the USA lottery visa scam mail which recorded the highest number of respondent in both phases.

On the tool that provides the most efficient protection against social engineering attacks, there are many tools that are aimed at providing security against socially engineered attacks. Many of these concentrates on the technology aspect such as anti-viruses firewall etc. But these tools are used by humans who are vulnerable as proven from the study. Thus, there is the need for a tool that integrates the psycho- social factors of the user into its design. This was included in the CLEMASEA model which was translated into a web application system and used to conduct the exercise. This was able to identify vulnerable users by their behaviors, offered them online training that made the users not to fall prey in the second phase with 95 percent efficiency. This is due to the fact that psychological, social, neuro-linguistic factors were all inculcated into the system. Therefore, an efficient defense system against social engineering (phishing) attack must be modeled around the user who is the target in such attacks. Such a tool must embody the psychology and social skill used in deception and can incorporate user awareness, training, education and policies into its design to achieve the desired effect (Jagatic et al., 200

5. CONCLUSION

It is an undisputable fact that the information revolution has led to many employees now categorized as knowledge workers and consequently handles organizational and personal confidential information digitally. This makes them vulnerable to cyber-attacks (Mann, 2008). Instead of attacking the technology system directly using brute force and other methods to get confidential information such as passwords, cybercriminals have resorted to attacking the weakest link in the information security chain; the user, to get the needed confidential information to attack mainly an information technology system; a concept referred to as social engineering (Mann, 2008).

Therefore, to protect organizational data against socially engineered attack such as phishing was the reason for this study. Thus, the study proposed a social engineering attack framework or model known as CLEMASEA which was translated into a web application system and used to conduct a simulated phishing attack on users of a community Bank in Ghana.

The study showed that the CLEMASEA was able to change the behavior of users, after been exposed to the simulated scam attacks. This was shown after comparing the first and second phases of the study exercises which showed a remarkable improvement of user's security behavior towards divulging confidential information.

The merits of the CLEMASEA system included the influence of user behavior towards security. This is because users have

pass through the stages to become Unconsciously Competent and therefore will be careful in divulging confidential information during both online and offline interactions.

The fact that users become aware of their vulnerability regarding information security, the personal desire to learn the acceptable standard behavior and best practices will lead to overall personal, organizational information security culture in the organizational setting.

Thirdly, since the model and exercise exposes the user to how insecure he/she is, it builds the foundation on which the need to be secured starts. This is usually the first step in building an information security culture in firms (S.H.Von Solms &Von Solms, 2008)

It was also realized that users are most likely to fall prey to certain type of email scams than others. From the study the USA Visa Lottery scam had the highest respondents. The percentage of this particular scam was 39.51% in the first phase of the exercise and 42.65 % in the second phase. Therefore, it can be concluded that in phishing attack, the choice of scam message is important in getting users react to the bait.

One major drawback of the CLEMASEA system is that, over reliance on the tool can lead to rigidity of users which can play counter- productive to the aims and objectives of the system. Even though information security is crucial in organizations, 'overprotection' can hamper the smooth flow of business processes. Thus, the use of the system should be done with caution so as not to defeat the intended aim.

6. **REFERENCES**

[1] Björck, F. (2005) Discovering Information Security Management. Diss.University of Stockholm. Report series No. 05-010, Stockholm.

[2] Chapman, A. (2010). Conscious competence earning model. Retrieved July 11, 2015, from http://www.businessballs.com/consciouscompetencelearningmodel.html.

[3] Dodge, J., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. Computers & Security, 26(1), 73-80. doi:10.1016/j.cose.2006.10.009

[4] Hasle, H., Kristiansen, Y., Kintel, K., Snekkenes,E. (2005) *Measuring Resistance to Social Engineering.* In Proceedings of the First International Conference on Information Security Practice and Experience -ISPEC'05 (LNCS 3439), 132-143.

[5] Herold, R. (2010). Managing an Information Security and Privacy Awareness and Training rogram, Second Edition. CRC Press.

[6]Jagatic, T. N., Johnson, N., Jakobsson, M., & Menczer, F. (2007, October). Social phishing. Communications of the ACM, 50, 94–100.

[7] Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: a real-world evaluation of anti-phishing training. Proceedings of the 5th Symposium on Usable Privacy and Security, SOUPS '09 (pp. 3:1–3:12). New York, NY, USA: ACM. doi:10.1145/1572532.1572536

[8] Kowalski, S. (1994) IT Insecurity: A Multi-disciplinary Inquiry. Diss. University of Stockholm. Report series No. 94-040, Stockholm.

[9] Mann, I. (2008). Hacking the human: social engineering techniques and security countermeasures. Gower Publishing, Ltd.

[10] Mitnick, K. D., & Simon, W. L. (2011) *The art of deception: Controlling the human element of security*. Indianapolis, IN: Wiley Publishing, Inc. Nohlberg, M. (2008).*Securing information assets: understanding, measuring and protecting against social engineering attacks.* (No.09-001). Stockholm: Sotkcholm University &University of Skövde.

[11] Pfleeger, C. (2003) Security in Computing (3rd ed). Upper Saddle River: Prentice Hall.

[12] Randolph, J.J. (2007). *Multidisciplinary methods in educational technology research and development.* Retrieved February 9, 2015 from http://justus.randolph.name/methods.

[13] Reeves, T.C. (2008). *Design-based research and educational technology: Rethinking technology and the research agenda, Educational Technology & Society*, 11(4): 29-40.

[14] Von Solms, S. H., & Von Solms, R. (2008).*Information Security Governance*. New York: Springer.