AALBORG UNIVERSITY

DENMARK

Implementation of SNS Model for Intrusion Prevention in Wireless Local Area Network

Isah, Abdullahi

Publication date:
2015

Document Version
Publisher's PDF, also known as Version of record

[Link to publication from Aalborg University]

IMPLEMENTATION OF SNS MODEL FOR INTRUSION PREVENTION IN WIRELESS LOCAL AREA NETWORK

BY
ABDULLAHI ISAH

DISSERTATION SUBMITTED 2016

AALBORG UNIVERSITY
DENMARK

IMPLEMENTATION OF SNS MODEL FOR INTRUSION PREVENTION IN WIRELESS LOCAL AREA NETWORK

BY:

ABDULLAHI ISAH

SUPERVISED

BY

Knud Erik Skouby
Professor and Director

Center for Communication,
Media and Information Technologies (CMI)
Aalborg University, Copenhagen - Denmark
Department of Electronic Systems

Aalborg University
DENMARK

2015

Dedication

This Research is dedicated to:

Muhammad,

Ali,

Fatima,

Hassan, and

Hussein

May the blessings of Allah

Be upon them.

Abstract

This research proposed and implemented a model known as a SNS (Social network security) based model for Intrusion Prevention in the Wireless Local Area Network of an organization. The model is built on two premises: on one hand it imparts the knowledge and skills of identifying and mitigating social engineering threats and attacks; on the other hand it provides an interaction structure called Bi-forminal ties on a social networking platform that facilitates real-time sharing, dissemination, countermeasures and real-time learning on social engineering based threats and attacks. An experimental design was used to implement and test the model. The experimental group was exposed to the mechanisms of the model for a period of 18 weeks after which both the experimental and the control groups sat for 3 hours test. The main hypothesis in the test was: there is no significant difference in the performance of the group exposed to the SNS based model and the group that was not exposed to the SNS based model in the identification and mitigation of social engineering based threats and attacks. A t-test for independent samples was used to analyze the test scores of the two groups. The t-test results led to the rejection of the main hypothesis. The alternate hypothesis was accepted, that there is significance difference between the performance of the group exposed to the SNS based model in the identification and mitigation of social engineering based threats and attacks and that of the group that was not exposed to the model. Thus, the experimental group performed better than the control group. The conclusion of the thesis is that the SNS based model is effective in the prevention of intrusion in the Wireless LAN of an organization. The model has contributed to the development of knowledge, theory and to the practical world by providing a socio-technical system for Wireless LAN security. The model is significant to organizations, computer and IT faculties, lecturers and students, and researchers. However there is need for further research on how the SNS model can be widely applied to multi-network of users for security collaborations.

Dansk Resume

Denne afhandling har udviklet og implementeret en model til at forebygge indtrængen i en organisations trådløse netværk (WLAN) - SNS (Social NetværksSikkerhed). Modellen bygger på to hovedelementer: 1) Opbygning af viden og færdigheder i organisationen til at identificere og afbøde trusler og angreb baseret på social engineering ; 2) Konstruktion af en samspilsstruktur på en social netværksplatform - kaldet Bi-forminale bånd, der letter realtidsdeling; formidling af modforholdsregler samt realtidslæring om social engineering baserede trusler og angreb. Der blev udarbejdet et eksperimentelt design for et forsøg med en eksperimentgruppe og en kontrolgruppe til at implementere og teste modellen. Eksperimentgruppen blev eksponeret for modellens mekanismer i en periode på 18 uger, hvorefter både eksperiment- og kontrolgruppen gennemgik en 3 timers test af reaktioner på trusler og angreb mod et trådløst netværk.

Hovedhypotesen i forsøget var: Der er ingen signifikant forskel i resultaterne i den eksperimentelle gruppe forberedt gennem den SNS baserede model og kontrolgruppen, der ikke var forberedt via den SNS baserede model. En statistisk t-test blev anvendt for at afprøve om de to gruppers testresultaterne følger samme fordeling. Resultaterne af t-testen førte til afvisning af hovedhypotesen. Det konkluderes, at der er signifikant forskel på resultaterne i eksperiment gruppen udsat for den SNS baserede model og i kontrolgruppen, der ikke var udsat for modellen. Eksperimentgruppen klarede sig således bedre end kontrolgruppen. Dette leder til den konklusion i afhandlingen, at en SNS baserede model er effektiv i forebyggelsen af indbrud i en organisations trådløse netværk.

Afhandlingen har gennem SNS modellen bidraget til videns- og teoriopbygning samt i praksis implementeret et socio-teknisk system til trådløs LAN-sikkerhed. Modellen har betydning for organisationer, computer- og it-afdelinger samt for undervisere, studerende og forskere. Der er imidlertid brug for yderligere forskning i, hvordan SNS modellen i vid udstrækning kan anvendes i multinetværk i et sikkerhedsmæssigt samarbejde.

Table of Contents

List of Figures:

List of Tables

CHAPTER 1:   Introduction

Attack and threats on Wireless network is taking a social dimension through social engineering whereas most solutions and scholastic contributions to network security are focusing on automated/technical system. I wish to argue that a social system of network security through a proposed model to be called SNS (Social Network Security) based model can complement the automated/technical system of WLAN security and serve as security to threats and attacks that are based on social engineering. Thus, my claim concerns a socio-technical centred security system as opposed to automated and encrypted system of network security.

1.1   Introduction

Is wireless Local Area Network (WLAN) safe and secured with technical system of security, a system that is software-based and automated? The social engineering form of attacks, which is rampant and on the increase with sophisticated improvements is giving a negative answer to this question. People – the users can sabotage any efficient and sophisticated technical system of security. According to Mitnick et al (2003), social engineering uses the weak human element to bypass technical protection. For example, Greening (1996) in his experiment, was able to lure students to disclose their passwords in response to unauthorized request. According to Ernst and Young (2004), lack of security awareness and practice by users is the top obstacle for effective information security. The proliferation of wireless network in the day to day affairs of individual and organizational activities is attracting both beginners and expert attackers. Much attention of wireless network security is focusing on technical solutions, forgetting or paying partial or little attention to non-technical system or social system of security. According to Yacin and Adam (2007), most security managers pay more attention to technical issues and solutions such as firewalls, routers, and intrusion detection software, while pay less focus on the user. Unless a balance

is maintained between the technical system and the social system for solutions to wireless network security, then a gap in security solution will continue to widen.

While there are numerous scientific researches on the technical aspect of WLAN security, on the contrary there is limited number of scientific studies that consider social aspect of security in WLAN. Even the few ones that have done so are focusing on security awareness and policy compliance. A social system of security that is of the people, for participation and collaboration with sense of accountability and responsibility, is absence in the efforts for security solutions. The proposed research contributes to the body of knowledge by addressing the identified gap. The research proposed a Social Network Security (SNS) based Model for a social engineering based Intrusion into Wireless Local Area Network (WLAN). The proposed model is to ascertain the claim of the research to the efficiency of the model in complementing the technical aspect of security, and the contributions of the model towards WLAN security. Intrusion detection and prevention in the SNS model is considered as a social system device that monitors network activities and the WLAN environment (in a human form) from the social engineering threats or malicious activities and use the social network to share, report, comment, and take actions on the experiences. The model is expected to improve WLAN security and complement the technical system of security by involving users – making each user accountable and responsible. The accountability is linked to the feedback received from a member in the social network on security experiences; and the responsibility is checked through participations in the social network through reports, comments, feedback, posting on security issues and taking appropriate security actions wherever desirable. Proper training and education, and user involvement, can help change mindsets and behaviors toward security, and make people the most effective layer in an organization's defense (Ernst and Young, 2004).

1.2   Background of the Study

The Increasing reliance on electronics and e-of-things boost the proliferation of Wireless LAN. Through the network firewall, users access web pages and the internet through the Wireless LAN. For instance there is increasing proliferations of wireless networks in the Nigerian society is a result of the Nigerian government's policy on ICT, which advise institutions and organizations both in the private and public sectors to operate on e-Applications (4.12: NICTP 2012). The policy has started with the banking industry where the Central Bank of Nigeria directed banks to embark on cashless transactions thereby reducing physical cash in transactions and reducing other financial crimes (Central Bank of Nigeria, 2011). Similarly the benefits attributed to wireless network of flexibility and mobility has contributed towards its growth in the Nigerian society. However one big challenge wireless network is facing is that of security. As a result of researches on wireless security carried out by Universities, research institutes, teachers, students and network security companies, the technical system of security is becoming efficient and sophisticated thereby making it difficult and tedious process for attackers to break or bypass a security system. For example, dubbed key hopping technology has the ability to change encryption key so rapidly in every 3 seconds thereby making it tedious and frustrating for the hacker to identify the key patterns (Ted 2001). According to Wu (2008), with key Hopping technology, wireless LAN users can rest easy knowing their data is secured.

Moreover, Wen-Chuan (2004) designed a proactive wireless Intrusion Detection System. It serves as a solution for WEP cracking, MAC address spoofing and war-driving, via short Message Service (SMS). As per network traffic control, Dong (2007) introduced a WTLS-Based Intrusion prevention model. The model introduced a logical sole path between wireless terminal and its destination so that IPS engine can detect and prevent threats

3

in the traffic. In another study carried out by Vartak, et al (2007) on the over-the-air pre-vention techniques, the researchers came up with a system for mitigation to unauthorized wireless communication access. In another study, Guarlin et al (2010) presented a frame-work of WIPS with an intelligent plan recognition and pre-decision engine using honeypot technology, which can predict future attacks and promptly respond to the attack. The re-searchers further designed an improved system for conduction plan recognition and making pre-decision. Although there are certain limitations and drawbacks in some of the wireless security researches, however such limitations are continually updated and corrected by ex-tended, reviewed and further researches.

To some extent, the technical system is becoming efficient in meeting wireless network security challenges. Against this background, organizations are concerned and confident with the technical system in providing solutions to security issues. Organizations spend more on anti-virus, firewall, anti-malware and other anti-malicious tools. The belief by individuals and organizations is that buying the most advanced technology or the latest threats detection systems can guarantee the network from intrusion, threats and attacks. Unfortunately, the answer is "no." According to Diana (2013), just like driving a car re-quires multiple parts working together, "driving" a corporate IT network safely requires a blend of the traditional triumvirate: people, process and technology. Unfortunately organi-zations fail to realize, as pointed out by ITIF (2011), that many security products rely on people behaving in a responsible and predictable fashion. Keibler (2013) says it is too late an action to rely on the endpoint to stop all the malware. A more effective approach is to start with employee awareness, partner with employees and help them to be another arm of the security program. Keibler (2013) added that there are some social engineering compo-nents in 70 to 80 percent of attacks.

Organizations develop confidence in the technical system as a result of the various research findings and innovations in wireless security. According to Sheng et al (2012), wireless security has emerged as a premier research and development issue. Numerous important aspects have been addressed, such as key management schemes in mobile ad hoc networks (Cameron et al, 2006) and distributed sensor networks (Chou et al, 2004), secure routing protocols (Albrech et al, 2005); and localization algorithms (Cranor et al, 2008) to prevent wireless sensor attacks; and privacy protection in RFID systems (Graner, 2001). *However, most of the researches on wireless security focused more on the technical aspect with a partial consideration on solutions for the social aspect.* Security should be seen as a social process and as such its solution needs a social component. Technical solutions, as important as they are, cannot work alone (Mororolla, 2010). The concentration on technical system for security solutions has created a gap in the system of security. This research aims to fill this gap with a social system of security by proposing a social networking security model, for collective participation in the identification and prevention of social engineering based attacks.

The efficiency of the technical system of security instigated attackers to write malicious software that only gets activated with the intervention of the user. The user is then turned into a proxy attacker by compelling or persuading the user to click a link or install dormant software. It is called dormant because it only gets activated with the help of the user. That is why despite the progress in technical solutions of security being achieved by research communities, yet there are certain intrusions that avoid detections once they get into a system. In some recent studies, most attacks evade detection with the intrusion detection systems. According to Gartner as many as 14 out of every 17 attempts evade detection today. Google recently conducted a study that shows the best scanner missed at least 75%

of internet-borne malicious files. The action of the user by activating the malicious software, turn them to be genuine thereby scanners could avoid them. iMPERVA, a security company conducted a study that shows newly created viruses evade detection over 95% of the time. Once infected, the user's computer will host dormant software, called a malware, which will steal user's passwords. The malware will subsequently transmit the password to criminal organizations. According to Kaspersky lab 75,000 new malware are released very single day. Most of these malwares are directed to the user, in form of social engineering, compelling the user to take action by clicking a link that activates them. According to Microsoft's recently published Security Intelligence Report, almost 45% of infections are as a result of malware writer using various social engineering to influence the user to take action that results in the user running a malicious file, thereby infecting their own machine. Malware writer does not have to spend longer time and go through tedious process trying to intrude into a network, the attacker just present the user with credible reason to install and run the attacker's program.

Security companies alone cannot keep up with the security challenges. It is no surprise that the existing technologies are unable to stop an estimated 85% of the attacks. The average intrusion goes undetected for six months or more. Individuals and companies alike face the challenge of keeping up with ever evolving security threats. Existing technical solutions have increasingly been rendered less and less capable by the fast evolving nature of cybercrime as a result of social engineering. This is a known issue by industry insiders and now demonstrated by various independent research organizations. The existing approaches to security are in need of support or complementary solutions. Attackers are now using social system (a non-technical system) to carry out their malicious activities. A social system comprises up of people and their interactions. People use network and IT devices to

accomplish their day to day activities and functions. No matter the level of sophistication of devices in securing the network from attacks, the user can give away the security measures thereby providing access to attacks. According to Czernowalow (2005), a single user abuse to security policy can cost more in terms of finance and related damages, than the installation of state-of-the-art security devices. According to one group of US security experts and analysts, some 400 breaches were reported in 2009 which compromised over 200 million records. Most disturbing, the group reported that 80% of these breaches were caused by insider attitude – the users (Motorolloa, 2005). User ignorance, user behavior, and user isolation in the security involvement, all contribute to the attraction of attackers in using a social system of attack.

Thus, user is the weakest link for any security measures adopted to protect the network and the information system of an organization. Attackers are now aware of user weaknesses and are using it to exploit both the user and the network. They do this through a social system known as social engineering. This is a system of manipulating the user to give out information or do something in the way a determined attacker wants. Through social engineering, a user can reveal his password, can reveal the identity of his network security, can disabled certain security functionalities, or activate a software that acts as malware or Trojan on the network. Social engineering uses various strategies to lure the user into becoming a proxy attacker. Any form of information gathering, be it online or offline, can turn out to be an element of social engineering (Christopher, 2011). A user is lured into opening an email attachment that contains a benefit but instead it is a security exploits; a fear is thrown into the user that informs user that harm or threats is affecting user's devices; and that causes the user to comply to further request that may remove such risks or danger. Ponemon Institute DarkReading report (2010) showed Web-borne attacks,

malicious code, and malicious insiders as the most costly types of attacks, representing over 90 percent of all cybercrime costs in a year per organization. Malicious insiders occupy the top in these three attacks. It shows that users are being used as proxy attackers through social engineering. According to Christopher (2011), many of these attacks could have been avoided if people were educated, because they could act on that education. A user is taken into courtship of friendliness that may end up exploiting the user to give away certain information; or the user is conditioned into a state of helplessness so that user must seek help from a determined attacker, who uses the helplessness of the user to launch an attack. *Social engineering also takes the advantage of user laissez-faire attitude towards the value of information and the failure of the user to observe security measures. All these point to the need for a social system of security.*

In an attempt to provide a social system counterpart of security to the technical system, security managers and network administrators of organizations embark on user awareness and security compliance so as to educate and caution the user on activating dormant software or breaching security regulations. The security policy defines the dos and don'ts for the user to observe and maintain fair security compliance to access control, network usage, running applications and using BYOD (bring your own devices). Organizations ensure that users observe and implement the security policies by providing users with update security regulations, awareness, and promotional campaigns. This is done through promotional methods, enforcing methods, and informative methods. In the promotional method, the IT department creates security consciousness packages in form of banners, home page of the organization's intranet or login page, or in the form of screen saves on the organizations' output devices. The enforcing method conditioned and indirectly threatens workers to comply with security measures otherwise violations could be sanctioned by

deferment of promotion or denial of other benefits. The informational method prepares leaflets, newsletters, information security guides, and email warnings to workers with a view to keeping them informed on security compliance*. As the technical system of security is not adequate enough likewise the so called user awareness and users to collaborate on security issues.security compliance policy, lacks a defined structure and pattern that can knit and bring*

Security policy advice users not to click on any suspicious email and also not to click on any link that asks for usernames and passwords, yet users out of curiosity, greedy, or anxiety, comply with the attackers' requests. This shows that user awareness and security compliance needs an add-up to make the social system of security valid and reliable. This add-up should have the features of user participation, collaboration, engagement and must have control mechanisms to ensure user accountability and responsibility. When BS7799 (1999) says that it is essential to ensure that all users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work, perhaps their statement points to the need for a collaborative and participatory system of security. Social networking is the system that meets such requirements for a collaborative system of security with all the desired control mechanisms for a team work, accountability and responsibility. Jemal (2012) identified a positive correlation between user information security awareness programme and perceived security effectiveness. Jamela (2012) added that the success of information security programme ultimately depends on establishing a security positive environment, where the end-users understand and take part in the behaviors that are expected of them. Researchers in healthcare and education have proved social networking as worthy in improving health care, and facilitation in teaching-learning system. For example, Robert (2011) introduced a model that

describes how social networks can provide powerful mechanisms for delivering more experts, timely and targeted information to the concerned actors in ways that can benefit preventative care, and transitional medicine through feedback loop between patients and researchers. Similarly in the field of education, Jernej et al (2012) confirmed in their study that integration of social networking platforms and learning management systems is needed and possible in practice. This research attempts to use social networking to propose a social system of security that is of the people, for the people, by the people, and the sense of accountability and responsibility in the identification and prevention of a social engineering intrusion in WLAN.

Therefore bringing users to comply with security policies is not yielding the desired result through user awareness and security compliance policy. This is because the process lacks accountability and responsibility. Moreover as a result of the increasing automation of office functions, the IT personnel are too busy to cross check who and who are violating or refusing to implement and observe the security policies. This situation lacks control and added to the existing human vulnerabilities of laissez faire attitudes towards security and low regard to the value of information. Thus, exposing the user as the weakest link as per security measures are concerned. Unless the user is held responsible, accountable and is engaged through a participatory program that makes the security system for the people, by the people and of the people, then any sophisticated technical system of security with its user security policy, may not be enough to provide the desired solution to security. The technical system of security must be complemented by a social system that is based on collaboration and user participation. ***The absence of such a social system is considered a missing link in the effort to provide a satisfactory social system of security which can complement the technical system. This is the missing link this research aimed to fill.***

It is the claim of this research that by creating a system of security that is of the people, for the people, and by the people, a social system of security that make the user accountable and responsible in complementing the technical system of security. This research aims to achieve this by proposing a Social Network Security based model for the identification and prevention of attacks on a WLAN network. The model is to be tested through implementing it on a social media platform of the Facebook by directing the experimental group to form a social networking group based on strong ties relationship so as to share intelligence on security instances and experiences. The group members were free to add members through weak tie relationship. Sharing security experiences to weak ties was not made mandatory to the group, but such weak ties relationship is desirable for the research to combine both ties in building a security network that is vigilant and rich in information without restrictions to protocols of hierarchy of authority or organizational structure.

1.3   Outline of the Study

This study is in 7 chapters. Chapter 1 being the introduction provides the general overview of the research. Chapter two is the literature review which was guided by the research questions and discussed what was already known in the field of this research through review of scholarly publications and research findings. Chapter 3 is the methodology that describes the approach followed in conducting the research as well as the tools/apparatus used in collecting and analyzing data. Chapter 4 provides the details on how the proposed model was conceived, designed, and developed. The chapter also provides the manual or instructional process to follow in using the model. Chapter 5 is dedicated to the analysis of the data collected. The hypothesis of the research was tested in this chapter, and the chapter also attempted to answer the research questions. Chapter 6 summarized and concluded the research from the major findings of the research. Chapter 7 made

the necessary recommendations, acknowledged the limitations of the study and suggested ways for improvements through further research.

1.4   Method

Details of the method and methodology used to conduct this research are given in chapter three, the methodology. The following explanation is just a brief on the method. The research used experimental design to collect data and answer the first part of the research question; and qualitative content analysis was used to answer the second part of the research question. The research identified the independent variable as the exposure of the experimental group to the SNS model; and the dependent variable being the level of learning as highlighted in each of the research hypothesis.

According to Vernoy and Kyle (2002), the experimental design is of three kinds: between subjects design, otherwise known as the independent-group design; within-subjects design, otherwise known as repeated-measure design; and mixed design. This research used the independent-group design. The population of the study comprised up of 152 wireless users and 80 of them were used as sample, using the Krejie and Morgan (1970) table of random sample. The test scores were used to test the hypothesis, and the contents of social media of Facebook, which was the platform used to implement the SNS model, were used to obtain data on the behaviour of the users in the implementation of the model.

1.5   Statement of the Problem

The fruits and benefits of digital society (or e-of-things) which is a global phenomenon and the Nigerian society is not an exception, should be enjoyed by the Nigerian community as well as the public and private enterprises. E-learning, e-government, e-banking,

e-commerce, e-health, e-communication, and e-socialization are meant to make life better and convenience as well as to accelerate growth and developments. The formation of an electronic society is achieved through network connection and such network should be one characterized with flexibility, mobility, and safety. Wireless network fill such conditions. In the attempt for individuals and organizations to implement and actualize the e-of-things and reap the benefits inherited with an electronic society, WLAN are existing in most organizations in the Nigerian society. Unfortunately wireless network by its nature is vulnerable to threats and attacks. The security challenges facing wireless network is a serious one which if it is not faced with the appropriate solutions, then the benefits associated with wireless network may turn out to be drawbacks to progress in all spheres of societal developments.

In the attempt to be secured from hackers and attackers, organizations use various anti malicious software, anti-virus, intrusion detection and prevention systems, and all sorts of firewalls and software based security mechanisms. Universities, teachers, students, and research institutes also contribute towards solutions to wireless security. Happily, the efforts are said to be paying in counteracting the activities of hackers and attackers. Some of the security mechanisms refresh their key patterns at an interval of some seconds. That makes it difficult and tedious to bypass or break a security system.

This therefore leads to too much dependence on the technical or automated-software based solution to wireless security. Unfortunately, the activities of hackers and attackers continue to grow through a non-technical system or a social system of attacks known as social engineering. This has indicated that a gap is created in the quest for solutions to wireless security and unless the technical system of security is complemented with a social system of security, then solutions to wireless security would continue to widen. Although

there are few researches that attempt to address the social aspect through user awareness and security compliance policy, yet they fall short of a system that bring users together for collaboration, engagement, and participation to security issues with sense of accountability and responsibility.

Section **1.7** clarifies further on the justification for the study of the problem. Thus, this research aims to contribute to knowledge by addressing the identified gap and proposed a model known as Social Network Security (SNS) based model for the identification and prevention of social engineering based threats on WLAN. Therefore, the research question addresses by this research is: **What is the effect of the SNS based model on users of Wireless LAN in an organization to identify and prevent social engineering based threats and attacks; and what is the attitude of the users in the implementation of the model on the platform of social media of Facebook?**

1.6   Motivation

This section explains the reasons why the questions raised in this dissertation are of interest to the author. There are five main reasons that contribute to the motivation in this research. First: The proliferations of WLAN in organizations is facing the challenges of novice and expert attackers and research is needed that can bring a solution appropriate to the current way of life of the wireless user. Nowadays workforce spends considerable part of their work time and personal time on social networking.

This indicates that people are collaborating on issues of common concern and interest. I perceive that such collaboration is much needed in the area of security. *As such I became motivated to fashion the security system on the pattern of social network.* Secondly, the average office worker is now literate in ICT (Information and Communication

Technology) and that motivated me to see the possibility in integrating the user in the affairs of collaborative security.

Thirdly, I became motivated by the fact that everything in life is balanced on two phases; but security is dependent on one phase of software-centred thereby lacking the second phase of social-centred. Hence I saw the need to consider how the social system of security can be a complementary solution to the technical system of security. With the increasing disguise of social engineering in malware forms, the social system of security need to be tested to determine its applicability and appropriateness.

Fourthly, the digitalization of office functions and activities is placing too much burden on security managers and network administrators. This research is motivated by the desire to see that the social aspect of security becomes a shared responsibility. Fifth: this research is motivated by the hope that it will contribute to knowledge by addressing the identified gap through the implementation of the proposed model.

1.7   The Knowledge gap

Although this section has been expounded in some parts of the background of the study as well as in chapter 2 – state of the art, it fits logical to give a brief highlight of the knowledge gap as follows: Previous researches focuses on:

1. Technical or automated-software based systems of security of WLAN;

2. User awareness and security policy compliance (the focus was on individualism rather than collective and participatory approach).

BUT, fail to address:

1a.   Social system of security, a system that fashion and structure security on a social pattern;

2a.   Collective user involvement, participation and collaboration in security matters

The identified gap in 1(a) and 2(a) above was the focus of this research.

Figure 1 below depicts the gap this research attempts to fill. The user being an important component of wireless network is the weakest link targeted by social engineering based threats and attacks. Security solutions are paying little attention to user involvement in the security system.

Instead of hackers spending longer and tedious time to break into a system or network, they find it easier to gain illegitimate access through legitimate means via the user. Most security administrators are engineers and scientist and such background created bias against socially based solutions thereby rendering the user a proxy attacker, assisting the hackers and used by hackers. Users comply and respond to hackers' requests through social engineering.

Figure 1: Wireless Components depicting user isolation

Figure 1 shows the user as one of the components of Wireless network. The network exists to provide services to clients – devices and computers. The understanding of limiting user to client of the network is one of the reasons that user is often neglected, ignored, and left unattended as far as security issues are concerned. As the computers and other devices in

the network are clients, they are as well components of the network. Likewise the user is both a client and a component of the network. Without the user, the network is said to be valueless. Attackers and hackers have so far recognized the user as component of the network, thereby attacking the user through social engineering.

1.8   SE outsmarted the next-generation Security Technologies.

At the recent DEF CON 21 Conference in Las Vegas, a live competition called Social Engineering Capture the flag showed the ease in which social engineering can be used to defeat the next-generation security technologies. John (2013) reported the proceedings of the competition at the conference and gave it the title: popular contest and presentation show real risks associated with social engineering. Prior to the date of the conference, the contestants were allowed to select their target companies. At the conference, the contestants occupied sound proof rooms and were given 20 minutes to call their target organizations and lure its employees into getting vital information necessary to launch an attack on their network. Among the information solicited by the contestants were the target's operating system, details of internal and third party technical support, and details of the wireless network. The highest score a contestant could get was to manipulate a target to visit a specific website. At the conference, some security professionals were viewing the competition as a child play which is not serious a threat to security, considering the latest security technologies they have in place. However at the end of the conference and the competition, those security professionals felt as if their network and all their computing devices are naked and exposed to threats and attacks.

One interesting thing before the kick up of the competition was, one of the contestants called his target to confirm about the security products in place. The target confirmed that the security had next generation firewall from top providers, application whitelisting,

egress filtering, and SMTP sandboxing technology. Then the contestant convinced his target that he wanted to fill out health benefit form online. As the target user opened the website in Internet Explorer and click 'yes' on a pop-up, the contestant shouted cheers and remarked that the user had accepted the new policy form and was done.

Equally, numerous Metasploit, Meterpreter backdoor sessions, showed up on the presenter's screens in front of DEF CON audience, causing cheers and applause. John (2013) concluded that the result of the competition had bypassed many hundreds of thousands of dollars of security technologies in front of a live audience.

Thus, this research contributes to knowledge by addressing the identified gap with a proposed model called Social Network Security (SNS) based model, which was implemented through experiment that assessed knowledge of the participants of the experiment in the identification and prevention of social engineering based threats and attacks; and the behaviours the participants were assessed through content analysis, while implementing the model on the social media of Facebook

1.9 The Purpose of the Study

The purpose of this research was to propose SNS model as a socio-technical system of security to Wireless LAN by implementing and testing the effect of the model on Wireless LAN users in the identification and prevention of Social Engineering based threats and attacks on University campus Wireless LAN; and to describe the behaviour of the Wireless LAN users regarding the use of the model as a social system of security.

1.10 The Objectives of the Study

From the purpose of the study, the research aimed to achieve the following objectives:

i   To propose SNS model as a social system of security to Wireless LAN.

ii   To implement the model and test its effect in the identification and prevention of SE based threats and attacks.

iii   To assess tricks and techniques used in social engineering.

iv   To examine social context authentication mode.

v   To examine countermeasures to SE threats and attacks.

vi   To combine o weak ties from strong ties connections for collaboration on security.

vii   To evaluate the functionalities of Social Media of Facebook for collaborations on security.

viii   To assess the attitudes of the Wireless LAN users regarding the implementation of the model.

1.11 The Research Questions

In order to achieve the aim and objects of the research, and set the boundaries that beam the focus and directions (as blue print) relevant for literature review, data collection, and choosing appropriate methodology for the research, the overall research question is stated as thus: **What is the effect of the SNS based model on users of Wireless LAN in an organization to identify and prevent social engineering based threats and attacks; and what is the attitude of the users in the implementation of the model on the platform of social media of Facebook?**

Specific Research Questions

The overall research question splits into the following questions:

i   How is the SNS model can be implemented to identify and prevent SE based threats and attacks by Wireless LAN users?

ii   What is the performance of Wireless LAN users regarding overall knowledge of the

SNS model in the identification and prevention of SE based threats and attacks?

iii   What is the performance of Wireless LAN users regarding tricks and techniques of social engineering?

iv   What is the performance of Wireless LAN users regarding social context authentication mode?

v   What is the performance of Wireless LAN users regarding countermeasures to SE threats and attacks?

vi   What is the performance of Wireless LAN users regarding Strong tie - Weak tie interactions?

vii   What is the performance of Wireless LAN users regarding usage of Facebook functionalities for security collaborations?

viii   What is the behaviour of Wireless LAN users in the implementation of the model?

1.12 The Research Hypotheses

The following hypotheses (both null and alternate) were formed in respect to research

questions 2 – 6, because they are quantitate questions and involved quantitative data.

H_0:   there is no significance difference in the performance scores of the subjects exposed to the SNS based Model in the identification and prevention of social engineering based intrusion on WLAN and those subjects who were not exposed to the SNS based Model.

H_1:   *the subjects exposed to the SNS based Model perform better in the identification and prevention of social engineering based intrusion on WLAN than those subjects who were not exposed to the SNS based Model.*

H_0:   there is no significance difference in the performance scores of the subjects exposed to the SNS based model on tricks and techniques of SE and those subjects who were not exposed to the SNS model.

H_1:   *the subjects exposed to the SNS based model perform better on tricks and techniques of SE than those subjects who were not exposed to the SNS based model.*

H$_0$:   There is no significance difference in the performance scores of the subjects exposed to the SNS based model on the social context authentication mode and the subjects who were not exposed to the SNS based model.

H$_1$:   *the subjects exposed to the SNS based model perform better on social context authentication mode than the subjects who were not exposed to the SNS based model.*

H$_0$:   there is no significance difference in the performance scores of the subjects exposed to the SNS based model on countermeasures to threats and attacks of SE and the subjects who were not exposed to the SNS model.

H$_1$:   *the subjects exposed to the SNS based model perform better on countermeasures to threats and attacks of SE than the subjects who were not exposed to the SNS based model.*

H$_0$:   there is no significance difference in the performance scores of the subjects exposed to the SNS based model regarding bi-forminal ties security collaborations and the subjects who were not exposed to the SNS model.

H$_1$:   *the subjects exposed to the SNS based model perform better on bi-forminal ties security interactions than the subjects who were not exposed to the SNS model.*

H$_0$:   there is no significance difference in the performance scores of the subjects exposed to the SNS based model on the use of Facebook functionalities for security collaborations and the subjects who were not exposed to the model.

H$_1$:   *the subjects exposed to the SNS based model perform better on the use of Facebook functionalities for security collaborations than the subjects who were not exposed to the SNS based model.*

1.13 The Significance of the Study

The research is expected to balance the imbalance existing from the sole reliance on the technical system of WLAN security system. The research complements and supports the existing technical system in WLAN security. The research is significance both to the academia, the practical world and professional fields as outlined below:

1. To the field of science and technology, the research contributes to knowledge by introduction the SNS based model for the identification and prevention of social engineering based intrusion on WLAN.
2. The research is significance to teaching and learning for it is an add-up to the existing curriculum of network security.
3. Individuals, organizations, and security professionals could find the research significance in the attempt to find social solutions to social techniques of Wireless LAN attacks through social engineering.
4. Government and other regulatory agencies can find the research useful for promulgation and implementation of participatory security measures.
5. The research is of significance to software engineers and developers by using the SNS model to come up with new design in WLAN social system of security.
6. Researchers in the fields of WLAN security could use the data and findings of the research for further analysis and advancement of knowledge.

1.14 Delimitation of the Study

There is the need to clarify the coverage of this research in terms of place and concept. In other words, the geographical scope (or boundary) and the conceptual scope (or boundary) of the research needs to be clarified.

The geographical boundary explains the physical area within which the research is confined. The conceptual boundary explains the specific knowledge-fields this research is focusing its attention.

The Geographical Scope

The research is within the University campus of UMYU (Umaru Musa Yaradua University) of Katsina state, Nigeria. Any environment outside the defined location of UMYU is outside the coverage and physical boundary of this research. Details justification for delimiting this research to University campus is in Chapter 3, under Methodology. However, University campus resembles many settings in organizations and as such it was considered

the appropriate environment for this research. University campus is a said to be a replica of many organizations whether private or public.

The Conceptual Scope

This research was not concerned with technical system of WLAN security, or automated-software tools and solutions to Intrusion Prevention. The research is concerned with socio-technical system of security for a social solution to WLAN security and a complementary solution to the technical system of WLAN security. The research is specifically concerned with WLAN Infrastructure. Threats, Attacks and security issues that are *purely automated and software-centred* are outside the conceptual scope of this study.

1.15 Operational Definitions of Terms

It is necessary to define some terms that have been used in the context of this research. Understanding or interpreting the terms from the usual meaning, may distort the actual meaning from the perspectives or context of the problem of this study. The terms below are defined operationally:

Attacks	*Is here defined as causing damages and/or offsetting a system, device, or program in the network and the wireless environment plus unauthorized access through tricks or Trojan style.*
Difference:	*Changes that occur from the application of a treatment.*
Formal ties	*The connections and interactions officially established among members of staff for collaborations and engagement.*
Implementation:	*Is hereby defined as Teaching-learning system and practical application of knowledge, skills and competencies acquired.*
Informal ties	*The connections and interactions socially established from the formal ties by members of staff.*
Intrusion	*Is hereby defined as any attempt or trick to gain access to a network, network resources, or obtain information from a user and asking the user to execute certain actions. It also includes any unusual or anoma-*

	lies observed or humanly detected on the network, devices, and environment of the organization.
Intrusion Prevention	*Is here defined as identification of threats and potential attacks by user; and responding to them promptly through user action or collaborative actions.*
Malicious	*Is defined here as any object, person, or program that is suspected to cause interruptions, intrude, or causes some damages to the environment, the network infrastructures, and computer systems.*
Prevention	*Is defined here as individual and collective actions to observe, listen, report, comment, discuss, and share experiences that are suspicious, doubtful, and unconfirmed.*
Proactive Skills	*Is hereby used as live events monitoring with the senses, knowledge and experience, anomalies within the environment, the network devices, the network connection, and the network services.*
Reliability:	*The ability of being dependable.*
Social Engineering	*Is defined here as any form of trick either online or offline that influence or persuade a user to give out information or act in certain ways as requested by a person, software or program.*
Social Network	*Is defined here as structure and patterns that connect people together for collaboration, interaction, and engagement for security collaborations.*
Social Networking	*Is hereby refers to the activities members of the social network carried out for the security collaborations.*
Threats	*Is hereby defined as anything that falls under Intrusion, attacks, malicious, plus unsolicited appearance and display of objects, person, or program on the systems and environments of the organization.*
Validity:	*The quality of having mate standard for application.*

1.16 Summary

This chapter has introduced this research by attempting to fill the gap created in the attempt to provide solutions to threats and attacks on network and information resources. In this regard, the chapter sated the research question to be addressed and the hypotheses to be tested. The chapter highlighted the motivation that prompted the need for this research as an attempt to provide a balanced and complementary system of security to the technical

system, which is given more attention and priority at the expense of the non-technical system of security.

The chapter described the main objective of the research as the implementation of SNS model that is of the people, for the people and by the people; in such a way that users of wireless network in an organization can be able to identify and prevent social engineering based threats and attacks.

The chapter gaves an outline of the method to be used in implementing the proposed model with an experimental study, followed by content analysis to assess the behaviour of the users of the model on the platform of social networking. The chapter concluded with definitions of terms so as to explain how some terms are meant in this research as against the meanings commonly associated with such terms.

1.17 Brief overview of the subsequent chapters

The chapters that follow in this thesis are:

Chapter 2 Reviews existing research publications in the fields of non-technical attempts to provide solutions to social engineering based threats and attacks on network and information security. A gap was identified in the process of reviewing the existing state-of-the-art; and the current research aimed to fill the identified gap.

Chapter 3 Describes the design, methodology and the implementation of the proposed model in experimental settings and how the attitudes of the participants were assessed on the social network platform.

Chapter 4 This chapter described the Theoretical framework underpinning this thesis. The chapter described the theoretical framework as both the foundation to the research question and as well the framework for the proposed SNS based model of this thesis.

Chapter 5   This chapter gives the details of the SNS based model.

Chapter 6   This chapter analyzed, interpreted and discussed the quantitative data collected from the experiment in one hand, and the qualitative data collected from the social network platform. The analysis on the quantitative data was to answer the major research question and test the hypotheses of this thesis. The qualitative data aimed to answer the research question on the attitude of the participants while implementing the model on the social network platform.

Chapter 7   This chapter concluded the thesis with summary, recommendations and suggestions for future research.

Chapter 8   Provides the list of references various literature reviewed in this research.

CHAPTER 2:   The State-of-the-art

Models, Frameworks, and Concepts for solutions to Social Engineering based Threats and Attacks

A review of related studies revealed that so far, no attempt has been made to address intrusion into Wireless LAN through social engineering, by implementing a social system of security on the platform of social networking. The intrusion into Wireless LAN through social engineering with user collaborations for countermeasures has been over-looked *by scholastic studies; despite social engineering is rapidly becoming the favourite attack vector for hackers; and despite social networking is widely applied in various areas for various purposes. This thesis conducted state-of-the-art scholastic review of non-encryption approaches to network and information security as well as on social engineering and its countermeasures. The state-of-the-art was critically reviewed within the domain of this study to justify the purpose of this thesis and highlighted the gap in the state-of-the-art which this thesis aimed to fill. This chapter also included the justification for the choice of method used to address the identified gap.*

2.1   Introduction

The purpose of this chapter was to improve theoretical and empirical understanding of the research topic: the implementation of Social Network Security based model for intrusion prevention of SE based threats and attacks on WLAN. The knowledge gained in the review of related studies was applied to update the research topic to the stat-of-the-art. The related studies were reviewed through brief appraisal of major concepts from academic peer reviewed sources and articles written by informed experts related to the research topic. In other words, the review examined concepts and established an understanding how different scholars approached the issue of network and information security. This was with the view to bringing out the gap in scholarship through the reviews. In the process, an understanding was established on how the current research can fill the gap. Thus, the scholastic

studies reviewed established the desirability for this research and the boundary/limitation of the study. This chapter also reviewed the methods used in this study, with the aim of justifying the choice of the approach adopted.

The following questions guided the review of the literature: what researches on this research topic have been done before? What others have said about this topic? How are those researches relevant to this study? How are the researches different from this study? Do the existing researches agreed with one another or there were disagreements? Are there flaws in the existing literature? These questions guided the current research to identify the gap in the literature. This in turn served to clarify the purpose of this research; which is *the implementation of social network security based model for SE based intrusion prevention in Wireless Local Area Network.* The review of the related studies was organized into three main portions with subheadings: the first part of the literature review deals with conceptual framework establishing an understanding of the topic. The second part deals with scholastic peer reviews on this research topic, which were further divided into sub-sections. The third part focused on approach, justifying the approach used.

This research does not focused on the review of technical-automated software solutions to Wireless LAN security, nor does it attempted to look into encryption techniques in network and information security. This is because network and information threats and attacks are shifting from technology based to non-technology strategies through social engineering that targets, manipulates, and turn the user into proxy attacker. The reason for this shift is as a result of bias to non-technical system of security. The system of security as well as researches for mitigating threats and attacks are in favour of the technical-automated, encryption and software solutions, thereby leaving the non-technical system unattended. This neglect turns the user into the weakest link in the security of network and

information resources. Security issues must be addressed by both technical and social systems. Too much dependence on technological solutions and approaches to security created a gap that allows hackers and attackers to play their games at ease. It is against this background that this research aimed to focus the review of the state-of-the-art of network and information security on the non-technical approaches.

2.2   Overview of Wireless Local Area Network (WLAN)

Tom and Les (2002) defines wireless network as transmission of data over the air through radio frequency where one or more devices communicate to one another without physical connections or peripheral cabling. Dongsheng (2012) assets that while WLAN permeated our daily lives to such an extent that many companies are considering to abandon the wired LAN, because it is old-style and clumsy. Unlike wired network where devices are connected to each other through physical wires for the transmission and reception of data and/or information, Wireless uses radio signals for communication to transmit and receive information and data without the need for wires. Information is passed and propagates in the air and easily accessible to anyone with the right facilities to capture it. Wireless network has its basis from Spread Spectrum, which is a modulation technology that spreads bandwidth in the frequency domain. It uses a wide bandwidth with a low peak power. Spread spectrum adds security to the Wireless LAN by making the signal hard to detect and intercept. Thus, spread spectrum is anti-jamming, anti-interference, and message privacy. Wireless is always an extension of the Local Area Network environment. Wireless has an edge over any means of communication in respect to deployability and flexibility.

WLAN security can be defined in terms of domains, functions, and/or concepts. In terms of domains, WLAN security can be categorized into access point security, signal security, client device security, and user security. In terms of functions, WLAN security

can be categorized into intrusion detection and prevention. In terms of concepts, WLAN security can be categorized into confidentiality, integrity, authentication, access control, non-repudiation, availability, and privacy. Thus, wireless security is measures - technical and administrative used to protect from both internal and external threats and exploits compromising the wireless network from intrusion, unauthorized access, disclosure, damages, and manipulation of the wireless network and its associated infrastructures. **The security measures are taken to protect both the types of wireless and their components.**

2.2.1 WLAN modes and components

Ankush and Katia (2005) identified two types of wireless modes: the ad-hoc mode which is similar to peer-to-peer networks where devices communicate each other *without* the access point; and the infrastructure mode in which devices communicate with each other through via the access point. Figure 2 describes the infrastructure mode of WLAN.

Figure 2: Depicts the infrastructure mode of WLAN.
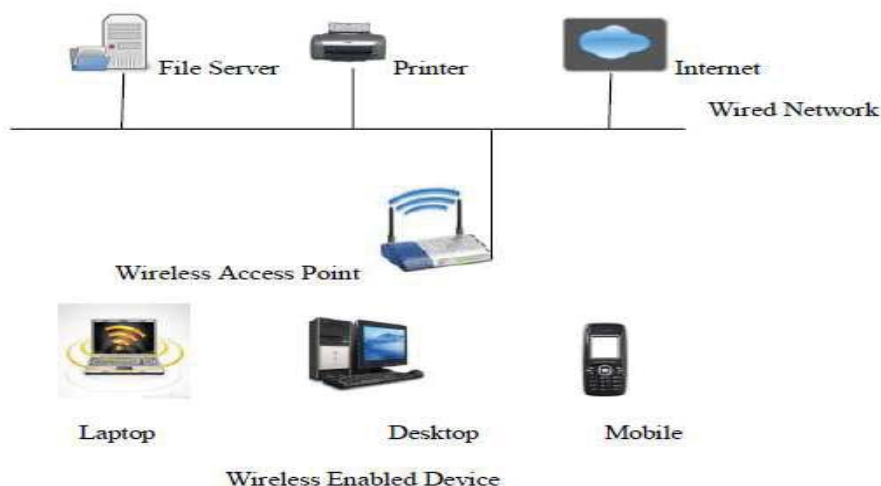
Source: Irfan Siddavatam International Journal on Computer Science and Engineering (IJCSE), 2011.

This research is focusing on the infrastructure mode of the WLAN. The installation and deployment of the infrastructure mode is made up of four components. Min-Kyu et al (2008) describe the components as: the radio waves or signals, the access point, the client devices, and the user as depicted in Figure 3; recognizes user as component of WLAN.

Figure 3: Wireless LAN components
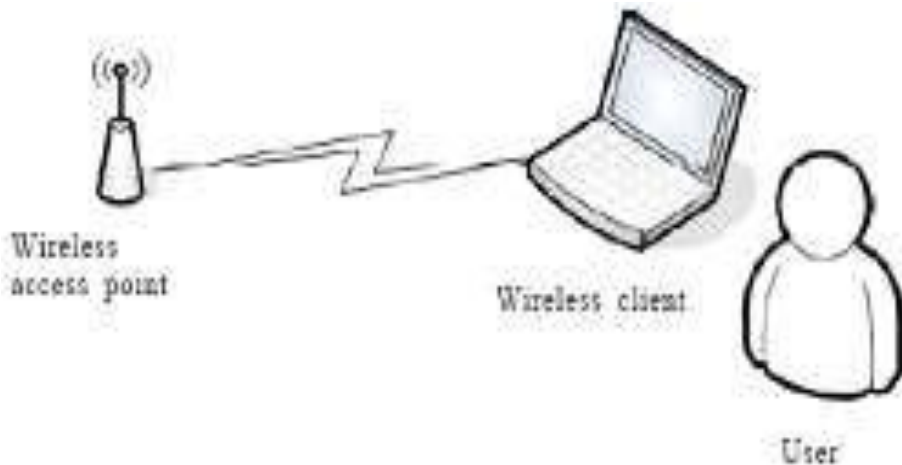
Source: Min-Kyu et al (2008)

Min-Kyu et al (2008) added that all the four components are vulnerable and open to threats and attacks, thereby compromising one or more of the three fundamental security objectives of confidentiality, integrity, and availability. Today's digital and electronic society depends so much on wireless network for transactions and activities. This is because of the numerous benefits associated with wireless networks as found by, Ankush and Karnik (2005): improve the productivity of the mobile employees by, reduce installations cost, flexibility (in general) by 38%; reduce in cabling cost by 61%; mobility within building or campus by 39%; convenience (no plug and play); ease of collaborations; and reduce in facility cost by 17%. This therefore promoted the deployment of wireless networks in offices

and organizations. **However, for security reasons, the deployments must adhere to standards.**

The common theme that appeared in the definition of wireless network is (Tom and Les, 2002). The most interesting thing about wireless network is computing and network devices can communicate without tie to physical wires. This has given users the freedom of connectivity without boundaries of space. This in turn provides flexibility of deployment and installation of wireless infrastructures. Other benefits achievable in wireless network include cost, convenience, availability and on demand access. Thus wireless network makes life easier, convenience and break the barriers of space, time, and distance in transactions.

No wonder, the benefits of wireless network attract individuals and organizations to embark on the use and deployment of wireless network in day-to-day affairs on many aspects of transactions. The increasing demand for wireless connections coupled with digitalization and automations of office and organizational functions, has boosted the proliferations of wireless networks. As vital information are flying over the air in the forms of finance, intellectual data, secrecy, technologies, knowledge and skills, saboteurs and criminals are ready and prepared to access, intercept, and cause havoc to the network and the information. With signals propagating over the air, it is easier to compromise the signals using the appropriate trapping devices. *However, the regulatory body for Wireless network soon realizes this and attempts to provide wireless network with integrated security.*

2.2.2 WLAN and its integrated Security

Transmission by wireless network floats over the airwaves and become open to hackers and authorized users. (2012) states that to protect data/information from being captured and modified, the IEEE 802.11 standard introduced what is known as Wired

Equivalency Privacy (WEP) protocol. The protocol defines rules and procedures by which data can be transmitted with certain degree of security assurance. As the popularity of wireless network increase and continue to grow, some flaws were noticed in the WEP. Kevin (2013) identified theses flaws as: passive attacks to decrypt traffic (based on statistical analysis); active attacks to inject new traffic from authorized mobile stations (based on known plaintext); active attacks to decrypt traffic (based on tricking the access point); dictionary-building attacks (attainable after long analysis of traffic on a busy network). However the biggest problem is when users share the key randomly or disclose the key to unauthorized person through social engineering.

The initial objective of WEP was to bring it to the same level of security with wired LAN. Dongsheng (2011) argue that WEP performance is disappointing, it is out-of-date and inefficient. Dongsheng (2011) addressed the flaws of WEP by Sormon (2004) established that organizations who wish to migrate to WLAN due to security issues can now do so by implementing 802.1X which implement advanced security techniques, and which are managed by a radiu server. Similarly, with 802.11i-based solutions, the integral WLAN security is still assured. Siemens recognize such assurance in Williams (2004) as thus:

"By incorporating 802.11i-based solutions as part of a multilayered approach, enterprise network managers can reasonably ensure WLAN security. Although threat mitigation is an ongoing process, 802.11i and Advanced Encryption Standard (AES) provide WLANs with security as good as that available for wired LANs."

It could be understood that all the previous authors attempted to describe WLAN security, but indicating the susceptibility of WLAN to attacks, aided by the user through hacker manipulation. This is supported by Bogdan (2007) who asserts that despite advancement in security in the field of network and information security, the field of Information security continues to witness innovations in cryptographic techniques, network pro-

tocols, and hardware token. Moreover, Siemens (2008) assert that the effectiveness of WLAN security is addressed by the integrated standard technologies in the three critical areas of data confidentiality and integrity; authentication and access control; intrusion and detection. Unfortunately, user security misconduct can compromise one or more of these critical areas. This is supported by Bogdan (2007) who argues that despite these advancements, user is the weakest link and human gullibility remains extremely vulnerable. Similarly, Tim (2008) assert that while WLAN security attempt to control who access what information through identifying, verifying, and confirming that the requester is not an impostor, yet there are attempts to by-pass this security scrutiny through the mechanism of brute force or guile. **He added that those who use this attack mechanism are called confidence men or con artist in the past, but now they are called social engineers. Thus, network enters a new generation of human centric threats and attacks.**

The evolution of Network and Information Security

Mahi and Anup (2005) argue that the evolution of information security started from technical, to process, and to the current (3rd) generation of human factor. The evolution started when the technical system of security started to prove insufficient in protecting assets in which concentration on security was on the emerging threats from viruses, worms, and distributed denial of service (DoS); and the counter measures used were firewalls, antivirus, and IPS. The concentration on these measures shifts threats to procedural and managerial lapses. This drew attentions to security controls through policies and risk assessments strategies. However, the failure to match theory with practice weakens the managerial controls. Min and Anup (2005) assessed that organizations spend large sum of money on policies and documentations of security strategies, but the documentation outnumbered the need to implement the strategies. This gave room for misconfigurations, excessive trust in

security technology, and lack of attention to security flaws in the technologies. *The conse-quences was the rise of human factor in security where user is exposed as an un-protected, unsecured, and open target to hackers.*

Figure 4: The evolution of the network and information security.
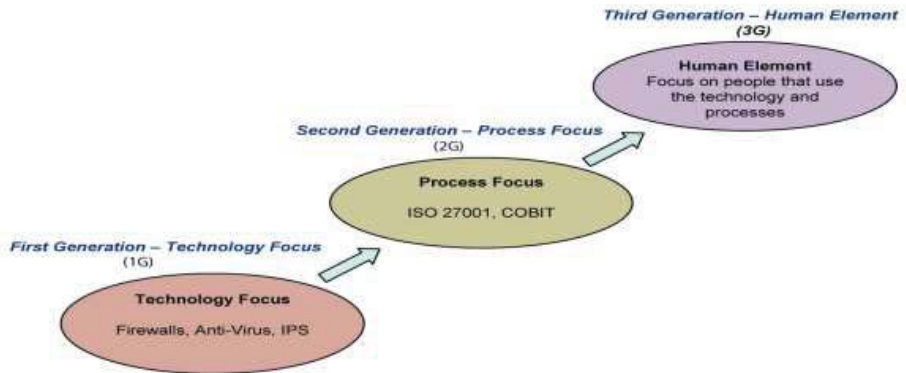
The evolution model of security has clearly exposed human factor as the current target of threats and attacks in this generation of e-of-things: e-learning, e-government, e-banking, e-security; which lead to the proliferations of wireless networks. The emergence of human factor threats and attacks on WLAN is evident in social engineering. This is col-laborated by Berti et al (2004) who assert that solutions to security is far beyond implemen-tation of physical and technical controls, social control is as well fundamental. The current research therefore identifies itself with the current generation of threats and attacks through social engineering.

2.3   Social Engineering (SE)

Social engineering is commonly referred to as the manipulation of people to give out in-formation or perform some action which otherwise would not have done if they are aware of the implications and the consequences. It takes advantage of human weaknesses and

believes that the weaknesses can be exploited. Ira and Winkler (1995) define social engineering as the term hacker community used to describe the techniques of using social interactions to obtain information about a "victim's" computer system, and in most cases password and log in credentials. They further assert that while organizations spend millions of dollars to protect their network and information resources, social engineering can bypass the expensive security measures. They concluded that security officers should consider non-technical aspects of security alongside the technical measures. In another definition, Gary (2008) defines social engineering as the use of social skills to manipulate user to provide the information that can be used to have an unauthorized access to assets. This is supported by Mitnic (2000), a renowned social engineer, defines social engineering as a collection of techniques applied to manipulate people to perform an action or provide confidential information.

In another definition, Aaron (2004), defines social engineering as the use of human relations to achieve the goal of infiltrating attacks through the information obtained from the victim. Dimension Research (2011) also describes social engineering as the act of breaking corporate security by manipulating employees into divulging confidential information, preferably passwords or other confidential information. The following graph (**figure 2.4**) is an extract from Dimension research that depicts the level of social engineering awareness among IT security professionals and general IT personnel.

Figure 5: Level of SE awareness
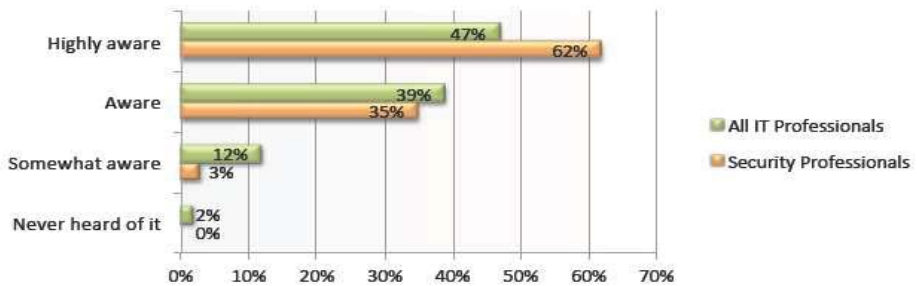
The chart displays the findings of a global survey conducted by Dimension Research under the sponsorship of Check Point between the months of July and August 2011. The survey involved 853 IT security professionals and general IT personnel. The aim of the study was to collect data about the perceptions of SE attacks and the consequences on businesses. It could be deduced from the graph that the result of the survey revealed that IT security professional and their counterpart in other IT related professions, are very much aware of SE. Their silence to focus on countermeasures indicates their expectations for solutions.

Meanwhile, their focus seems to concentrate on the technical-automated system for solutions to threats and attacks. However, the automated-technical system is proving insufficient to challenge the current generation of threats and attacks, not because the technical system is incapable, but because of the shift in focus on attacks; and coupled with the difficulties - requiring more persistent efforts to crack the technical system, cause attackers to carry out their nefarious acts through less difficult, low persistent, and through the weakest link.

Instead of attacking machines and software directly, they resort to attacking the user through social engineering. Kevin (2012) defines SE as using influence and persuasion to

deceive people by convincing them that the attacker is someone he is not, or by manipulation. Sherly et al (2010) also define SE as the use of disguise, cultural ploys, and psychological tricks to get computer users to assist in their illegal intrusion or user of computer system and networks. Similarly, Dang (2008) define SE as the art of persuasion to cause individuals to disclose sensitive information or perform an act. However, Nyamsuren et al (2007) added that social engineering includes illegitimate access and possession of physical hardware items and exploitation of information by means of cunning. He added that as long as individuals continue to fall prey to hackers, allure of gratuity and greed, then the sophistication of security system and the strict implementation of security policy will not protect organizations from SE attacks. As a result, the social engineer is able to take advantage of people to obtain information, or to persuade them to perform an action item, with or without the use of technology. In another definition by Maridna et al (2013), SE is the art of utilizing human behavior to breach security without the victim realizing that they have been manipulated. As a result of his role in popularizing SE, the following extract from Wikipedia, describe Mitnick, the renowned social engineer:

At age 12, Mitnick used social engineering to bypass the punchcard system used in the Los Angeles bus system. After a friendly bus driver told him where he could buy his own ticket punch, he could ride any bus in the greater LA area using unused transfer slips he found in the trash. Social engineering became his primary method of obtaining information, including user-names and passwords and modem phone numbers.

Mitnick first gained unauthorized access to a computer network in 1979, at 16, when a friend gave him the phone number for the Ark, the computer system Digital Equipment Corporation (DEC) used for developing their RSTS/E operating system software. He broke into DEC's computer network and copied their software, a crime he was

charged with and convicted of in 1988. He was sentenced to 12 months in prison followed by three years of supervised release. Near the end of his supervised release, Mitnick hacked into Pacific Bell voice mail computers. After a warrant was issued for his arrest, Mitnick fled, becoming a fugitive for two and a half years.

According to the U.S. Department of Justice, Mitnick gained unauthorized access to dozens of computer networks while he was a fugitive. He used cloned cellular phones to hide his location and, among other things, copied valuable proprietary software from some of the country's largest cellular telephone and computer companies. Mitnick also intercepted and stole computer passwords, altered computer networks, and broke into and read private e-mail. Mitnick was apprehended on February 15, 1995 in Raleigh, North Carolina. He was found with cloned cellular phones, more than 100 clone cellular phone codes, and multiple pieces of false identification.

Mitnick (2002) claims the followings on BBC News Online.: "The lethal combination is when you exploit both people and technology," and again: "What I found personally to be true was that it's easier to manipulate people rather than technology," again: "Most of the time organizations overlook that human element," he concluded: "The weakest link in the chain is the people," The biggest threat to the security of a company as claimed by Mitnick, is not a computer virus, an unpatched hole in a key program or a badly installed firewall. In fact, the biggest threat is the user. The user is easier to manipulate people rather than technology. This is often overlooked by organizations and IT professionals. The biggest threat to the security of a company as claimed by Mitnick, is not a computer virus, an unpatched hole in a key program or a badly installed firewall. In fact, the biggest threat is the user. *Thus it is easier to manipulate people (users) rather than technology. This is often*

overlooked by organizations and IT professionals; as there are various forms of SE which
are ignored and not taken seriously.

2.4   Classification of SE

Sandouka et al (2009) identified ten kinds of social engineering: impersona-
tion/pretexting, dumpster diving (trash searching), third party authorization, phishing, vish-
ing/IVR, spam emails, instant messages, pop-up windows, social software, and Trojan
horse. This converged under two broad divisions: technical-based social engineering and
human-based social engineering. This is confirmed by Huber et al (2009); and supported
by Abraham et al (2010); and Bezuidenhout et al (2010).

Against this background Mohammed et al (2010) proposed Taxonomy of social en-
gineering attack (SEA) aimed at enlightenment on how to identify SE attacks and take
counter measures. They model is depicted in **figure 6**. It is the Taxonomy of Social Engi-
neering attacks.

The Taxonomy reveals that social engineering attacks are both human based and
technical based. According to the taxonomy anything physical presence that attacks a net-
work system, is considered as human based; and anything online and software based influ-
ence to the user, is considered as human based. While this taxonomy helps through some
lights on SE, the model of this research added more entities that play significant roles in SE
attacks.

Figure 6: Taxonomy of SE attacks
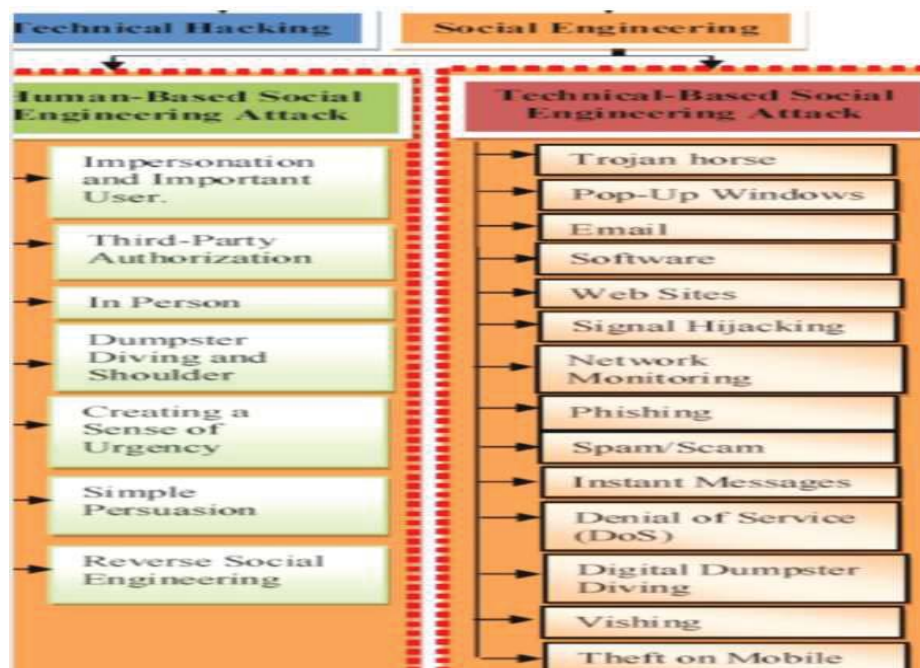
Source: Mohd et al (2011): *Social Engineering Attacks model*

The model does not differ with the previous models in their conceptualization of SE. The model has contributed to the understanding of SE and its classifications. While the model does not explain how the identified SE attacks should be counteracted, the current study found the contributions helpful in considering how the proposed model could provide user with the requirements necessary to identify and prevent SE threats and attacks on their WLAN.

Sandouka et al (2009) discovered that social engineering is often overlooked because of the misconception that technology is enough; users overlook the capabilities of SE; and as a result of laziness, fatigue and subjective judgment, security policies are not observed or implemented properly. Their findings agreed with the claims of Mahi and

Anup (2005). In 2004, Computer Crime and Security Survey conducted by CSI/FBI indicated that 66% of security incidents were from inside – the users. User is becoming the biggest threats to organizational network, assets and resources. The most sophisticated security technology cannot beat user threats. Scott (2007), argue that security is fundamentally a human issue. Army (2007) collaborated this by asserting that unlike applications that can be updated or patched, systems that can be hardened, end users – whether through naiveté, carelessness, or malicious intent, continue to expose IT resources to serious security threats. The user succumbs to the wishes and command of the hacker through various techniques.

2.5 Techniques in SE

Technically, connectivity between client and server is done through the user agent, called a UA, by initiating connections to the HTTP server. The UA initiate the connection with request, and upon authentication protocols, the request is approved by taking the client to the request site and the information requested is provided thereon. The basic requesting information is usually the request method, the Uniform Resource Identifier (URI), and the protocol version. Social engineering follows the same pattern, but added an incentive or gratuity to the client (or the user). In a study conducted by Workman (2008) with 588 participants in insurance and financial organizations in the US, the study attempted to found our whether the marketing strategies used by marketers and advertisers also apply to social engineering techniques. The result revealed that participants tamed with gratuity are willing to comply to the request even if it means giving away their login details, corporate data, email addresses, and other sensitive information. However, in a security system or model that is transparent with accountability and responsibility obviously exposed to all users, the

compliance to phishing and socially engineering request may not succeed or supported. The current research aimed to deactivate such habits with the proposed model.

Social engineer takes advantage of human weaknesses and believes that the weaknesses can be exploited. Kurt (2013) mentioned five routes a social engineer takes to lure the victim. The first route is diffusion of responsibility away from the target individual. This means that the victim is made to understand that the engagement has no implication or liability to the victim. The second route is the attacker masquerading the boss. The third is minimizing conflict with the target. The fourth is imploring the target to have strong sense of moral duty. The fifth is allowing the target to feel in control. The sixth is increasing sensory perception for the target. The seventh is intimidation. Kurt (2013) suggested that the best way to counteract SE is to educate employees to identify the attack, and create more barriers than holes for the attacker. He concluded that the organization should create a central security alert system so that user can promptly spread the information across the board. This is in line with this current research that proposed a social system of security involving the users.

Byod, (2003) states that deception in SE is of two types: simulation and dissimulation. (2003) assets that simulation resembles mimicking, spoofing or imitation to reality, and it is a kind of is phishing attacks. (2003) mentioned other examples relating to simulation, like a false email from Microsoft asking the user to apply updates or patches. (2003) also identified decoying as part of simulation, it is a case of warning an alert announcing an attack and the attention of the user is required to subvert the attack. On the other hand, dissimulation as fined by Bowyer (2003) is covering the truth. (2003) mentioned that the act of covering the truth is done in three ways: information masking (hiding malicious codes in a software), by Trojan horse, and by curiosity (like attaching a nude picture) in an email. In

another attempt to describe the techniques used by hackers to lure users into their nest, Albert (2007), represents the factors that influence user to yield to the traps of social engineering. The following diagram in **figure 7**, visually describes those factors

Figure 7: Factors influencing user in SE

Source: Albert (2007): *A Practical Approach for Combating Social Engineering in Your Enterprise*

Although the diagram may not have covered other psychological elements that explain easy yield to hackers' wishes, yet it contributed to the understanding human elements in propelling attacks. From the diagram, *it is clear that some psychological elements were identified to be the gateway for social engineer to influence the user to disclose log in password or the details of the network thereby facilitating unauthorized access to the network.*

2.6   Wireless attacks and Social Engineering

WLAN is prone to threats and attacks because information is exposed through its electromagnetic propagation over the air. From the year 1999, Wi-Fi was released. Wi-Fi is the term used to describe the brand product belonging to a category of Wireless LAN; and since the release of Wi-Fi fear over threats and attacks continues to mount in organisations and by security professionals. In 2001, WEP (Wired Equivalence Privacy) access protocol was discovered to have some security flaws which facilitate bypassing the security with less effort. In 2003, the flaws were corrected with the introduction of WPA (Wi-Fi Protected Access). The increasing dependence on IT infrastructures coupled with increasing proliferations of BYOD continues to put IT security in solutions chaos.

Organizations must accept BYOD as inevitable, but use it to the best advantage. One area BYOD could be put to advantage by organizations is in the implementation of the SNS model of this thesis. The workplace is changing with users becoming more IT focus and oriented. The best thing to do by organizations is to consolidate the evolving changes to an advantage. In as much as security is becoming the number one concern in this digital age, the integration of the workforce into a security system that is participatory and collaborative, is not only essential but highly desirable. BYOD can be used to achieve this level of workforce engagement for security.

The use of BYOD in the workplace facilitates the implementation of the SNS model and achieve desirable performance as per as security measures and controls are concerned. Threats and attacks are evolving every minute, and with BYOD, users can on real-time learn, update, and share their security encounters promptly and immediately. Thus with BYOD, the workforce is current, interactive, engaged and active in their contributions to security matters. This therefore promotes construction and assimilation of security

knowledge through social learning on the platform of social media. With the integration of BYOD in the SNS model implementation, security is shifted from central control to user-centred control where participations and real-time learning are emphasized. Thus the pyramidal security control is now flat and horizontal promoting security collaborations and engagements of all users.

The most fear expressed by organizations about BYOD is the issue of security and privacy. As BYOD is to be used for security collaborations, such fear is then turned into asset. In this digital age, it becomes imperative to prepare the workforce for cyber security skills on an ongoing learning process. The achievement of this can be made through the integration of BYOD in the security system that is of the users, by the users, and for the users, as contained in the SNS model of this thesis.

Dalamini et al (2009) assessed that the future of IT (and network) security continue to be clouded with fear, anxiety and uncertainty. They declared that two things stand out in the IT security challenges: IT infrastructures are vulnerable and hackers are after the vulnerabilities. The second challenge is that threats from social engineering are becoming sophisticated and this requires innovative ideas to cope with the challenges. The proposed model of the current research is one of the calls for the innovative ideas. Dalamini et al (2009) also claimed that the 21st century is witnessing emerging threats from human factors that are motivated by pervasive computing – the e-of-things (everything goes electronics). This therefore place the society on dependence on IT infrastructures, which as Dalamini et al (2009) observed, *is opening more doors for hackers and attackers to deceive users through phishing and other forms of social engineering, so as to gain access to their information and network resources.*

2.6.1 Social Engineering in Phishing

One of the fundamental components of SE is phishing attacks. Phishing in electronic communication means attempt to lure the user to provide information or perform some actions that imply some benefits to the user. This implies that any form of deception either online or offline is referred to SE. Gulati (2003) established that behaviors that are vulnerable to SE attacks are trust, carelessness, curiosity and ignorance. Gutner (2013) states today's threats and attacks rely on social engineering to leverage and exploit technology weaknesses.

The success of phishing depends so much on social engineering. Gunter (2013) established that phishing attacks rely upon social engineering for its success. This is because the victim must be persuaded or convinced before performing the actions the determined attacker is expecting. Gunter (2013) further illustrated that the phisher has many other nefarious approaches of social engineering victims into giving out confidential information.

For example the victim may be tricked into updating network login details, for the system has recognized login attempts with the victim's credentials. The victim is now required to login with his/her normal login to confirm that he/she was not the person who made the previous attempt. The phishing message coined in social engineering continues as thus: This is necessary so as to block the other person from further accessing the network through your account. Gunter (2013) further added that the phishing rely on social engineering to cause the user to perform auxiliary services on behalf of the phisher while the phisher perform the rest of the actions.

Phishing, as the name sound, is exactly similar to the word "fishing," meaning deceiving the fish with a food, whereas the food is attached to a hook that captures the fish as

the fish grabs the food. The fish, in most cases, cannot get free from the hook once it is captured. Phishing in the electronic IT world is sending genuine looking emails or instant messaging, asking the user to open an attachment or click a link in order to access an offer or update profile.

Once the user performs the action expected by the attacker, the information provided by the user is then used to launch an attack, thereby making the user the fish, forefront, or proxy of the attacker. Gunter (2013) defines phishing as "the process of tricking or socially engineering organization's employees into imparting their confidential information for nefarious use." The technique of phishing is called by Emm (2006) as take the bite and gets hooked. Phishing is also named as semantic attacks. Schneir (2000) defines semantic attacks as the form of attack that target human vulnerabilities in their interactions with computing resources.

A number of studies, notably by Mercuri (2006); Brody et al (2007); Anderson et al (2008); and Eisenstein (2009) have found that phishing is one of the common techniques used by hackers to influence users to carry out attacks. The hook of phishing is associated with benefits, offer, fear, trust, or command that causes the user to bite the hook or execute the instructions. This could be in the form of clicking a link, opening attachments, filling a form, resetting username and password, or answering online questions.

Matthew added that the aim of spear phishing is to gain access to the organization's network and information resources by tricking the victim to provide IP or network credentials or other information that would facilitate access to the network by the attacker. Emails being the common mode of communication, as highlighted by Gunter (2013), that email remain to be the favorite vector for phishers. The criminals mimic corporate website, corporate and individual emails so as to establish credibility or make the user to trust the hook.

The threats and attacks from phishing are increasing and becoming sophisticated in style, including screen captures and man-in-the-middle data proxies. RSA (2013) reported that between the years 2011 to 2012 phishing attacks increased by 22% and has caused the global economy over $1.2B.

Another join survey by US and UK firms having between 100 – 4999 employees have found that 55% of the companies surveyed experienced we-based phishing attacks in 2012. In another study conducted by Sarel et al (2006), on the web contents of 200 US banks, they found that customer awareness to phishing attacks is higher with bigger banks than with smaller ones. These all points to the fact that phishing is becoming a serious security concern that efforts should be geared towards countermeasures, thereby acknowledging and clarifying the purpose of this research.

E-mails remain the favorite medium used by phishers to hunt their victims, although other means continue to emerge, as Gunter (2013) pointed out in figure 4. These emerging tools include exploit material and attachments used to deliver specialized payloads, such as key loggers, spyware, rootkits and bots. Others are message boards; web banner, advertising, instant chat (IRC and instant messenger) and Voice over IP (VoIP).

Figure 8: Methods used in Phishing
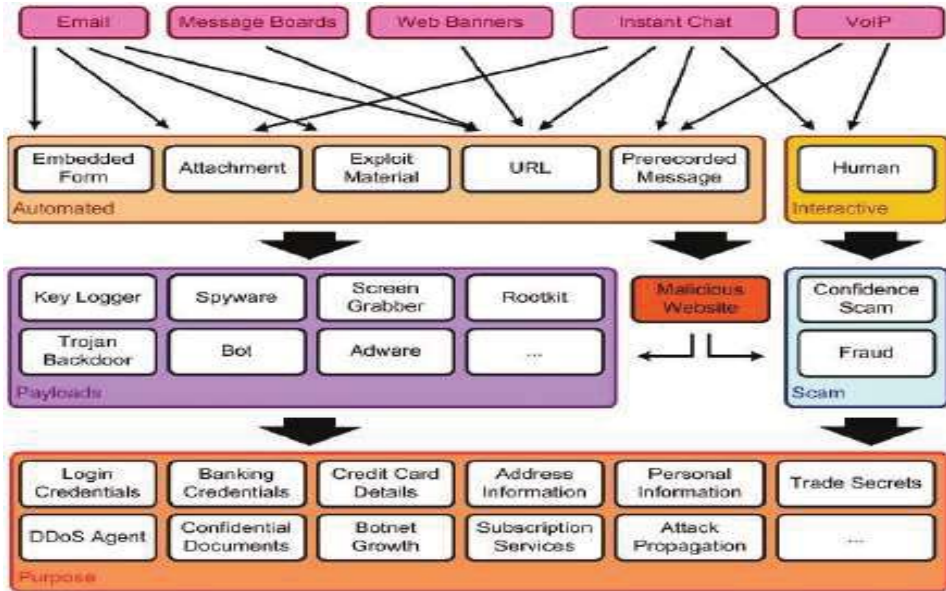
Source: Gunter, O. (2013). *The phishing Guide: Understanding& Preventing Phishing Attacks*

As observed my Marshal et al (2005) and Knight (2004), it takes little effort with less cost to create spoofed website or email. Various studies have identified various styles of phishing. For example, Goring et al (2007) identified code-based key-logger; Eisen (2009) identified in-session Phishing; Bargadiya et al(2010) identified search engine phishing; and Rush (2005) identified drogant, rod-and-red, lobspot, and gillnet phishing. However, five main types of phishing are the dominantly user focused. Matthew (2013), identified two types, the normal phishing and spear phishing; While, Gutner (2013) added Pharming, "Smishing", and "Vishing". The normal phishing is associated with sending unanimous emails to unanimous individuals or corporate victims; while spear phishing is focusing on specific and targeted individual or organization. Webroot (2013) identified automated phishing countermeasures as thus:

2.6.2 Smishing

Using Short Message Service (SMS) on mobile phones, with various styles of social engineering tones, user can be tricked into performing some actions for the phisher. The following examples (a – c) reported by Gunter (2013) are SMS messages to potential victims:

a.   *Automatic credit watch alert! A new line of credit has been established for you at The Big Electronics Store [Well known store]. If this is an unauthorized application, please call 1-800-xxx-xxx.*

Thus, calling the number for curiosity purpose may lead to more tempting actions to

Surrender certain information that could be to the advantage of the phisher.

b.   *You have exceeded your monthly Universal Cell text messaging allotment.   Text messages will now be charged at 50 cents per message.   Reply to this text message with your online authorization code to send an additional 500 messages for only $2.*

c.   *hello, this is Sharan at The Power Company. I am urgently trying to contact you to discuss your move to Los Angeles and confirm the closing of your account and your scheduled end of service. At the present time, all power to your address will be terminated at 9:00 p.m. tomorrow evening. Please call customer support at 1-800-xxx-xxx to arrange for final bill payment.*

2.6.3 Vishing

Gunter (2013) describes "vishing" as the combination of voice and phishing by leveraging IP-based voice messaging technologies (Voice over Internet Protocol, or VoIP) to socially engineer the intended victim into providing valuable information. The use of IP telephony provides easy cover for the attacker, because as Gunter (2013) pointed out the calls can start and be terminated at a computer anywhere in the world. Furthermore, Gunter (2013) identified the followings factors that make vishing appealing to the phisher:

- Ability to reach victim from any location in the world

- It is cost less

- Ability to mask or encapsulate caller ID data

- Ease of automating calls (war dialing)

Bypassing phrase analyzer technology in the victim's network or device

- Lexical analysis – by identifying frequent expressions

- Reputation analysis and backlisting – by flagging websites associated with phishing messages and the websites recognized to have been capturing information from victims.

- Signature recognition – by identifying malware in attachments

Mardina (2013) suggested that the only way to mitigate security risks from SE is to educate users to create awareness to the SE threats. While the definition of SE falls short of certain elements that should explain the reason why user is the victim of social engineering, the following studies throw more light on dispositions that make user the target of SE. Instead of manipulating hardware and software to gain access to organizational network or take possession of certain information, hackers manipulate the user to execute their criminal activities. Phishing attempts to persuade the user to reveal information useful for the attacker. Phishing also involved planting malware onto victims' network with the aim of trapping the user to take the bite of what is offered on a webpage.

Through email and clickable link, attackers can install malware that exploits the network. Phishing is increasing with sophisticated strategies and styles. From January 2008 to January 2010, phishing attacks doubled its action (Phishing work group, 2011). Ira et al (1995) experimented SE on a company's network and the result yielded sensitive company information obtained that allowed the hackers to infiltrate the company's network and cripple the information system, despite extremely good security measures. Ira (1995) further revealed that many of the weaknesses used by the attackers are common to most companies. They suggested that expanding upon the weaknesses will assist companies in over-

coming weakness posed by SE through employees alerting their coworkers, and implementing good security awareness programme.

2.6.4   Intrusion through Malware SE

Social engineers and phishers prefer to access the network and its resources through the user. Sherly et al (2010) observed that for social engineering malware to succeed, it needs to be activated by the end user. Although the technical system can block it, but as Sherly et al (2010) assert, once the malware is inside the end user's machine, it opens backdoors to spread to other machines and build defense for it detection. Various channels are used by authors of malicious codes to send social engineering malware. These channels are identified by Sherly et al (2010) as email, social software, websites, portable storage devices, mobile devices, and bring your own devices (BYOD).

Through social engineering, malware is spread by hackers through email attachment, clickable links, file or multimedia download. A hacker can also compromise some web sites, infecting the website in such a way that when a user visits the websites, the user's device will automatically be taken over by the malware. Thus web-based malware include IFRAME injection, Javascript Injection, and Redirect Infection. In **figure 9** Sherly et al (2010) describe how SE is used to attack a victim.

Figure 9: How SE is used to attack a victim

Elodie (2008)
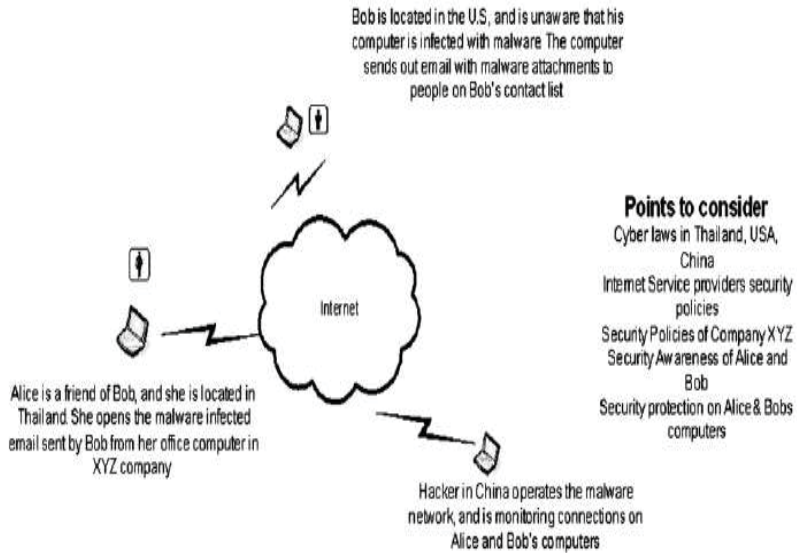
Through SE malware, as Elodie (2008) assessed, a friend's compromised system can send another victim URL recommending visit to the site to view some pictures. He further added that irrespective of the level the SE malware was sent, it usually contains phonographic links/images; feminine name; soliciting for donations; free games and anti-software tools.

2.6.5 SE at Web level

Websites are the launching ground for malware on user's networks and computers. The social engineering malware website camouflage, mimic the original websites. Sherly et al (2010) stated that websites are used by hackers to fool users by altering the content, appearance, or images of the website. Tiauzon (2006) reported that in 2008, malware was able to send query to CNN news and obtain data that it used further to attach malware and

send it again to the news and sports section of the news giant. In the efforts to ensure that user does not remain a proxy to hackers and a gateway to threats, many scholars attempt to transform user to the state of TES (Technology Equivalence Security), on human-based (semantic) attacks. For example web indicators and domain name are areas that attracted the interested of researchers to provide the user with the fundamental skills to avoid being misled or fooled by fake domain names.

In spite of the standard measures like SSL and TLS, users are still deceived into entering their passwords on scam websites. There are various studies that attempt to im-prove user habit in this direction. Among such studies are: VeriSign (2012) which exposed user to SSL authentication for security control, as a reliable authentication of the site the user is submitting information.

Similarly, Batya (2002) et al characterizes users' conceptions of web security. The study drew from three technology- educated communities of 24 participants from each community. The results revealed errors of commissions among the responses of the partici-pants. In another study, Evgnenity et al (2002) exposed users to mograhp attack whre suers a fooled into accepting a fake website in which an equivalent letter in a foreign language is changed in the URL name. They demonstrate such as thus:

> "*To demonstrate the feasibility of the described attack, we registered a homographed*
> *Domain name* http://www.microsoft.com*3, which incorporates Russian letters .c.*
> *and.o.. While it may be tricky to type in, especially if your computer does not fea-ture a localized keyboard layout, you can access this URL from*
> http://www.cs.technion.ac.il/~gabr/papers/homograph.html4 *".*

This is collaborated by Sherly et al (2010) who asserted that camouflaging strategy manipulate words in web addresses, psychologically taking off the attention of the user on the wordings.They further added that the malicious codes alters the user's office or home

network address settings, thereby given the hacker control over the network. The work of Amir et al (2002) also supported this by stating that in spite of sites invoking SSL to protect users' passwords; attackers succeed in getting users' passwords through spoofed web pages. Against this background, Amir et al (2002) developed Trustbar in which user can assign name or logo when Trustbar returns secure site certificate or otherwise as the user log onto the site. They tested the Trustbar and found it effective, but cautioned that OS vulnerabilities could render it ineffective. They recommended user education and guidelines for secure web and email usage could enhance user security habit. Moreover, Collin et al (2002) measure the effect of extended validation only legitimate certificates and the effect of reading help file about security features in IE 7. They found that picture-in-picture is as effective as homograph attacks. They also found that participants who received tutorials are better in the identification of real and fake web site.

However, hackers would still mimic the trust indicators. The countermeasure to this would be users who is security proactive, and that is the focus of the current study. In additions to these scholastic contributions security vendors also developed user-tutor interfaces that warn and guide user on security precautions and practice. For example Mozdev (2013), offers toolbar indicator that enable users to save trusted website visited and when later wanted to revisit that site again, if spoofed website appears, it then notify user of distrust. Similarly, Soopstick (2013) offers anti-Phishing tools. while efforts in this directions are laudable, however, technical packages outnumbered non-technical packages and like the security policy mentioned in the upper part of this chapter, users either found it too technical to do the right thing, or the approach that can transform the user is lacking enabling structures. Other contributions protecting user from phishing attacks are that of Stuart et al (2007) who evaluated website user authentication measures. Their findings revealed

that users on the role play disregarded security attack cues and entered their passwords while participants who received security training were more careful in putting their pass-words.

Researches attempt to teach users how to identify and counteract SE. Their contri-butions have proved that users with the appropriated training can able to succumb SE threats and attacks. However, Chris (2009) observed that unless education is made period-ic habits, users may forget to apply the knowledge or apply it wrongly. This is in support of the model of the current research that is based on real time, continual and updating knowledge and competencies of users. In another attempt to desscribe how users are lured into a spoofed website, Knight (2004) designed the stages a user is taken to a spoofed website as depicted in

Figure 10: User lured to Spoofed Website

It could be deduced from figure that, though not an attempt to access network log in credentials, but the process could be used an adopted for that purpose too. This has con-

tributed to the understanding of the process for blended programme aimed at user knowledge.

Various authors have proposed the use of toolbars to deliver phishing messages to users. For example, SpoofStick (2004) can indicate to users the hidden domain name when phishers use a legitimate domain as: www.paypal.com.wws2.us, but SpoofStick would display it as wws2.us. Wu et al (2006) claimed that those solutions are not effective for the following reasons:

One, the position of the indicator is not strategic enough to raise the attention and action of the user. Second, users ignore the security warning because the intention is not to apply security control but to access some web contents. Third, the inconsistency in web indicator confuses users to ignore the warnings and consider them as waste of time. Fourth, the warning signs offer no alternative actions to users, thereby making users to take the risk of submitting their information, as their own alternative.

In view of these weaknesses, Wu et al (2006) proposed web wallet which a browser type where users can enter sensitive information and the web authenticate the destination site before allowing user to send the data. The result of the implementation of the test wallet revealed that it significantly reduced the spoof rate of normal phishing attacks from 63% to 70%, and achieved 100% prevention of the phishing attacks while in use. While the current research is not developing a technical solution in the case of web wallet, however such solution is considered as instructional resources to the current research.

2.6.6 Social Engineering in IM

Automated Social Engineering (ASE) through IM (Instant Messaging) is another form of attack that is common on social sites. Tobias (2012) experimented on Honeybot man-in-the-middle automated SE, and proposed countermeasures against the attack. In

their experiment they demonstrated how to take control of IM (Instant Messaging) by ASE (Automated Social Engineering) mimicking man-in-the-middle attack. They bootstrap the conversation between two participants and influence them to click a URL link inserted in the chat messages. They found that after sending four messages, about 4 participants clicked on the link. Similarly, Huber et al (2011) experimented on ASE by inserting a bot chats on Facebook (FB) users to lure them to malicious online survey. Through the use of Artificial Intelligence Markup Language, they were able to stand in the middle of the conversations and sending replies from each to each participant. After three sent messages, they found that 80% of the participants enjoyed and remained longer in the conversation than the human true human chat. These studies agreed that although technical solutions can be set to control this type of attack, but suggested that user awareness and training is the best. These studies have contributed to the understanding of sophistication of SE and the current research is fit in their recommendations by extending awareness to real live unconscious competence security habit.

2.6.7   SE in Social Software

Social software enables communication and interaction among users. Sherly et al (2010) describe social software as loosely connected applications that enable intaractions across the web, and it includes instant messages, social networking, websites (FB, Twitter, Myspace, Linkedln), blogs, Wikipedia, etc. Most of the social networking sites are hunting ground of attackers. Narain (2010) states that social sites, like FB and Twitter are attacked by deceiving users to click a link that end up to downloading nefarious software into users' systems and the network. Sherley et al (2010) added that SD_BOT is also common social software spreading from infected friend's system. Similarly, Fergusen (2009), reported the

spread of Koobface on FB in which he received a message from friend (spoofed profile) suggesting a video link, and Fergusen observed as thus:

"Clicking the Install button redirects to a download site for the file setup.exe which is the ***new Koobface*** *variant detected as WORM_KOOBFACE.AZ. It is hosted on an IP address in another part of the world, and in the last hour, we've seen 300+ different unique IP addresses hosting setup.exe and we're expecting more. All seen IP addresses hosting the said malicious file are now detected as HTML_KOOBFACE.BA*."

On the same Security blog, the following quoted comments were made by some contributors:

"*Researchers at Trend Micro are reporting that a new variant of the Koobface worm is spreading on Facebook.* http://is.gd/lmlS*."*

"*Don't go viewing any weird videos sent to you from friends. Even if they claim to have you in the star role!* http://tinyurl.com/dm6tcg*."*

"*RT* @gilzow*: Researchers at Trend Micro are reporting that a new variant of the Koobface worm is spreading on Facebook.* http://is.gd/lmlS*."*

All these indicate that social engineers are writing malicious software and utilize the curiosity and socialization of users to help them activate and install the software for further threats and attacks. Jagatic et al (2007) argue that Myspace, FB, Orkut, and LinkedIn are potential harvesting ground for hackers; as a result of their circles of friends hackers can harvest large amount of valid social network data.

2.6.8   SE at Email level

Automating email anti scams and phishing attacks is not easy. This encouraged research on user-based solutions. Sullivan (2004), reported Anti-spam firm MailFrontier Inc. survey where 1000 consumers were showed legitimate emails from companies but most of the time the participants could not distinguish between legitimate and spam emails. The worst of it was the genuine emails were mostly marked as spam. An email being the common channels of communication is as well becoming the common channels for malicious codes. Kienzle et al (2003) reported that the first social engineering malware (email) to hit

the world was in 1987, in the form of Christmas tree – Trojan horse. In another study, Fergusos (2005), attempted to promote email security awareness among corronade cadets with exercises aimed at exposing lapses in security awareness. The exercise began with hours of training awareness after which the 512 randomly selected participants were sent email message with a bogus URL that when clicked, it returns 404 error or page not found. The result showed that even with the training, more than 400 participants clicked the bogus URL and enters their credentials. The study recommended that regular awareness exercises with practical should be deployed to promote awareness and minimize network downtime. This is in line with the current study and extended the training to live sharing of experience on the social network platform.

In another study, Downs et al (2006), wanted to know how users confront suspicious emails by interviewing 20 users. Their findings revealed that users fall victim of emails scam not only because they are not aware of the dynamic styles of the context, but also because awareness campaign fail to enlighten users on the consequences and implications of their actions. In a similar study, In another scenario, Marcus (2005) described how access to network and its resources can be facilitated through email social engineering, where an employee receives an email from the system administrator informing him of the latest news on the spread of new virus worldwide; and ask the recipient to immediately download the attached software and run it for security precautions. The recipients comply and the concealed software sent success execution to the sender. Similarly, Jagatic et al (2009), in their Alice and Bob experiment, Bob was fooled into filling his university credentials in the spoofed email link. Using IU authentication, they were able to validate the passwords of the target victim. Moreover, in a real life incidence, a social engineering technique through email was used in January 2007 to steal over $1.1m. Dang (2008) re-

ported that customers were deceived by spoofed emails they received from their Nordea bank, to download and install anti-spam software for their security. Over 250 customers complied whereas concealed in the software is Trojan horse that furnish the criminals with the valid passwords of the customers, which they used to log into the website of the bank and steal money. In similar development, MessageLabs (2007) reported increasing escalation of spear phishing where executives of companies are targeted through malware emails. The malware authors crafted email with clickable links and sent to top executives. The clicked links directs the executives to web sites that download malware into their machines and copy keystrokes or gather sensitive information.

2.6.9 Pop-up Windows

Sharek et al (2008) examined methods used by adware and malware to trick users into clicking on malicious pop-up window buttons. Their findings revealed that despite the simultaneous appearance of warning windows besides the flashing pop-ups, the participants pressed the OK bottons, thereby activating the concealed malware and adware malicious software. The pop-ups windows in **figure 2.10** shows the genuine and spoof windows to deceive the user into clicking the hacker's windows. Thus pop-ups windows are becoming an emotional means of getting a quick action from the user. Pop-ups that are often used by Microsoft and other software developers to send messages to users are now turn into malicious carrier by hackers. Getting rid of pop-ups required technical skills otherwise user may end up doing exactly what the hacker wants.

Figure 11: Genuine and Spoofed pop-up windows

Real popup warning window

Fake, flashing popup warning window with black background visible (Fake 2)

Fake popup warning window (Fake 1)

Fake popup warning window with minimize button and status bar (Fake 3)

2.7   Implementation of WLAN security

The implementation of security on WLAN is approached from different strategies. Finn et al (2005) also stated that enterprises considered security as technical problems and thus confronted security with technical solutions, whereas procedural and user behaviour open more vulnerabilities for threats and attacks. Thus, security is said to be effective where both technical and social are married, integrated and support one another. While technical solutions continue to be the first line of defense, Anderson (1999) observed that user threats and vulnerabilities are difficult to control by automated technical system, like email habit. User threats continue to escalate, and as BERR (2003) found, 52% of organizations do not carry out any user risk assessments; and 67% do not prevent confidential data leaving on USB stick. In another study conducted by Ryoda (2009), 95% of data loses were attributed to users, while only 5% of the incidence was related to technology. Determined attackers are persistent and sophisticated in social engineering. There is an old African saying, that the vulture is a patient bird. Likewise nowadays hackers and attackers, they can initiate a relationship, continue to nurture that relationship until it is ripe for turning it

into marriage; and then start planning and executing their attacks. Using various SE techniques, hackers can penetrate a wireless network through spoofed web page. Amir et al (2002) observed that hackers find it easy and convenient to use spoofed web page to fooled users into getting their login details than using eavesdropping and other wireless cracking tools. This is also collaborated by Mitnick (2002) who stated that social engineering is the favorite tools for hackers and malicious code writers, because it is easier to trick user to give his/her password than to spend considerable efforts trying to crack a system.

Implementation of security system of any kind falls under technical, process, and user controls. Fin et al (2009) refers to these controls as technical, formal, and informal controls, where informal control refers to human. Although Zhang (2009) sees security implementation as technology based and people based, yet both agreed to the user based system of control. This agreement is supporting the focus of the current research. Fin et al (2009) defines each of the security controls as follows:

Technical Controls: are measures taken – physical and automated to protect the assets of the organizations against impeachment in confidentiality, integrity, and availability. Measures taken include bolts and locks, antivirus software, firewall, and IDS). Technical controls are easy to implement and the results are immediate. This is collaborated by Patricia (2008) who found that current approaches to security are focusing on technical measures, like firewalls and intrusion detection system.

Formal Controls: are the measures taken through defined code of conduct and procedures to regulate the application and usage of the assets. These measures include security policies, discovery and risk assessments, and segregations of responsibilities and implementation of indicators. Formal controls take time to implement and must undergo series of drafts, legal definitions, and series of reviews.

Informal Controls: are the measures taken to create security conscious, proactive, and security active user. Dealing with people is difficult and takes time to implement any solutions involving the user; like training the user to defend against social engineering threats, may take months or years. Patricia (2008) suggested that people should be given top priority in countermeasures to security threats and attacks. Most of the threats and attacks find their ways through users, and various ways can be devised to control user behaviour that might lead to compromising the security system. Carl (2009) examined various human factors that can be applied to monitor and controlling the user. Among the issues discussed include whistle blowing, monitoring staff activities, and snooping rights.

However, user monitoring could lead to clash of interest. Carl (2009) concluded by stressing that user threats cannot be eliminated but can be assessed and managed, including application of maximum "education, education, education"! However, Kerry-Lynn and Steven (2009) assert that despite user education, the culture of user towards security implementation must as well be addressed. Although assessment and managing user threats is part of the non-technical solution, but integrating the results of the assessment and managing it through education and best practice is another, which the current study have addressed.

2.7.1 The Automated-Software (technical) Contributions to WLAN security

The current study focused on WLAN security from non-computing and non-technical approach. Thus the review focused on user centered security related literature, including security policy and in-depth review on social engineering intrusion and countermeasures. Although the current research is not about automated-software security on WLAN, brief contributions of what have been done so far in the technical system of

WLAN security is hereby given so as to clarify the purpose of this study and expose the gap the current research aimed to fill.

There are many researches on intrusion prevention on Wireless Local Area Network. Each of the researches attempt to provide the mechanism for avoiding and preventing intrusion. Wen-Chuan, H. (2000) proposed a proactive wireless intrusion Detection System. This system provides solution for WEP cracking, MAC address spoofing and wardriving, through short Message Service (SMS) and proactive techniques. In the area of wireless traffic control, Dong, L. (2007) introduced a WTLS-Based Intrusion prevention model. The model built a logical sole path between wireless terminal and its destination so that IPS engine can detect and prevent threats in the traffic. Wireless Transport Layer Survey (WTLS) was then developed and used to test over-the-air traffic. In another study carried by Vartak, A. et al (2007), the researchers experimented on the over-the-air prevention techniques and came up with a system for mitigation unauthorized wireless communication access. In another study conducted by Jack, T. (2008), WLAN network security threats were discussed and his findings show that threats could be prevented through adaptation of attack techniques. In a similar study, Guarlin, C., et al (2010), presented a framework of WIPS with an intelligent plan recognition and pre-decision engine using honeypot technology, which can predict future attacks and directly respond to the attack.

Computers, access points and the transmission media is mostly the object of attacks. The various counter measures to these targets were provided by Min-Kyu C. (2008) in his study of wireless network security threats, vulnerabilities, and counter measures. Other researchers in the field of wireless intrusion prevention considered code injection as a safe method for intrusion prevention. According to John, (2011), the plethora of residual domain code injection counter measures, buffer over flows still plagues modern software. He

added that many of the attacks tested by test bed are now out-dated and thus a perfect "score" of protection countermeasures against them is of limited value. In their studies of RIPE (Runtime Intrusion Prevention Evaluation), John (2009) presented RIPE which executes a total of 850 buffer-over flow attacks against popular defence measures. They added that the main purpose of RIPE is to provide a freely available test bed which developing of defence mechanisms can use to qualify the security coverage of their proposal and compare them against previous work using a well-defined and real-world set of attacks. In another study by Shedhani, A. et al (2009), making use of secret keys generated by a private symmetric polynomial function and well-designed message exchange, the key distribution protocol can allow new sensor nodes to be added, deter code capture, and cope with the situations when base stations are either online or offline. Intrusion can be presented if the source of an attack can be trace.

In other studies, Yang, X., et al (2009) designed a hyperbolic position boundary algorithm to localize the origin of an attack signal within a vehicular communication network. The algorithm makes use of received signal strength reports for locating the source of attack signals without the knowledge of the power level of the station that is transmitting packets. Another area that attracted the attention of researchers is capture node. Conti (2011) demonstrated that node mobility together with local node cooperation can be leveraged to design secure routing protocols that detect node capture attacks. These researches and many others, not mentioned here, contributed in making intrusion into WLAN difficult and frustrating for hackers and attackers. A lot of researches were conducted on intrusion prevention on WLAN, as shown in the subsequent paragraphs.

In another study, Chenoweth el al (2010) in their study, explored wireless user vulnerabilities using Nmap scan to quantify the number of wireless users who were not ade-

quately protected. They conducted the study in university environment, and the results of the Nmap scans were used to determine the proportion of wireless users not using a firewall, the prevalence of malicious applications, and the proportion of users with open ports. Although the numbers of users found to be opened to vulnerabilities were small, yet the result indicated that security operates on voluntary user compliance. Their study contributed to technical automated security which this study claims is the concentration of many researches, it also indicated the absence of social aspect of vulnerabilities which their study and previous studies in the previous paragraphs were not able to address. Thus, these researches are pointing to the gap created in for the need of social system of security to complement the technical system.

This is necessary because the concern on security is more on hardware and software, forgetting the most important aspect of the security – the wetware, or the user. As a result of sophistication in in automated security systems, hackers are shifting their strategy to user vulnerabilities. Hackers, through social engineering, lure the user to give out information or act the way the determined attacker wants. Instead of the hacker spending time trying to crack a wireless system, all the hacker can do is to proxy the user to do that for him through clicking a link, or giving out certain information that will lead to the attacker's motive. Michael (2007) asserts that many security countermeasures can be automated through security technology by making them mandatory for users.

Michael (2007) in: Ong et al (2007) reports that there are significant reasons why automation in-and-of-itself cannot alone solve the problem. Despite the provision of the automation system of security, Sherif et al (2003) assert that there are cases where users must be responsible for the security of their systems. The case of social system of attacks through SE is demanding user involvement. Thomas (2013) asserts that SE is the hardest

form of attacks to defend because it cannot be defended with hardware or software. A successful defense will require both the technical and the social system to integrate.

2.7.2 The non-technical approach to security implementation

Similarly, different approaches to the implementation of security were proposed. Kruger (2006) argues that security can only be successful where both technical and procedural methods are put together. He further stated that "the implementation of effective security control depends on the creation of a security positive environment, where everyone understands and engage in the behaviors that are expected of them." Although the methods used to achieve this by Kruger (2006) is based on security procedures, the current research went beyond that to ensure practical user behaviors are established in the work place. This is in line with the suggestion of Valentine (2006), that an active team-work for security should be established across the organizational strata, because security is an ever-evolving field with new threats, techniques and philosophies emerging every day. This is also similar to the work of Von (2004) that attempts to move security away from policy based to culture based implementation. This is supported by Kerry-Lynn (2006) who argues that to install information security culture in any organization, security must be second daily activities among employees.

Similarly, Beach (1993) states that although corporate culture is supposed to direct employees attitudes, towards security, however the contrary is the case. This results to various security abuses. The implication of the views of Beach (1993) is the calling up of a system of security that embraces user culture in the workplace into a model that blends organizational culture with employees' culture.

This is indeed one aspect of the concern of the current research. Helen et al (1996) discovered that participatory approach to security is significant in supporting the technical

aspect of security that is indicating weaknesses due to constant reported cases of threats and attacks. This is further supported by Deloitte et al (2005); Posthumus, et al (2004); and Von Solms (2004), who stressed that the non-technical, human elements of security suffer neglect at the expense of the automated, encryption methods of security. *Other studies that supported complementary solutions to automated system of security, are those of Audit Commisstion (1994); Chidley (1995), and Gartner (1995), all suggested for a social aspect of security as complementary to the technical system.*

2.7.3 Procedural and User-Centred control measures

Organizations are making tens of thousands electronic activities ranging from clicking of mouse to browsing and communications over the networks, and as John (2003) assessed, if one slip or wrong doing in the series of activities is made and committed by single user, then the whole system is said to be in compromise to confidentiality, integrity and availability of information and network resources. This is also collaborated by Czernowalow (2005) who claimed that a single case of user security abuse can cost more thatn the expensive security system.

There are quite number of studies that attempt to focus attention of network and information security on the user. Jeffery et al (2005) developed an end-user security taxonomy, which maps technical knowledge with user behavior to motivate security attitudes. The test on the taxonomy revealed that a user equipped with the technical knowhow on security coupled with desirable attitudes to security, will have intrinsic motivation to apply and comply with security policies. Fin et al (2009) developed an IS model that fit in a socio-technical system where technology, users, and managerial strategies play a role in the provision of effective security to network and the information system. Da Veiga et al (2009)

suggested user-focused security implementations for successful security measures to be realized.

Similarly, Clifford (2006) suggested that organizations should embark on more user-centred security training. Against this background, Valentine (2006) suggested that organizations should develop security awareness that include seminars, online courses, videos, and "Pre-packaged Awareness Programme." Valentine (2006) further state that as a result of the increasing changes in styles of attacks that are becoming more sophisticated, philosophical and user-centred, a more static and cross sectional form of security should be established. However, Deloittee et al (2005) found that nearly 45% of organizations worldwide, do not consider security awareness of any significance in network security.

This has supported the lukewarm attitude organizations are given to security thereby allowing more threats and vulnerabilities through the user. However, in an attempt to provide a form of structure or model for incorporating security culture in organization, Kerry-Lynn et al (2009) proposed two models. The first model, known as the conscious competence learning model was developed to provide stage by stage security knowledge acquisition by users; and the second model known as knowledge creation model, describes how organization can create security knowledge and disseminate it to users across the organization.

Although the constructs of the two models are useful in the construction of the model of the current study, yet the models fail to show under the platform the dissemination of knowledge should be implemented. This gap is part of what the current research is addressing. The following diagrams show the two models with their respective constructs.

Figure 12: Model of security knowledge creation in Users

	Tacit knowledge _To_	Explicit knowledge
Tacit knowledge	Socialization	Externalization
Explicit knowledge	Internalization	Combination
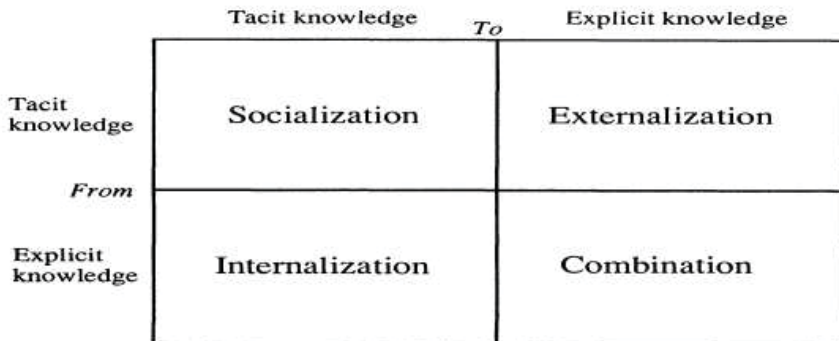
Source: Ikujiro, N. (1994) *Dynamic nature of organizational knowledge creation*

Kerry-Lynn el at (2009) argue that by diffusing this model into security practice, the user in the work place shall be equipped to the stage of recognizing and fighting threats and attacks. While this model shows how security knowledge is created and disseminated among employees, it does not provide the stages and process of doing that. This limitation is addressed by Schein (1994), in the conscious competence learning model. Kerry-Lynn et al (2009), adopted the Schein's model and came up with a model known as MISSTEV (model for information security shared tacit exposed values). The model (**figure 2.12**) is shown in Appendix I.

Kerry-Lynn et al (2009) argue that the MISSTEV model is supposed to provide the necessary skills and competencies in security to users and at the same time it is live security system that inculcates daily security practice among employees.

Another model that addressed user behaviour and embedment of security culture in the organization is that of Eloff et al (2009). They proposed ISCF (information security culture framework) which organizations can use to implement information security components that would influence users to develop, comply, and apply security culture appropriate

for protecting the assets of the organization. The **Figure 2.13** depicts the ISCT model and is shown in Appendix I.

Akin to the previous model, is PDCA a model proposed by Coles-Kem et al (2010). They used Theory of Crime Prevention to propose a Plan-Do-Check-Act model that can enhance information security management design. The model focuses on how users can be monitored security wise in such a way that user threats can be controlled through an ISMS cycle. This coincide with the model of the current study in which users activities' for security collaborations can easily be seen and monitored. This is possible through the posts, comments, likes, and sharing a user made on the social networking platform. The model proposed by Coles-Kem et al (2010), is depicted in the figure 13 below.

Figure 13: PDCA Model
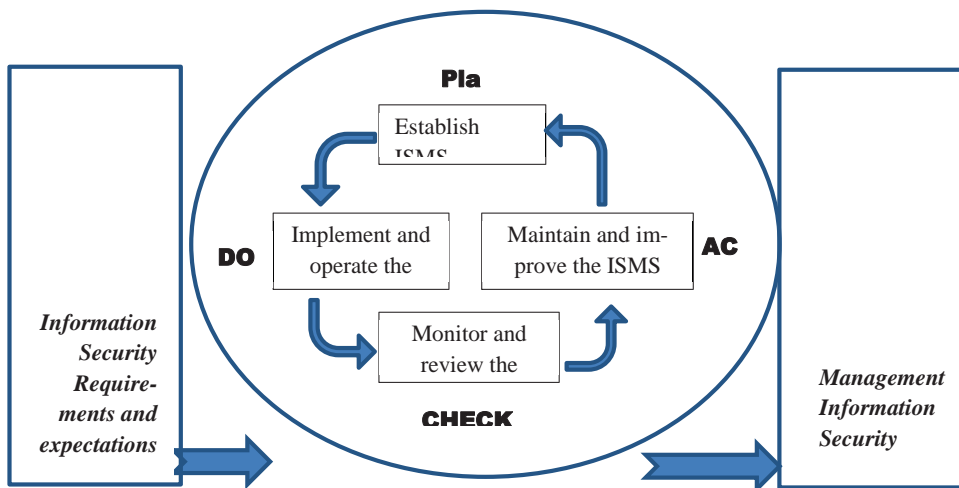
Source: Coles-Kemp (2010): *Insider Threat and Information Security Management*

The model has contributed to the understanding of security implementation control, but it does not differ significantly with the previous models that focus on the same frame-

work with this model. The current research wish to make security control more of user centred than management centred.

Similarly, John (2003) proposed user security behaviour model, which aims at improving user security behaviour through awareness and conformity. The model identifies two components that are significant in enhancing user security behaviour: the first component is user understands security roles and responsibilities; and second is the user's ability to conform to the expected security behavior (roles and responsibilities). The model is depicted in the following figure.

Figure 14: User security behavior improvement model
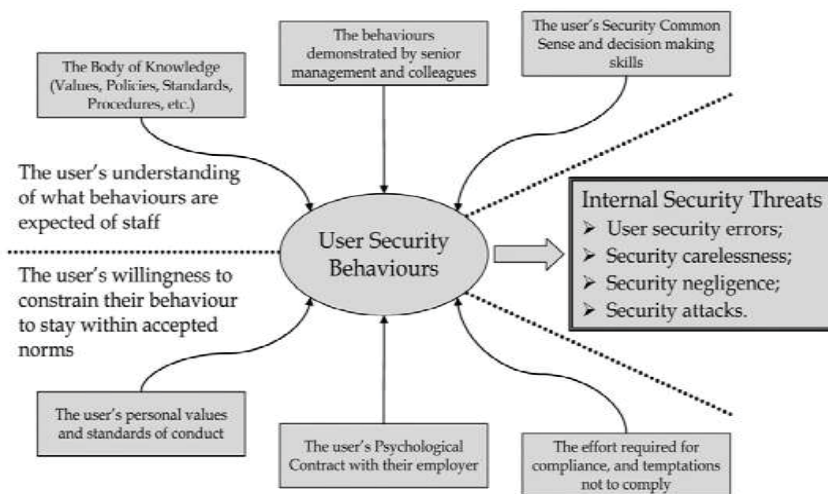
Source: John (2003): *User security behaviour improvement model*

The model in figure 14 is similar to the previous models that emphasize user training and compliance. It differs with the current research that aims at collaborating users to become proactive to the current threats and attacks through SE. The previous model has

contributed to an understanding of how various factors can converge to establish the desired security behaviour.

While this framework recognized the need for user involvement in securing the assets of the organization, yet it fail to address the procedure of how the established security culture can be applied in such a way that responsibility, commitment and transparency in security conduct can be made obvious and observable. This limitation is part of what the current research had addressed.

Other studies have attempted to establish security culture in such a way that compliance is integrated in user attitudes to security. Steven et al (2009) established that by addressing some variables in security compliance, the right culture to security can be developed among users. They suggested that through appropriate training and user commitment to security, the right security culture could be developed. **Table 1** depicted the stages in attaining the security culture.

Table 1: Levels of Security compliance: *Source: Steven et al (2009)*

Compliance	**Culture**	***The ideal state, in which security is implicitly part of the user's natural behaviour.***
	Commitment	*Security is not a natural part of behaviour, but if provided with appropriate guidance/leadership then users accept the need for it and make an associated effort.*
	Obedience	*Users may not buy into the principles, but can be made to comply via appropriate authority (i.e. implying a greater level of enforcement than simply providing guidance).*
	Awareness	*Users are aware of their role in information security, but are not necessarily fully complying with the associated practices or behaviour as yet.*

Non-Compliance	Ignorance	*Users remain unaware of security issues and so may introduce inadvertent adverse effects.*
	Apathy	*Users are aware of their role in protecting information assets, but are not motivated to adhere to good information security practices.*
	Resistance	*Users passively work against security, opposing those practices they do not agree with*
	Disobedience	*Users actively work against security, with insider abusers intentionally breaking the rules and circumventing controls.*

In another effort to involve users to participates in security in such a way that users have the ownership of security affairs in the organization, Helen (1996) proposed the Orion Strategy, in which users and the management come together to plan, decide and implement security affairs. The major goal of the approach was to marry users with security skills thereby integrating security culture into users and the management. While this approach is heading towards the direction of the current research in bring users to collaborate on security, yet it differs with the current study in terms of real-time application of the security measures. While the previous approach is informative and bureaucratic, the current study approaches security on real-time countermeasures and sharing of security experiences among users. However, the model provides structure of user participatory approach to security, useful to the current research in planning the security modules.

While the importance of training and awareness framework for user security practice, has been emphasized by various authorities, and Steven et al (2009) assessed that formal classroom training is more quality assurance in terms of body of knowledge delivery as per security training is concerned on the employees. The results of their findings can be seen in figure, where security guide lines brochures has the least impact in teaching se-

curity attitudes among users. Although this study is not similar to the current research, but the approach to security has exposed the current research to the best methods to adopt while imparting the security body of knowledge to the participants.

Table 2: User attitudes towards data security

Instructional Method	Employees attitude towards mobile data security		
	Good	Variable	Poor
Formal Classroom Training	64%	29%	7%
Individual Training when issuing devices	28%	40%	32%
Written Guidelines	29%	38%	33%
Users figure it out for themselves	16%	31%	53%

Source: Steven et al (2009). *User Acceptance of IT Security.*

In the effort to equip the user with the knowledge necessary for confronting the ever escalating threats to information and network resources, Daniel et al (2013) proposed a web-based security knowledge sharing portal, which aimed at bringing users to collaborate on the platform of knowledge sharing. The participants of the study were introduced to the functionalities and implementation of the model that mainly focus on ontology of sharing security knowledge; and users can contribute to the reservoir of knowledge, edit and share the knowledge. The model is said to be similar with the current research in structure, but differs in terms of platform of implementation, type of security knowledge to share, and motivation for the collaboration.

The issue of security cannot be confronted effectively without a good knowledge of user behaviour and attitudes towards security. In view of this, Jeffery, et al (2004) conduct-

ed a study on 1167 users on user security related behaviours and found that user behaviours are classified according to six categories mapped on two dimensional matrix of expertise and intentionality. The taxonomy indicates that any form of user behaviour falls in any of the six categories. Although the current research differs with the previous research in terms of user confrontation to security, yet the taxonomy of the previous research has exposed the current research to the understanding of training needs in each category appropriate for construction the security training module for the participants of the current research.

Another research that is closely related to previous research is that of Fin et al (2009), who developed system dynamics model that classify the interconnectivity and interdependency of security controls, for managerial control of security system. Both Fin et al (2009); and Jeffery et al (2004) attempt to address the knowhow of security controls, but the former is focusing on end user controls and the latter is focusing on managerial strategic security control. However, the findings of Fin et al (2009) supported the justification for the current research, in which their findings revealed that enterprises failed to adopt holistic view to security; rather than making security proactive through equal attention to non-technical issues, enterprises security systems were reactive, technical and addressing the symptoms instead of the root cause.

The managerial and procedural aspects of approaching security also draw attention of scholars in finding solution to non-technical issues of security, RUsecure (2002) affirmed that handling security issues through policy is only half the equation, users must know how to match theory with practice. This is supported by Rossouw et al (2004) who suggested a framework on how policies and procedures should be effectively and logically presented to users until the desired security culture is achieved. This can be achieved

through regular training supported with practical applications. This is similar to the features of the model of the current research. Another model that address user security issues at managerial level is that of Kritzinger et al (2006). In the model, the authors identified some levels on interrelated relationships that management could use to provide an effective magerial control of information security. However their model does not differ with previous models that either address security policies or implementation of security procedures, which users might abuse and refuse to implement. Their model is depicted in **figure 2.16.** It is shown in Appendix I.

The model in figure 2.16 looks hierarchical and in today's digitalized, automated, and paperless organizations, hierarchical system of information dissemination and awareness is unfit. Selznick (2008) assets that the nature of security requires flat platform that can easily disseminate information so that appropriate decision is taken without restrictions to protocols and routes processing. Against this, Patricia (2008) developed Tactical governance for security model, in which security system should be have holistic approach - administratively, integrating users with awareness in various elements of security and use of cohesion strategy to achieve good practice and compliance. The model differs with previous models by bringing in legal requirements in the security system. The model in figure 2.17 was able to outlined security approach from ethical and managerial actions, yet it is similar with previous models and frameworks in terms of their focus on security assessment and knowledge awareness. The current research goes beyond this with real-live user participation in security issues. *The TGS model is in Appendix one as figure 2.17.*

While previous researches focus on procedural and user security issues, some studies approached the issues of security on both technical and non-technical perspectives. Dhillon et al (2001) assessed organizational approaches to security and found that soci-

otechnical approach to security was not yet embraced as means of confronting vulnerabilities and attacks. In support to these findings, Sara et al (2009) proposed macro ergonomic approach in understanding security as a sociotechnical system, which describes how human and organizational factors may contribute to the presence of vulnerabilities in computer information security. A related study to this one is that of Carl (2009), which focus on applying the appropriate tools to achieve a balance between the technical controls and procedures with specific attention to human factors. The issue of sociotechnical approach to security is also supported by Jones et al (2008) who argued that despite the improvement in technical controls, through encryption, access control, minimum privilege, monitoring, auditing and reporting, it is essential to have a balance between the technical and non-technical controls, for a holistic approach to security. The previous studies fit with the current study in approach to security but differ in the implementation of countermeasures. However, they have provided an understanding to the current study of the contextual requirements appropriate for settings in the current study.

Kenneth et al (2009) developed an information security policy process model, which is structured as policy development cycle. The model has presented a structured pattern of handling security policy in such a way that security issues are confronted within the policy framework. However, the appealing feature of the model that attracted the attention of the current research is the structure would be useful to reflect social engineering threats in an iterative process for user identification and facilitation in the social learning process of the model.

The model does not differ from the previous model that emphasized on sound and clear security policy. The success of any security implementation depends of articulated security policy, yet the current user disposition and enlightenment on the use of BYOD

require a policy system that is made up of the people, by the people and for the people. The structural pattern of the previous model could be reviewed to introduce such a system, which the current research is similar to such system. The information security process model is depicted in **Figure 2.18 in Appendix I.**

While the policy process model is independent of users and authoritative, the content process model developed by Eirik et al (2010) is democratic – involving users for security attitudes transformation through dialogue, participation and collective reflection. The model is depicted in **Figure 2.19**, in Appendix I

The model in figure 2.19 used an experimental study with quantitative and qualitative methods in collecting and analyzing data. The quantitative methods aimed to find out whether the intervention had any effect on awareness and security behaviour; the qualitative method explained the basis of the change in behaviour. The result of the quantitative analysis revealed that the experimental group improved significantly in their security behaviour and they were willing and enthusiastic to individually contribute to the security system of the organization; while at the same time the control group did not show such change of attitude, and thus remained as they were from the beginning of the study. The results of the qualitative analysis showed that group participation was the main cause for the change of behaviour from security laissez-faire to security enthusiastic.

This study is similar with the current research in approach but differs in implementation of the acquired security knowledge. The previous study was able to found that group participation in security affairs is powerful in confronting threats and attacks, and the current study focus on how the group can collectively utilize their security knowledge and attitudes to identify and prevent threats and attacks they were exposed to. Other studies attempt to focus on user and compliance to security policies.

2.8   Security Policy Compliance and User Awareness

In the attempt to improve security, organizations embark on drafting WLAN policy imposing restrictions - don'ts and does. The security policies are aimed at educating and enlightening the user on the dangers and risks associated with behaviours that exploit or turn into vulnerabilities to the WLAN. Everett (2010) asserts that any form of security policy falls under any of the followings domains: promotional policy (advertising security awareness and associated risks); enforcing policy (sanctioning the user and disciplinary measures on violations); or informational policy (educating, training, and enlightening the user). In spite of the variations in the security policy, security breaches coming from people inside an organization are bigger than all other sources combined together .

In his study on information system user security, James (2012) developed a structured model of the user knowing-doing gap. The model examines the role of organizational narcissism and its effect on user attitudes towards following the reorganization's information security policies and procedures. Using the theory of planned behaviour, James (2012) was able to explain how narcissism and user attitude towards security should be changed through training efforts. Two of the hypotheses postulated by the study are: users who perceive a higher vulnerability to the threat to their information systems have a more positive attitude towards observing security precautions; and users who perceive a greater locus of control have a greater perceived behavioral control. The result revealed that perceived vulnerability of the organizational information system is significant in affecting attitude towards the intended behaviour of complying with the organizational information security policies. James (2012) concluded that if the workforce has a clearer concept of the damage the organization might sustain in the event of an information security compromise,

there should be an improvement in their attitude following security policies. He also added that user should be in control and responsible for the security of the information assets, by being the first line of defense. This study is supporting the approach of this current study that approaches WLAN security from the social system of the user, for the user, and by the user.

The provision of security policies is not adequate in protecting the network through user breaches. Pettier (2001) suggested that security policies should be written in such format that SE and related topics are well defined and elaborated. While, Grey (2008) lamented that security policies should only be made available to the employees through the organization's intranet. Contos (2006) argues that security policy is a way of giving away security measures by exposing the organizations' security strategies. John (2003) did not see it that way, he observed that instead of security policy to elicit an active security behaviour in users, it instead turn users into sleep and passive to security practice.

However, even if security policies are well defined and an efficient of compliance is adopted, there is the issue of compliance. Various empirical studies proposed the issue of compliance. Kirsch et al (2007) suggested that employees should be mandated to comply with information security and called his concept as mandatories. This differs with Pahnila et al (2007) who argued that enabling conditions and user education are significant in promoting compliance. Similarly, Rogers (1983) argued that compliance is best achieved where user understands the threats and knows how to cope with the identified threats as they occur or image. However, Myyry et al (2009) see compliance from the perspectives of moral discipline. If users are cultured o moral basis to protect the assets of their organization, then compliance can be achieved. This is in consonance with.

While the importance of security policies is recognized by organizations, yet organizations fail to have a systematic system of dissemination and implementation of security policies. The findings of Heather et al (2003) revealed that dissemination of policies is great hurdles to organizations. Heather et al (2003) reported in Siponen (2000) that despite the importance of security awareness, organizations are not given it the priority it deserves. Heather et al (2003) further found that organizations promulgate security policies only because it is common practice, and fail to use it as a system of user responsibility in the security system. Heather et al (2003) concluded that specific system of dissemination and implementation of security policy is lacking.

Although the current research is not focusing on security policy, but its relation to its dissemination and implementation has directly or indirectly support the current research. However, Eloff et al (2005) argue that implementation and dissemination of security policy is costly and complex cutting across the organizational strata. They suggested that for security to be effective and successful, all aspects regarding security must be addressed in a well-structured and holistic manner. Compliance to security policy must be matched with training. In view of this other studies focus on how the user should be trained to face the emerging SE threats and attacks facing network and information resources.

2.9   Training the User

The technical system of identifying intrusion into WLAN should be complemented by the non-technical, user-based system. Some studies have attempted to establish that user is able to identify socially engineering threats and phishing from all its features and styles. For example, Furnell (2007) studied 179 participates who were exposed to 20 latent phishing messages, and found that users failed to distinguish between genuine and fraudulent messages. In the attempt to extend Furnell's research,   Sheng et al (2007) confirmed the

effect of exposure to phishing cues to have some impact in identifying phishing websites. In their study participants were exposed to 20 websites without prior exposure to phishing techniques. In the middle of the presentation, the participants had a break; and during the break the group divided into three groups: one group played anti-phishing game, the second group read anti-phishing tutorials, and the other group did a different thing unrelated to phishing. The result revealed that the game group performed remarkably well in identifying phishing so also the reading group, but not as much as the game group. The control group remained the same. The previous studies are similar in approach to the current study but differ in context and platform for implementation. They have contributed to an understanding of how users should be trained to understand and identify phishing threats and attacks.

In a related study, Wright et al (2010) found that knowledge base, experience and personality traits account for the reason why users are able to detect phishing camouflage. Their work attempted to phished 446 subjects for valuable information. The result revealed that users with any of the three mentioned elements appeared suspicious to the phishing context. The current study aimed at developing all the three elements through the proposed model through social learning on the social network platform of the model.

However, this contradict the work of Jakobsson et al (2006) who have found that 11 percent of users still went ahead to read spoofed emails, click a link, and enter their login details. This also collaborated with the study of Wu et al (2006) who found that users disregard taking action on toolbar anomalies signs they were exposed to, under the pretext that security is not their concern. Furthermore, Kerry-Lynn and Seteven (2009) affirm that "one of the most prevalent problems facing the successful implementation of information security practices and procedures is the human element."

Kumaraguru et al (2010) developed an e-mail-based and anti-Phishing education system called "PhishGuru" and an online game called "Anti-Phishing" that teach users how to use cues in URLs to avoid falling for Phishing attacks. In the implementation of their teaching-learning model, they used instructional principles in the learning of science. The method proved effective in teaching users to identify fraudulent websites and emails. As a result of the similarity of this study with the current research and the relevance of the teaching learning system to the current research, some details review of the PhishGuru research is carried out as follows:

PhishGuru *Study design:* the participants were divided into four groups: the embedded, the non-embedded, the suspicious, and the control groups. The embedded received simulated phishing email and the subjects were exposed to an intervention (awareness and protection) while clicking a link. The same applied to non-embedded group, but the difference is an email instead of a link. The suspicious group received an email from a friend with a phishing warning, but without support for protection. The control group received the same email without phishing alert or support for protection. Figure 2.20 is shown in Appendix I. It depicts the comic strip intervention design, teaching Johnny not fall for Phishing.

The model was an experimental type and the results of their study revealed that embedded training is more effective in training users to distinguish between genuine and phishing email messages. The results further discovered that participants in the embedded group were able to transfer knowledge from one situation to another as compared to the other groups who did not show this capability. The suspicious group was no better than the control group. Against this background, Kumaraguru et al (2010) suggested that phishing

awareness is not enough without training followed with practice, to identify fraudulent events and counteract.

With the Anti-phishing study, Kumaruguru (2010) designed anti-phishing lab study in which 28 participants were randomly assigned to either tutorial condition or game condition. The tutorial group studied 17 printed pages of anti-phishing, and the game group played a game with the same materials given to the tutorial group. The study measured the participants' knowledge acquisition by examining their performance results on false positive, false negatives, as well as identification of correct web sites before and after the intervention. The results revealed that both groups performed well but the game group exceeded in the performance. This therefore signifies the desirability of combining both methods if effective learning outcome can be achieved. In view of this, Sherley (2010) proposed social responsibility model to train users in the identification and prevention of various SE threats they may encounter. **Figure 2.21** appeared in Appendix I and is titled: Social responsibility to combat malware

Herberg et al (2010) proposed a shared responsibility model in figure and assert that to combat social engineering malware, interactions between end-users, government, laws and security policies should be bonded; and suggested that deviation to compliance to security policies should be penalized. They also recommended on going awareness training with test and evaluation for success. Similarly, Beziodemjpit et al (2010) proposed periodically applied user-friendly aid, named SEADM. It was aimed at assisting users and IT system administrator in the daily awareness of SE threats, thereby providing level of protection. Their model is depicted in figure, in the authentication section of the literature review.

Still in the area of security awareness, various authors have researched into the area and found partial or complete absence of security awareness among users. For example, Yacine et al (2008) explore factors affecting information security awareness and one of their findings revealed that security awareness is absent even in higher educational institution. Against this background, they suggested that users should be regularly trained, and be made to understand that they are accountable for any security misconduct. They also recommend wider reach of user security awareness among users in organizations. There recommendations tally with those of Puhakainen (2006) who suggested training, campaigning, reward and punishment; and each can be applied independently, without concurrent applications of the three measures. However, while these authors have contributed to the approach of tackling user security indifference, yet the actualizations of their contributions need a system that is on real live social collaboration on user security issues; and this is what the proposed model of the current research aimed to achieve.

Similarly, In figure Kritzinger and Von (2010) proposed E-awareness model (E-AM) in which home users acquire seucrity knowledge and were forced to apply the acquired knowledge for security pracices. While previous model emphasize educationa and training, the E-AM added compulsary application of the acquired knowledge. The model also differs with the current study that propose collective participation on security on social networking platform. However, the model has contributed the understanding of the system of making the user acquired security knowledge, which is revelevant to the current study. In **Figure 15**, Kritzinger describe the process of user knowledge absorbtion.

Figure 15: User awareness
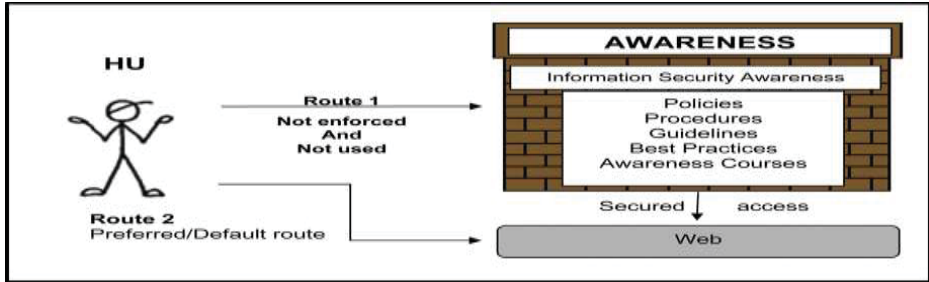
Source: Kritzinger and Von (2010)

The model describes the procedures the user is conditioned to understand absorb and acquire the security awareness and is held responsible with coercion to observe and apply the security conducts before surfing the web. While sanctions and enforcement may lead to noncompliance, yet with proper human authentication system, compliance to security issues could be observed.

2.10 Non-Automated system of Authentication

Social system of Authentication provides means of controlling and maintaining the CIA triad of security. Tim (2004) established three steps process of identification, authentication, and authorization (IAA). Tim (2004) further related the process to questions format as thus: Identification asks the question, "do I know you?" Authentication asks the question, "are you who you said you are?" And authorization asks, "are you supposed to be here?" Tim (2004) concluded by suggesting that to evade and minimizes SE attacks, organizations must maintain constant vigilance through implementation of effective awareness programme that keep security from SE at the forefront of its employees' minds.

2.10.1 Human factor Authentication

The access to the network through user by means of social engineering is both through indirect route (online) or direct route (offline). The user should be able to authenticate both requests that confront him/her. The technology-based authentication tools could work more effectively if users complement the process by doing the right thing in their browsing sessions. However, in most cases fail the system and compromise the network. Herzberg (2009) found that users exposed to browser health indicators, ignore SSL/TLS validation to confirm URL authenticity, and straight ahead enter their login credentials. In a similar study, Egelman et al (2008) found that 58 out of 60 participants ignore the warnings signs sent to them, and yet send their credentials despite the appearance of the phishing warnings

2.10.2 Password

The most commonly used authentication means to gain access to network and network resources is the password. It is like a key to a padlock; the easier it is to possess the key the easier it takes to unlock the padlock. As Gunter (2013) observed, almost all security mechanisms used by any organizations can be compromised or thwarted by poor passwords. This is collaborated by the work of Florencio et al (2007) on users' password habits, in which their study found that users reuse passwords, users were careless on passwords formation, and users forget passwords easily thereby making them to use easy to remember passwords.

The use of easy to remember passwords supported the claim of Grunter (2013). Likewise as Ka-Ping et al (2006) pointed out the strength of password depends on its difficulty to guess. They asserted that simple and easy to remember passwords are vulnerable to

dictionary attacks. Ka-Ping (2006) developed tools that helped user to achieve convenience and security in login sessions. Their password hashing tools help users to manage multiple accounts with a single password turning it into different passwords with memory convenience and security. Hackers use various means to get password from users so as to get legitimate access to the network and its resources.

One of the most commonly used means by hackers to obtain user's password is the password login form. As can be seen in the following figure, Ka-Ping et al (2006) found that users are fooled into filling online form with their surname and passwords. This is done through corrupting or spoofing the web browser. Although passpet was able to help users from phishing, but Karlof (2012) observed that passpet is vulnerable to dynamic pharming, which is a hijacker of DNS and send the victim's browser malicious JavaScript as exploit.

In a BBC News: "At least 38 million accounts breached." Early October 2013, Adobe confirmed data breached where the username and passwords of its millions customers were stolen and their accounts compromised. One of the spokesmen of Adobe and other commentators attributed the incidence to poor password habits among customers. This indicates that intrusion into corporate or local wireless resources through user credentials is common phenomenon among electronic users.

2.11 Workplace Structural Interactions

Whenever people meet to work together for the achievement of certain common goals, they are directly or indirectly engaged in a social network. Southworth et al (1998) define formal ties as that relationship among members of a group that is based on defined and specific roles and functions; whereas the informal group is based on voluntary cooperation that emerge among the members and not from the formal structure. The various

author who attempted to distinguish between formal and informal organization, notably Baker (1999); Mintzberg (1983); and Watson et al (2003), have all agreed that formal structures are created by deliberate plan and recognized standards; and Hartman et al (1990) assert that the informal networks are formed as a result of social interactions among actors.

Behavioral interactions in organizations are affected by structural patterns. Selznick (1948) argued that employees often deviate from the formal settings because of its inherent nature of depersonalization. This is further elaborated and established by Noorderhaven (1992) who asserted that irrespective of penalties enforced for noncompliance to established procedures, employees prefer informal relationships. The role of informal ties is necessary for the success of any objective. Olaf (2008) examined the coexistence of formal and informal networks in organization and found that surprisingly, top management disregard their formal contacts, to some extent, and work with informal actors for strategic issues. He also found that informal ties are formed and maintained at the vertical level rather than at the horizontal level. This shows that a node at the lowest level of the hierarchy can have informal ties with a node at the highest level of the hierarchy. This is a desirable connection for the implementation of a plan. This study has contributed to the understanding of the interdependency between formal and informal ties, which is one of the tools for implementation in the current study.

In his study of Network structure and team performance, Grund (2000) asserts that network density and intense interactions between individuals increase team performance. This was the findings of his study with 23 soccer teams where mixed-effects modeling were implemented for 76 repeated observations on the interactions network and performance of the teams. In similar study, Prasad and David (2013) conducted a meta-analysis

of 37 studies of workforce teams in natural contexts and found that team task performance and viability are higher where teams are configured with densely interpersonal ties.

In their studies of group exchange structure and its effect on work outcome in virtual teams, Claudia, Williams, Christine, Mark, Jonathan and Anson (2006) collected data on electronic communication from 50 virtual teams made up of 233 business studies students and the result revealed four main structures: unified generalized with high exchange relationships among group members and high information sharing and cooperation; unified generalized with isolates – indicating high exchange among members and negative exchange among some isolated members; unified balanced – indicating low-quality exchange relationships among members and low trust and concern for others; and unified balanced with isolates – indicating low-quality exchange among most members and negative exchange with some isolated members. However, DiMicco (2008) found that working within the same department feel the need to connect to each other, but find connections with co-workers in other departments more valuable.

In another study conducted on inter group relations and group performance, Jay (2013) examined 80 individuals in 4 groups' experiment that manipulated the extent to which the groups experienced success or failure in an intellective task before facing isolation. The results revealed that intergroup cooperation is favorable for intellective tasks. In their studies of knowledge intensive teams, Siyuan and Jonathan (2013), hypothesized based on small group research and network theory that in a highly centralized critical knowledge structure, everyone shares critical knowledge with a single person on the team. From the data they analyzed of 177 teams in a multinational organization, the result indicated that centralized critical knowledge structures have negative relation to executive-rated team performance.

Similarly, Olaf (2012) collected data from two German multinational organizations to test the predictions regarding the coexistence of formal organizational structure and informal networks. Using QAP and ANOVA to analyze the data, the results revealed that greater number of informal ties are built and maintained in a vertical rather than a horizontal direction.

The findings throw more light on the interdependency between formal structure and informal networks. However, organization is a social network itself and implementation of security measures can take style from the social network settings for a more collaborative efforts.

2.12 Social Network

Social network has been in our societies for centuries, but it has made no great impact in any time than the present time of e-of-things: e-marketing, e-learning, e-collaboration, e-health, and e-conference. Charles (2010) defines social networking as the process of connecting entities together based on their social bonds or ties. In a social network theory, Nooy et al (2005) describe social network as structure of ties or relationships. Charles (2010) added that social network consists up of actors (nodes or points) and ties (links or relationships). Thus individuals are nodes in the social network and their interaction established on a relationship that is linked or connected to social networking.

Social network cut across all spheres of individuals and organizational activities. In today's digital world, social network can be defined as a technology for collaborations, knowledge sharing, communication, participations, engagement, and interactions on social media of Facebook, Twitter, intranet, or other forms of online platforms. It is a technology that knit people together based on common interests, objectives, or purpose. Social network is revolutionizing the work place faster than any technology has done. Margaret (2006)

asserts that: In organizations, real power and energy is generated through relationships. The patterns of relationships and the capacities to form them are more important than tasks, functions, roles, and positions. Conscious or unconscious of this quote, many organisations are beginning to employ the use of social network for one purpose or another. However, haphazard use of social network will not yield the desired result without a structured, tested, and modeled pattern.

In their study on the adaptation of Social network in educational context, using TAM as their theoretical framework, Sacide et al (2009) came up with a model that addressed two of their hypotheses: (a) image acquisition will positively affect usefulness perception in social network environment, and (b) social factors will have a positive influence on social network usage. Their study accepted the two hypotheses and considered them relevant in social network adaptation in educational context. The social factors described in their study include many factors related with individuals and their social environments as in relationships with others, status in a system, feeling of belonging to a community with common interests and expectations. A study closely related to this is that of Robert (2011). Image acquisition in their study referred to publishing profile information, sharing, comments and other activities. *Their approach to the usage of social network for education is in line with this research, most especially the two hypotheses. Their proposed model, though in education, is relevant to the understanding of the conduct of this research as it inclines towards usage of social network for security issues.*

Social network provides an understanding and knowhow on group structure and interactions of the group. Wassermann et al (1994) defines social network as a mathematical technique for analyzing social relationships, patterns and the implications of the structural relationships. In their study of the application of social network theory to animal be-

haviour, Amelia et al (2009), video recorded the behaviour of elephant in group over two months period. Their findings revealed that social network is a powerful approach to the understanding of group dynamics. Although the current study is not aimed at understanding group dynamics, but the concept is useful to structure and pattern the participants of the study in groups based on the concept of social network.

In a similar study on the use of social network theory on entrepreneur's linkages development, Mastura el at (2009), proved that strong is important source of consultation at the initial stage of the project and as the matures to advanced stage, the weak tie played dominant role in the consultancy services. The implication of this study is that strong and weak ties can play supporting roles in achieving a goal or implementing a project. This is in line with the current study aimed at combining both ties to collaborate for security on the WLAN.

2.13 Social Networking on Facebook Platform

People and interactions are inseparable. John et al (2009) define social networking as ties and interactions between people which occur on web 2.o technologies or other forms of technologies, like telephone and mobile devices. They added that FB is gaining popularity among workers and this supports the findings of Skeels and Grudi (2008) that 37% of the work force use FB and 17% use it daily. However, some organizations ban the use of social network sites in the workplace. The reasons for this, as identified by John et al (2009) are: consuming employer's time resources; consuming organization's bandwidth; unguarded statements to colleagues and customers; and could be a channel for phishing attacks.

However, UTC (2007) suggested that permission to use network sites should be granted at break time, after all employees have right to their private life. In order to avoid

the cited concerns over the use of public network sites, some organizations prepare to have their own inter network. John et al (2009) identified some of the internal network sites as Blueshirt, People connect, and SelectMinds, Watercooler for HP and Bluepages for IBM. However, the popularity of the FB has rendered these internal network sites less enthusiastic to workers; and added that most of them have similar layout and functionalities like that of FB. In addition, Alessandro and Ralph (2006) asset that FB is of interest to researchers because: it is a mass social phenomenon; and it is a unique window of observations where true life data can be obtained. Similarly, Shi-Ming et al (2013) assert that FB has been the recognized as one of the most representative of social networking sites.

We are in the era of "Web 2.0", or "Social software," which Ractham et al (2010) describe as multi-channels platform for interactions and collaborations. This has pave way for knowledge creation, and dissemination of information. The society is transformed into virtual world, where an individual is now, as Turkle (1984) claim, transformed into a virtual-self that regenerate the physical self into a node on a network. The sense of belonging inherent in human nature is reinforced in social networking. Davies et al (1995) assert that, social networking bond members together and each one feel a sense of belonging as a result of reciprocal obligations common in the social network.

The increasing awareness of benefits and wider applications of social network technology has attracted the attention of individuals and organizations on the use and implementation of social media for collaborations. There are various authors whose researches found social media to be effective platform for teaching, learning, and implementations of projects. Among such authors are Arjan et al (2008); and Evans et al (2009), and recommended social media for knowledge creation, collaborations, feedback and sharing of resources. Similarly, Chien-Kuo and Buo-Han (2013) used FB club as a teaching platform to

97

develop product design, and found that: members without FB club were not able to engage in the discussions; the study demonstrated that members were having fun and learning become interested and enthusiastic to the members.

The use of Facebook as a social media and platform for education and learning has been examined by different authors; notably Peter et al (2012) evaluated the FB implementation within educational context for the purpose of creating a social constructivist learning environment for introductory course in MIS. They found the use of FB effective for creating such learning environments. Knowledge creation and learning on the platform of FB is best fit in the constructivist learning theory; which Kasemvilas et al (2009) describe as system of learning that engage learners into social interactions facilitated by collaborations and sharing of ideas and resources. Their contribution was able to propose pedagogy for teachings to use FB features with variety of learning style to promote knowledge creation and sharing. The study was able to identify FB as effective platform for the promotion of live interactions for knowledge exchange among participants.

The easiness of FB use made their participants to be enthusiastic in the learning process. This is supported by Ractham and Daniel (2011) who experimented on the use of FB for learning MIS, and found that learners found FB easier to adopt in the learning process because of its popularity and familiarity with most learners. They also found that learners leverage social networking with knowledge creation, discussions, and sharing learning experiences.

However, they cautioned that the use of GB depends on the instructor's ability to marry the learning contents with the appropriate and creative instructional materials. Moreover, Shih (2000) implemented blended approach combining peer assessment on Facebook with face to face interaction. The results revealed that Facebook enhance learning,

and that learners collaborated effectively thereby promoting trust among learners, improve communication, established active learning, and learning attitude. In another study, Terence et al (2009) developed a module called CommonGround, which is a Facebook platform to improve learners' communication skills and awareness. The results revealed that students were able to integrate their learning activities with Common Ground much easier than expected; and the students reported remarkable improvements in their social awareness knowledge.

Similarly, Rocael et al (2012) created an experience of doing e-Moderation of a learning process on Facebook. Their findings revealed that 77% of the participants indicated that social networks enhanced their learning process through sharing and scaffolding knowledge. On the aspect of information exchange, 62% of the participants indicated that FB participation is better than discussion groups, because of the availability of online resources.

2.13.1 Facebook a Platform for learning Social Engineering

For the purpose of this research, FB is the ideal media because it is a social learning platform that can enhance and enrich users' knowledge and skills on social engineering attacks that is common on social media, particularly the FB. There are many researches that confirmed how SE attacks were successful on the FB.

Among such studies are Boshmaf et al (2008) who used bot attack against Facebook users, influencing them to accept fake profile requests. In the first phase of their study, they sent over 5000 requests and 976 returned accepted. Again from the accepted numbers (976), they used the mutual friends' contact of this number and sent over 3000 requests, out of which over 2000 of the requests were accepted.

Facebook has become the weapon of choice by hackers to deliver malware that can damage an organization's network. A social engineering malware threat is highest in Facebook than in any social media. Facebook is increasingly becoming the harvesting ground for hackers and attackers. If there is a better social media for learning social engineering threats and attacks, then Facebook is the ideal media and platform for social learning on malware threats in social engineering.

Figure 16: describes the flow of information that could lead to the SE attacks
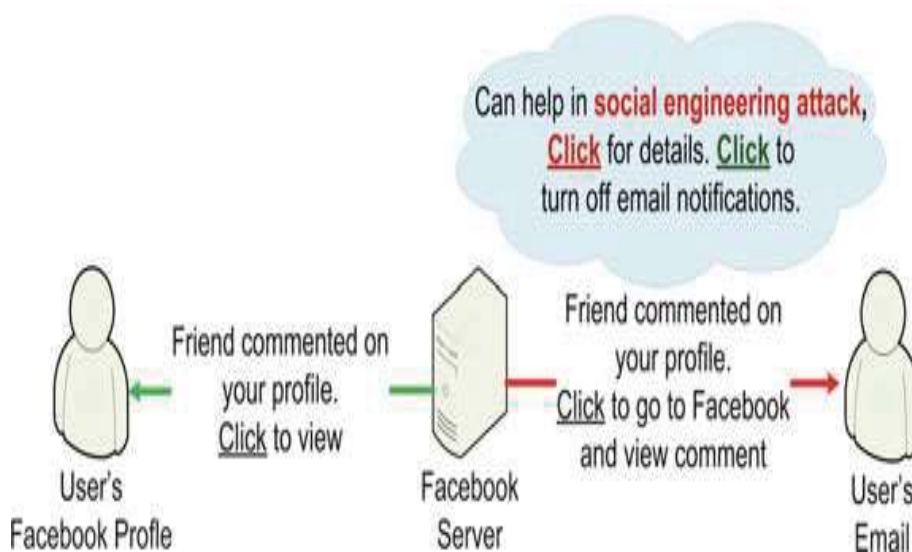
Source: Boshmaf et al (2013).

In a related study, Mahmood and Desmedt (2013) used spear phishing attack (with spoofed profiles) and sent 225 friends requests, and 90 returned accepted. In the second phase of their attack, they sent over 595 friends requests, and 370 returned accepted. The unusual thing that happened in their experiment was that the mutual friends of the already accepted friends, sent over 3000 requests.

Similarly, Yazan et al (2013) evaluate how cybercriminals use the online social network platforms like Facebook to infiltrate user privacy by the spread of botnets and malware. Their study confirmed the claim of this study that social media of Facebook is the ideal platform to engage users for the training, identification and prevention of SE threats and attacks on their networks. **Figure 17** depicts the visual description of the attacks of online social platforms with botnets.

Figure 17: visual description of the attacks
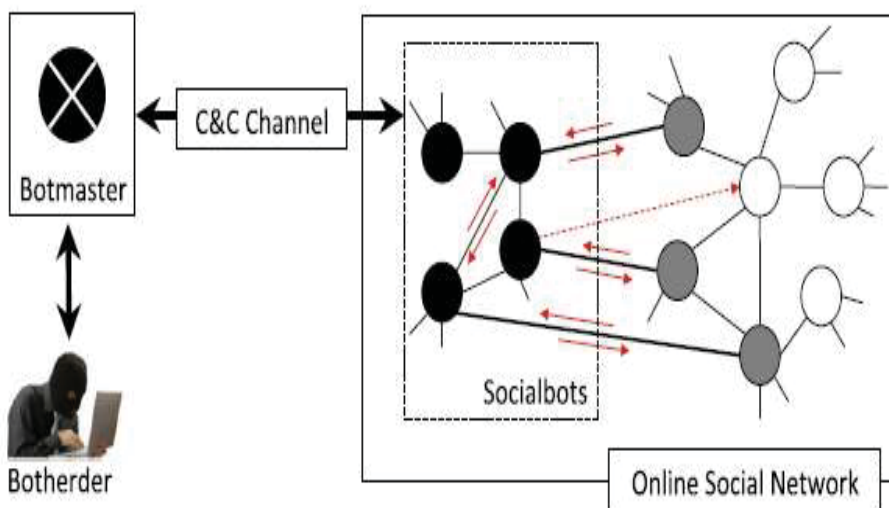
Source: Yazan et al (2013): Design and analysis of a social botnet

Yazan et al (2013) describe the process as thus: "*Socialbot Network (SbN). Each node in the OSN represents a user profile. The socialbots are marked in black. Infiltrated users are marked in gray. Edges between nodes represent social connections. The dashed arrow represents a connection request. The small arrows represent social interactions. The SbN can be part of an existing botnet, where each ''zombie'' machine is additionally infected by the socialbot malware that controls a fake user profile in the targeted OSN.*

2.13.2 Comment on Social platform

The free (online) English dictionary defines comment as a written note intended as an explanation, illustrations, or criticism of a passage in a book or other writing. In the Facebook, comment is not different from this definition. However, the comment made on the Facebook may be interpreted in different ways. The following figure depicts Shih's Facebook participants commenting on a subject matter.

Figure 18: Participants comments on Facebook

In another study, Terence et al (2009) developed a module called Common Ground, which is a Facebook platform to improve learners' communication skills and awareness. The results revealed that students were able to integrate their learning activities with CommonGround much easier than expected; and the students reported remarkable improvements in their social awareness knowledge. Similarly, Rocael et al (2012) created an experience of doing e-Moderation of a learning process on Facebook. Their findings revealed that 77% of the participants indicated that social networks enhanced their learning process through sharing and scaffolding knowledge. On the aspect of information exchange, 62%

of the participants indicated that FB participation is better than discussion groups, because of the availability of online resources.

2.13.3 Like – on social network platform

Liking is related to the way an individual is viewed or accepted in terms of his/her views and relations. Radostina (2013) conducted an experiment with 532 students grouped in 134 four-member teams. One of the prepositions of to the study was to confirm team members' sense of feeling known early on the team lifespan is positively associated with team members' perception of personal leaning in the team lifespan. The result shows that sense of feeling has strong impact on team member's outcome in interpersonal interactions, learning, and team performance. Motivating members to contribute more to the content of discussion is also acknowledged by Ru-Chu (2011) who state that: "For instance, when students receive "like" "👍 1 person" from others, they may be motivated and feel more confident."

Porterfiled et al (2011) assert that when user clicks the like bottom, the news feeds of the user's friend or group display such action, thereby keeping records of those who care. Dominic (2013) identifies the following reasons as clicking lie on Facebook: agreement with what is being said, sign of appreciation, one is associating himself with it. Also Glazer (2012) assessed that like is an indicator of degree of engagement among fans. Likewise the Facebook help indicated that the like button act as an expression of acknowledgement and care about a content. The commentators of Dominic's perception of "like", further comment as thus:

"I think people often use the "like" button to simply acknowledge that they saw the posting."
"I know the button LIKE as something u like and appreciate?"

Moreover, the Facebook help added that "like" on a content signify connection to that content and of course a positive one. Peter (2013) also sees "like" as a form of support for specific comment. Similarly, Chien-Kuo and Buo-Han (2013) found that "like" brings positive reinforcement to the uploader of content, thereby motivating the person to bring more of such contents. Moreover, Rocael et al (2012) evaluated like functionality and found that 92% of the respondents used this functionality on their Facebook learning interactions; and the authors interpreted this functionality to mean approval and meaningful participation. Thus, It can thus be seen that like is one of the Facebook functionalities that is related to transparency, and accountability. The proposed model of the current research aimed to integrate transparency in user security habit.

2.13.4 Groups in social network platform

Group is one of the features of FB that translate the 1970s theorization of social networking. Shih-Ming et al (2013) define the Facebook Gorup as exclusive platform formed by members with common interest; they generate discussions and share information exclusive to its members. Wang et el (2012) also define FB Group as a learning management system to share learning resources; and their study found FB Group to be appealing to students in the learning process. Similarly, Chu (2011) found that FB Group members ethically use online resources than non-Group members. Slavin (1995) found that the online group promotes meaningful discussions leading to problem solving tasks

2.13.5 The FB "wall" post

Wall post is the foremost and principal medium of interactions among members of FB (and groups). Yan et al (2013) found that members' posting on the wall is influenced by: quest for information, emotion, and community building, desire to turn the group live-

ly. Moreover, The Facebook wall is in consonance with the Theory of Social Influence, propounded by Kelman (1958), who argues that people's actions and thoughts are influenced by the group they attached to. He identified three levels of influence as Compliance, Internalization, and Identification. Venkatesh and David (2000) describe compliance as the expectation the group has on the individual to behave in agreement with the norms and conduct of behaviour acceptable to the group. While Dholakia et al (2004) describe Internalization as the adaptation or aligning one's conduct to the defined values by the group. Kelman (1958) describes identification as the attempt made by individual by compliance and internalization to establish and maintain his/her identity in the group. Selwyn (2009) conducted qualitative analysis of the FB "wall" activity of 909 undergraduate students in UK. Among the findings of the study include: use the FB to recapitulate their learning experiences and valuable means exchange information among peers, thereby established, thereby identifying their identity and satisfying the expectations of the group.

2.13.6 Sharing on the social network platform

Sharing is a way of making content available to as many contacts as possible. Chien-Kuo and Buo-Han (2013) assert that sharing enhances and promote learning. Rovai (1992) defines sharing as a mutual contribution to awareness, through disclosure of knowledge to varied number of people. He further describes sharing as group participation, intellectual progress, and gradual convergence, leading to awareness. Sharing experience is an integral part of user proactive in security.

It has been assessed by Vygostky (1978) that sharing contents enrich learners with new concepts and strategies. The model is closer to the current research, but differs in the lack of specification on how the security knowledge and awareness should be acquired, which the model of the current research has addressed. Their model is depicted below:

Figure 19: Sharing experience model
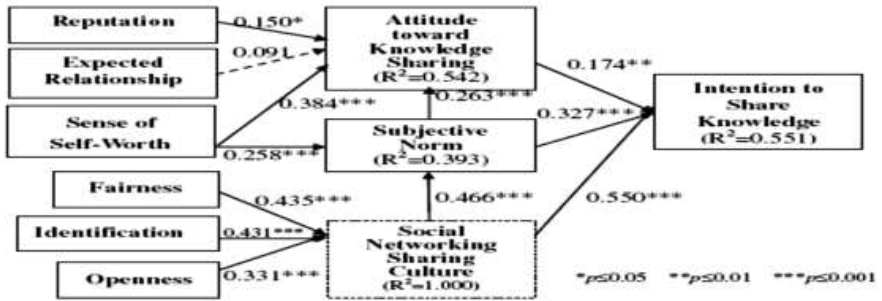
2.14 The Social networking approach

One opportunity inherent in Social Media (SM) is Social Learning (SL). Thomas et al (1998) asset that transfer of knowledge is best effective in SL situation. The few employees knowledgeable in security issues would impart that knowledge to those with low awareness and knowledge. Thomas et al (1998) identified four facilitating techniques in SL: conformity, obedience, reciprocity, and commitment. In the conformity facet, members attempt to meet to the expectations of the group interest to demonstrate belongings. Thomas et al (1998) suggested that group members that are not inconformity with each other should be isolated, and formed an interest group of their likes. This is in line with the approach of the current study by allowing informal ties from the formal ties of the organizational structure, the freedom to interact for security collaborations.

On the other hand, obedience, reciprocity, and commitment as promoted by Thomas et al (1998) imply contribution, liking, and commenting on issues of concern with the view of meeting these attributes. Thomas et al (1998) concluded by suggesting the grouping of employees across the strata of the organization if effective security awareness programme can be achieved. This again is in consonance with the current research of structuring the users into groups that facilitate interactions for security.

Moreover, Social networking is a form of online learning that has its root in the Constructivist and the social learning theories. The studies of Hrastinski (2009) and that of Woo and Rees (2007) have confirmed that both constructivist and social learning theories contribute to effective application of web-based learning that focus on collaboration and sharing of knowledge. This is supported by the work of Wang (2010) who asserts that web-based learning is ideal for learning system that promotes sharing of knowledge and resources. Moreover, Duffy and Jonassen (1992) assert the constructivist claim that there is no one right approach to the way to interpret the world we live; and as Stefan (2008) added, that the challenge of the teacher is not to transfer knowledge from his/her reservoir, but to devise means through which learners have the opportunity to interact, collaborate and share learning experience among themselves.

Sefan (2008) also state that many researchers agree that reservoir of knowledge is not limited to an individual (teacher) manipulation, but should spread across the continuum of minds for collaboration and sharing. In view of these arguments, the current research incorporated social networking (in a form of online) learning to approach the issues of security threats and attacks emerging from SE. This choice is supported by the claim of Sefan (2008) that online knowledge delivery is the more powerful and effective means of learning, collaboration and sharing of experience than any means ever known, thereby having positive effect on learner by retention and application of knowledge.

Kent et al (2003) assert that social networking is becoming critical for the growth, survival and prosperity of organizations. Such survivals include protection against threats and attacks on their networks and information resources. The various studies reviewed so far have indicated that security awareness training to users are on instructional traditional method of knowledge delivery, and non-focus on online platform as proposed by the cur-

rent research. If users should retain the knowledge exposed to them, apply the knowledge, and share their security encountered experiences, then the chosen approach made by the current research, is the appropriate and desirable. Various studies, though not in the field of user security, have all found this approach effective for the present purpose of the current research. For example, Fredericksen et al (2000) found that effectiveness of learning depends on learners' interactions, participations on the subject matter, and feedback process; which the social networking approach has provided. The findings of New Jersey Institute of Technology also confirmed the effectiveness of the social networking approach taken by the current research. The study was conducted by Hiltz et al (2000) and found that participants on collaborative group perform better than those on instructional group.

The study of Astin (1996) also confirmed that the more learners interact with one another on a subject matter, the more the learning outcome and the better the performance of the learners in the application of the knowledge acquired, or experience gained. Participation which keeps learner active is also embedded in social networking. Participation, which Sefana (2008) describe as process of engaging learners in doing, thinking, feeling sense of belongings, and live engagement in all the activities for being part of engaging experience and keeps learner active.

2.15 The SNS based Model (appeared in Chapter 5)

Previous studies attempted to address the issues of security through:

1. Policies, which state the dos and don'ts on the wireless network, the wireless infrastructures and the WLAN environment;

2. Administrative strategies. Which plan, direct, coordinates, and control user online and offline activities;

3. Awareness and Training, which provides the user with basic knowledge necessary to operate safely on web interactions;

4. Collaborative efforts to consider security as everybody's responsibilities'

5. Risk and vulnerability assessment which identified areas of user weaknesses.

If one considers the above five security solutions focused by previous studies, the conclusion could be that the areas are adequate in addressing the escalating social engineering threats and attacks. However, this thesis found a gap created by the previous studies, which is the absence of a system of security that is OF the users, BY the users, FOR the users, that can continuously educate, update, inform and share security experiences ON REALTIME situations in the user's work place or organization. Hence, this thesis introduced, implemented and tested the SNS based model to fill the gap created by previous studies in addressing the social engineering based threats and attacks on network and information resources of an organization. The SNS (Social Network Security) based model is a model designed to fill the gap in the state-of-the-art efforts to provide solutions to the social engineering based threats and attacks on Wireless LAN in an organization.

The model is in the form of Socio-technical structure. The increasing reliance on connectivity, e-of-things, electronic and paperless organizations in the day-to-day functions and activities of organization, requires a technically skillful workforce that can identify and counteract the escalating threats and attacks on the network and information resources of an organization. The modern day organization is becoming more technical and connectivity is inevitably becoming an indispensable input and resources to the workforce of an organization. For an office worker to discharge responsibilities effectively, efficiently, and satisfactorily, availability of network is highly desirable. However, availability of network could be disrupted through threats and attacks.

Therefore for an undisrupted network service the user of the network must be technically skillful in the recognition and identifications of the threats and attacks on the network and information resources. Previous studies have attempted to provide frameworks and models that could address user weakness in security controls. However the previous studies were not able to provide a system or model that can develop the security skills in users on a continuous learning process and in real-time. The absence of such a system is a serious gap in the quest for social engineering solutions targeting the user. Threats and attacks are evolving like wild fire, and without a corresponding system that provides user with a real-time security skills, the quest for solutions to security would continue to widen. The implementation of the SNS based has been found to be effective in filling the gap created by the previous studies.

The Gaps specifically addressed by the SNS model.

Considering the discussions in the previous paragraphs, this thesis addressed the following specific gaps created by the previous studies. Thus, this thesis was able to identify the gaps created by the previous studies in terms of:

Patterns: of exposing user to social engineering security skills. While previous studies focused on traditional pattern and convergent curriculum in imparting technical skills on social engineering to users, this thesis provided user-centred sequential chains of skills in a divergent and systematic curriculum. Patterns and contents in learning situation must go hand in hand, otherwise, the learner (the user) is lost in the midst of the training and thus cause some lack of interest. The previous studies failed to address this thereby creating a gap for functional and effective awareness training. This study filled such gap by addressing the gap in the implementation of the SNS model, of which details is given in chapter 6.

Implementation:

The previous focused on theory with little or no room for user to practice what he/she have learned. Knowledge without practice is like telling an uninterested story to an uninterested audience. Here again, the previous studies created a gap in terms of implementation of the acquired technical skills on social engineering threats and attacks. This thesis filled such gap through implementation of the SNS model in such a way that users learn and practice – identify and counteract social engineering threats and attacks on their Wireless LAN.

Streaming and real-time Learning:

Skills acquisitions and competency must be continuous (proactive) as against static or (reactive) approaches as proposed by previous studies. The previous studies focused on periodic workshops, training, and seminars. Such approaches give no room for user continuous learning to update self for state-of-the-art security challenges. Thus, a gap is created in terms of a continuous security skills learning process that is up-to-date and current. This thesis filled such gap with real-time security skills learning process as contained in the SNS based model.

Real-time User Collaborations:

Previous studies only mentioned the need for users in an organization to collaborate on security matters; they failed to show how such collaborations should take place. Thus a gap is created by previous studies on how to bring users to collaborate on security issues. This gap is filled by this study through Bi-forminal ties, which is a formal and informal group interactions exercised on the platform of social media of Facebook.

User Security implementation Monitoring:

The user is the weakest link in security defense. Therefore there should be a real-time monitoring system to know how the user is performing as per security implementation is concerned. The previous studies could not provide a system that can reveal the contributions and performance of the user on security issues. Thus a gap is created by previous studies in addressing user security responsibility, ownership and accountability in collaborative structure. This thesis filled such gap through organizing users to apply Facebook functionalities of Post, comment, Share and like to collaborate on security experiences. This establishes responsibility and accountability among users through online presence and performance.

State-of-the-art approach:

Previous studies introduced various models to address the issue of social engineering based threats and attacks. While it is an effort to the right direction, yet the effort failed to include the most widely used system of interaction that knit users together for participatory and collaborative purposes. Nowadays social networking penetrates all facets of human life and hardly an individual is not belonging to one kind of social network or another. Since security is considered in previous studies as everybody's responsibility, then a system that could address security in a socially networked approach is a fit to addressing the problem of security. The previous studies created a gap for a state-of-the-art approach to mitigate against social engineering based threats and attacks. The focus was more on individualism than user network approach to implementation of security measures. The gap is filled by this thesis with the introduction of social network platform for security collaborations.

Socio-technical against Managerial biased approach:

Previous studies focused on managerial control thereby creating a gap in user freedom for collaborations on security. The managerial control inhibits Bi-forminal interactions among users for security collaborations. The managerial control approaches failed to provide a social structure that facilitates and enables users to share security experiences and develop their competencies. It is also often doctorial in its security policy thereby threatening users who may in the long run ignore relevant security policies; and thus pave way for various threats and attacks.

2.16 Summary

The literature reviewed so far, has indicated the need for a socio-technical system of security that is on real-time in developing user security skills; real-time in identification and prevention of social engineering based threats and attacks. The insufficiency of the previous studies in providing such a security system, created the gap which this thesis aimed to fill. Most of the reviewed studies recognize and acknowledge the emergence of new form of attacks through social engineering; and also most of the studies confirmed user as the problem of security and often described user as the weakest link to security measures. In view of this, various studies attempted to provide models and procedures that would address security issues in SE at the user link. In such attempts, most of the studies focused on user awareness, user training, and compliance to security policy with sanctions for noncompliance.

However, most of these attempts were addressing issues at individuality rather than group collaborations for security. The very few studies that proposed social responsibility for security were not able to set the modalities on how users should collectively discharge the security responsibilities. ***The overall review of the literature has indicated that most studies on solutions through social engineering were not able to come up with a socio-***

technical system of security that is of the users, for the users and by the users for real-time collaboration on security issues; and that could at the same time serve as platform for continuous user training on social engineering threats and attacks. A gap still exist in previous studies on how social engineering threats and attacks can be approached by proactive security structure that provides users with an enabling security structure. Thus a gap in literature was created, which the current study aimed to fill.

CHAPTER 3: **Methodology and Research design**
FOR THE IMPLEMENTATION OF THE SNS BASED MODEL

This chapter reports how the research was conducted with strict adherence to planned, systematic and organized, collection, analysis and interpretation of data through standard, appropriate, universally recognized and SHOLARLY accepted procedures and tools. The justification for the selection of the research methods and designs were also explained. The aim was to conduct the research scientifically and objectively – distancing the researcher from the research through reliability and validity measures as well as control of compounding, extraneous and subjective variables. The chapter also expounded on the theoretical perspectives which guide the conduct of the research.

3.1 Introduction

The study was aimed at implementing SNS (Social Network Security) based model for the identification and prevention of Social Engineering (SE) based threats and attacks in Wireless Local Area Network (WLAN) of the University campus of Umaru Musa Yaradua (UMYU) Katsina, Katsina state. This was achieved through standard plan and design of the research; systematic collection, analysis and interpretation of data; and through instrumentation by using appropriate tools and procedures, as explained in the subsequent headings in this chapter.

The first phase of the research question as indicated in chapter one, showed that this research was experimental study; and the second phase of the research question showed that the research involved a qualitative study. The subsequent headings in this chapter explain how both the experimental as well as the qualitative approaches were used to carry out this research. However, the philosophy underpinning this research is described first.

3.2   The Research Paradigm

A paradigm is a conceptual framework that establishes intellectual direction about issues and phenomenon of our world.   An understanding of phenomena towards solving a problem requires a systematic and methodological inquiry, which is termed as research. Research is also the process of knowing the unknown. Any type of research is identifiable to a philosophy. A research may fall in either of the two types of philosophical paradigms – the positivism and the interpretivism. The implication of research paradigm is to the collection and analysis of data. It also guides the research on best fit to research design and approaches.

The positivism emphasized the importance of an objective scientific method free from bias and subjectivity. A researcher under positivism sees his role as collector of facts and then studying the relationships of one set of facts to another. Positivist inclines to quantitative analysis of data through valid statistical techniques to produce quantifiable and generalizable conclusions. Positivism stresses the importance of studying social and organizational realities in a scientific way that mirrors the research process used in the natural sciences. *This description of positivist best fit this research and was considered as the underlying philosophy upon which this research was founded*. On the other hand, interpretivism is concerned with an understanding of human's perception of the world. Interpretivist sees facts as the product of human interactions. The Interpretivist is less to quantifiable analysis but more to subjective interpretations. The Interpretivist claims that in order to study phenomena, human feeling, attitudes and reasoning are relevant. Thus it focuses more on words, text, images than on numbers and statistics. The second phase of the research question of this study is concerned with behavioural analysis. *The characteristics*

and process of Interpretivist are desirable and best fit to address the second phase of the research question.

Having identified the two research paradigms as relevant and applicable to this research, the following table further identifies the characteristics and/or process of each paradigm for the purposes of referencing and check listing the application of each process.

Table 3: Characteristics and Process of Positivism and Interpretivism

POSITIVISM	➢ Work from scientific principle. ➢ Analyse phenomena in terms of variables. ➢ Start with theory and test/refine theory with data. ➢ Data should be collected by dispassionate researchers. ➢ A highly structured research process should be used. ➢ Theories can be used to predict future relationships and behaviours. ➢ Quantitative data are preferred. ➢ The validity and reliability of data are important for formulating.
INTERPRETIVISM	➢ Knowledge is constructed by human beings. ➢ Analyse phenomena in terms of issues. ➢ Researchers cannot be wholly dispassionate – they are involved and will influence situations to a certain extent. ➢ Flexibility may be required to allow the emphasis of the research to change. ➢ Qualitative data are preferred. ➢ Generating rich data is as important as the ability to generalize.

3.3   The Research Methodology

Research methodology prepares the research work towards answering the research problem in a systematic manner that follows certain protocols called standards that are accepted to the entire scholarly community. From the philosophical paradigms described in section 3.2, this research was able to map out the pattern and structure for the conduct of carrying out this research in a planned and systematic process. Against the background of

research paradigms and coupled with the research t question of this study, this research used both quantitative and qualitative method. In the qualitative method, experimental design was used; and in the qualitative method, qualitative content analysis was used.

3.4   The Quantitative Approach

Quantitative method refers to the systematic empirical investigation of phenomena via statistical, mathematical, or computational techniques. Quantitative method provides information only on the particular cases studied. More general conclusions are hypotheses. The quantitative method verifies which hypotheses are true. While there are different types of research methods, each addresses certain kind of question.

Quantitative method asks and addresses the following questions: which is the effect of a given cause? What is the cause of a given effect? How do we mitigate a given effect by manipulating a given cause? Lee and Ormrod (2001) identify three classes of quantitative method as descriptive, experimental and causal comparative.

This research adopted the experimental study. It is concerned with the manipulation of one variable to determine the effect of such manipulation from the outcome of the changes in the variables. The main pillars of experimental study are: controlled condition, random assignment, and manipulation of variables.

All these conditions were applied in this study as can be seen in the research design. Furthermore, the following table shows how the characteristics of quantitative research match this study.

Table 4: Characteristics of Quantitative method Matched to this Research

Quantitative Characteristics	Remarks of fit to this study
• Emphasized on collection and analysis of numerical data	✓ Test was conducted to participants and results obtained analysed statistically

Quantitative Characteristics	Remarks of fit to this study
• Scoring to measure distinct attributes of individuals and organisations.	✓ The test performance of the participants was scored and numerical data was obtained.
• Comparing of groups or relating factors by experiments.	✓ The two groups of the study were compared on the variables tested.
• Employing statistical analysis of data sets.	✓ T-test of independent sample was used to analyse the data.

3.5 The Pilot Study

Testing logistics and setting a feasibility study are necessary for the identification of issues that may be a threat to the reliability and validity of the study. Prelim study otherwise known as the pilot study serves as check and balance between methodology and instrumentation of the study. The methodology must correspond to the instruments and vice versa, with reasonable control to deficiencies or drawbacks that may invalidate procedure and the conduct of the research. In order to achieve quality and efficiency in the conduct of this study, pilot study was conducted on a group of 40 students randomly selected from the department of Office Technology and Management of Hassan Usman Katsina Polytechnic. The students were randomly assigned to experimental and control groups. The experimental group was exposed to a demo version of the SNS model for a period of one week. This followed with two days simulation of the SNS model on the social media of FB. After an interval of three days, both the groups sat for a posttest. The findings from both the posttest and process of running the pilot study revealed two important issues. In the first place, one of the dependent variable – the social context of authentication was not understood to the participants. Secondly, intervening and compounding variables kept on surfacing during the conduct of the pilot study. Such intervening variables were: participants mingling with the control group and the control group intruding in the presentation session. This was a serious problem which could not have been exposed or noticed without the pilot

study. With the cooperation of the research assistants, this problem was overcome in the main research implementation. It was overcome by engaging the control group in some office applications learning modules which run concurrently with the administration of the intervention to the experimental group.

3.6   The Experimental Design

Between groups pre-test post-test design was used to determine whether the program or intervention (the SNS based model) had the intended casual effect on the experimental group. Three major components guided the application of the experimental design. The components are: pre-post-test design, the treatment and the control group, and random assignment of the study participants. How each of these components was administered is described in the subsequent sections. Figure 2 depicts the sequence of using the experimental design.

Figure 20: The Sequence of the Experiment
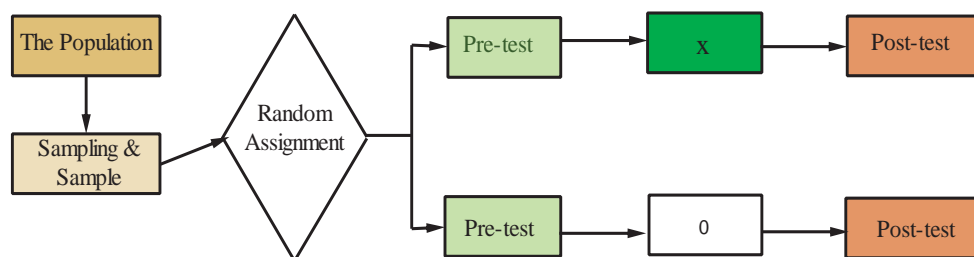
In the Pretest-Posttest design, the population was the first to be identified, then followed by sample of the population, and then:

- Subjects were randomly assigned to treatment and control groups.

- Pre-test was administered to all subjects in the groups.

- The researcher and the research assistants took control of measures on confounding influences to ensure that both groups experience the same condition, with the exception of the treatment group that received the treatment.

- Post test was administered to all the subjects in the two groups.

- Posttest scores were compared to determine the effectiveness of the treatment, which was the learning of the SNS based model.

Thus, the design followed the structure in table 5.

Table 5: Structure of the conduct of the Experiment

RANDOM ASSIGNMENT OF SUBJECTS TO:	1ST OBSERVATION (MEASUREMENT) DEPENDENT VARIABLE, 0_1= PRETEST	EXPOSED TO THE TREATMENT (X), INDEPENDENT VARIABLE	2ND OBSERVATION (MEASUREMENT) OF THE DEPENDENT VARIABLE, 0_2 = POSTTEST
Experimental Group	Experimental Group's Average on the dependent variable.	X	Experimental Group's scores on the Dependent Variable
Control Group	Control Group's Average on the dependent variable.		Control Group's scores on the Dependent Variable.

The Independent Variable (IV) is the knowledge and skills acquired on the SNS based model. The Dependent Variable (DV) is the learning outcome which was the ability to identify and prevent social engineering based threats and attacks.

3.7   The Population

A "Population" made up of all the subjects the study aimed to study. The entire users of wireless local area network were the target population of this study. There were 97

subjects identified as the users of the Wireless Local Area network in the University administrative environment. The population was therefore identified as 97 subjects.

Considering the allowance for the use of sample in research, this study attempted to enjoy such provision by using sample instead of the entire population. The use of sample also eliminates those subjects who for one reason or another may not be able to participate in the research; thereby affecting the validity of the result. A sample is considered appropriate and in order if used in the standard way.

3.8   The Sample and the sampling procedure

A "sample" is the representation of the population. It is part of the population that was used to study the entire 97 population of the users of WLAN. A sample that is statistically determined is considered generalizable on the entire population. This research came up with 80 subjects as the sample of the population. The 80 numbers were obtained from the table of random sample. Krejie and Morgan (1970) table of random sample was used to arrive at the 80 numbers.

Table 6: Determining Sample Size from a given Population

N	S	N	S	N	S	N	S	N	S
10	10	100	80	280	162	800	260	2800	338
15	14	110	86	290	165	850	265	3000	341
20	19	120	92	300	169	900	269	3500	246
25	24	130	97	320	175	950	274	4000	351
30	28	140	103	340	181	1000	278	4500	351
35	32	150	108	360	186	1100	285	5000	357
40	36	160	113	380	181	1200	291	6000	361
45	40	180	118	400	196	1300	297	7000	364
50	44	190	123	420	201	1400	302	8000	367
55	48	200	127	440	205	1500	306	9000	368
60	52	210	132	460	210	1600	310	10000	373

N	S	N	S	N	S	N	S	N	S
65	56	220	136	480	214	1700	313	15000	375
70	59	230	140	500	217	1800	317	20000	377
75	63	240	144	550	225	1900	320	30000	379
80	66	250	148	600	234	2000	322	40000	380
85	70	260	152	650	242	2200	327	50000	381
90	73	270	155	700	248	2400	331	75000	382
95	76	270	159	750	256	2600	335	100000	384

Source: Krejie and Morgan (1970). Determining Sample Size for Research Activities

Note: "N" is population size

"S" is sample size.

3.9   The Random Assignment

Prior to the random assignment, the two groups sat for test of equivalency known as pre-test, which was used to establish the similarity of the groups. While random selection points to external validity, random assignment focuses on internal validity.   Random assignment scientifically assigns subjects to both the experimental and control groups in such a way that each participant has an equal chance of being assigned to either of the two groups. The aim was to ensure that each group mirrors each other. One significance aspect of random assignment is to control confounding variables that might invalidate the research. The random assignment eliminates problems of differential influences by making the groups similar on all extraneous variables (Johnson, 2009).

The sample population of this research was 80 subjects. The subjects were divided into two groups of 40 subjects each. The experimental group had 40 subjects and the control group also had 40 subjects. Random assignment was used to decide who should be in which group. The random assignment software from the following link:

http://www.graphpad.com/quickcalcs/randomize1.cfm, was used to assign subjects to groups. The following random assignment was generated:

Table 7: Random assignments to groups

Exp. Group	3 11	13 14	16 18	21 25	26 29	31 33	34 35	40 41	42 43	44 46	48 51	52 54	55 59	60 61	63 65	68 69	70 71	72 74	75 77	79 80
Control Group	1 2	4 5	6 7	8 9	10 12	15 17	19 20	22 23	24 27	28 30	32 36	37 38	39 45	47 49	50 53	56 57	58 62	64 66	67 73	76 78

3.10 The Pre-test

In order to ensure that the two groups were similar in terms of knowledge and skills of social engineering, security of WLAN, social media application, and collaborative participation on social networking, knowledge-based exam consisting up of 50 items was administered to the two groups. The exam was administered with the coordination of the research assistants.

The two groups sat for the exam on the same data, at the same time and in two different locations in the University campus. After the pre-test was conducted the intervention or treatment started a week later.

3.11 The Intervention/treatment

The experimental group received training in form of teaching and simulation for 18 weeks on how to use the SNS model to identify and prevent social engineering based threats and attacks on WLAN. The SNS model was divided into 6 modules; and using blooms taxonomy of learning, each module was presented to the experimental groups within two to three weeks as depicted in Table 8.Thus, the implementation of the model consists up of three stages: the teaching-learning stage, the testing stage, and the follow-up stage. A period of Twenty four weeks (24) was spent exposing the experimental group to the SNS-based model; and after the completion of imparting the model to the experimental group, experiment was conducted to ascertain the effectiveness of the model, to test the hypotheses of the research, and to answer the overall research question.

Table 8: knowledge/skills based implementation of the SNS Model

Wks.	Content	Activity	Duration
1-6	~ An overview of Wireless LAN ~ Threats and attacks on Wireless LAN ~ User as component of Wireless LAN ~ Definition of Intrusion Prevention ~ Social engineering – meaning and concepts ~ Techniques and types of offline/online ~ SE threats and attacks ~ How to identify both forms of attacks and their respective techniques. AIDAC	Lectures Discussions Role Play Visual Display	2 hours Each day For 5 days
7-12	~ Social Engineering Malware, and Phishing ~ Anatomy of the threats/attacks ~ Threats vectors and Mitigations ~ Visual identification/human factor ~ Authentication ~Understanding user's position and roles in protecting the network. ~ Online user behaviour and vulnerabilities	Lectures Discussions Role Play Visual Display	2 hours Each day For 4 days

Details of the contents are available in chapter five.

Module 2: Social Networking and the SNS model

Wks.	Content	Activity	Duration
13 - 19	Understanding social network for collaboration ~ Collaboration for IP on WLAN. ~ Understanding Facebook and its structure ~ Using Facebook for Social Networking ~ Using the SNS based Model ~ Training on the use and Application of the model on the social network	Lectures Discussions Role Play Visual Display	4 hours Each day For 4 days

Wks.	Content	Activity	Duration
20 - 22	~ Revision ~ Nodes and Ties in the social network ~ Groups and relationships ~ social system of IP through the use of Acquired knowledge and skills of the SNS Model.	Lectures Discussions Role Play Visual Display	4 hours Each day For 4 days
23 - 24	~ Revision ~ Plenary Discussions ~ **Test**	Plenary session Qs and Ans. Attempting a test in form of Questionnaire in close ended and open ended design	2 hours each day for 3 days for plenary and Qs/Ans sessions. One day for the test for 2 hours

3.12 Blooms taxonomy of learning

Blooms taxonomy of learning was used to administer the treatment to the experimental group. Blooms taxonomy of learning is a learning model that provides a structure for presenting knowledge to group of learners with varied abilities and backgrounds. It is a process oriented model that facilitated the administering the SNS model to the treatment group. The model was developed by Benjamin Bloom in 1956. Figure 3.2, depicts the Blooms taxonomy of learning and by the side of each hierarchy, this research described how the level was used to administer the treatment.

The relevance of using Blooms taxonomy of learning in this research is because for the subjects of the study to be able to identify and prevent social engineering threats and attacks in the implementation of the proposed SNS based model, the following domains must be involved:

  a. Imparting of knowledge;
  b. Developing of skills;
  c. Developing of competencies;

The applications of the above three domains are suitable and appropriate with the blooms taxonomy of learning. Blooms Taxonomy of learning is a classification of learning levels that maps the way learning is designed and information is processed. Thus it is the categorization of learning objectives and goals in the course of imparting knowledge to learners. It was proposed in 1956 by team of educational psychologists led by Benjamin Blooms; and it was revised by Anderson (2001).

Bloom was an American educational psychologist who made influences to the classification of educational learning objectives and to the concept of mastering learning. Blooms divided the educational learning objectives into three areas or domains: Cognitive, Affective, and Psychomotor. The goal of Blooms' Taxonomy is to focus on all the three domains while preparing the learner for a more functional education. The cognitive domain is divided into six categories or layers, with each layer presenting increasing complexity: Remembering, Understanding, Applying, Analyzing, Evaluating, and Creating.

Figure 21: Blooms Taxonomy of learning and how it was used to administer the treatment.
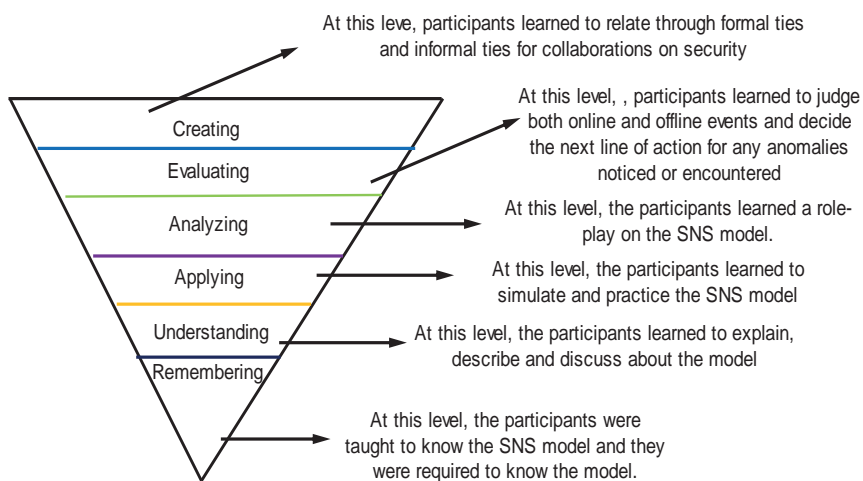
3.13 The Posttest

After administering the treatment to the treatment group, a Posttest was administered to both the Experimental and the Control group. Thus, the same data was collected from the two groups with the aim of ascertaining whether the intervention had a casual effect. The structure and pattern of the questions asked during the post-test is shown below in Table 8.

The test was conducted In the Wireless laboratory and computer laboratory of UMYU – Umary Musa Yar'adua University, Katsina – Katsina State, Nigeria, both the experimental and the control groups consisted up of 80 participants took the test on the same date and at the same time.

The SNS-based Model Test was administered to the two groups and was made up of 60 responses in 50 questions with fill in the blank and multiple choices. In the multiple choices, each question in the test has four to five answer options from which a subject was to select the correct response. The following conditions and pre-requisites were satisfied prior the implementation of the test:

- Participants must keep their systems ON and connected to the internet;
- Participants must observe the behaviour of their systems;
- Participants must observe the behaviour of their network;
- Participants must observe the behaviour of their OS.
- Participants checking their emails at regular intervals;
- Participants were often directed to some websites;
- Dumped items/devices were placed on the participants' tables;
- Participants remained online on the Facebook;
- Personal and professional engagements by research assistants in some sessions of the test.

The third stage of the implementation was the follow-up stage made up of content analysis on the Platform of Facebook for SE based IP on the Wireless LAN - assessing what the participants were doing after the implementation of both stages one and two. The details of the questions are provided in the appendixes. However, the following is the structure of the test and the marks awarded for correct response. The questions given to the participants did not follow the order in the following structure, but were mixed-up for the reason of controlling due advantage for the experimental group. The total number of correct responses for each subject made up of the total scores of the subject in the test. Thus,

Table 8: Interpretation of subject's Test scores

Subject No:	Overall Questions	Correct Response	Total Scores or Performance
01	50	10	10 – Each question carries one mark.

Security features were disabled in the systems used for the experiment with the aim of infecting them with malware that followed the user to the sites visited and influenced the user to do something or reveal certain information. The aim was to test the subjects' ability to identify and mitigate any malicious encountered through the correct responses to the questions in the test.

Table 9: SNS-based Model Test for IP in Wireless LAN

Module	Question Theme	Question Categories	Subjects' Activity	Mark Awarded
I	Tricks and Techniques of SE	Questions covered Online-offline tricks and threats through: Pop-ups, Phishing Websites, Malware, Clickable links, Road Apple, email Scams.	Subjects were directed to some websites, and asked to answer questions relevant to the sites. The questions also referred to the implanted items dumped on the subjects' seat for response to offline SE	Correct response to an answer earns 1 (one) mark.

Module	Question Theme	Question Categories	Subjects' Activity	Mark Awarded
II	Human Factor Authentication	Questions covered Online-offline human way of authenticating a threats or attacks through: Website anomalies, browser behaviour, OS behaviour, email messages, professional engagement, personal engagement, and environmental suspicions.	Subjects were directed to certain websites with certain anomalies and as well asked to adjust certain settings of their browsers'. Offline SE threats were also made available and the subjects' attention TO to the materials was drawn in answering the questions.	Correct response to an answer earns 1 (one) mark.
III	Counter Measures To SE Threats & Attacks	Questions covered: measures on Clicking a link, opening an attachment, modifying browser settings, filling online form, downloading, installing a program, picking a dumps diving, and accepting instructions or executing request from unknown persons.	Subjects were asked to answer the questions by selecting the correct response on how to respond to various threats and attacks that are SE based malware and phishing attacks.	Correct response to an answer earns 1 (one) mark.
IV	Formal Tie Connection	Questions covered subjects' ability to connect to constituted authority, IT officer, superior, subordinates, colleagues, and written formal report.	The questions asked subjects to select the appropriate response as per sharing, disclosure and reporting abnormalities and suspicious identified both online and offline activities and interactions.	Correct response to an answer earns 1 (one) mark.
V	Informal Tie-Connection	Questions covered subjects' ability to connect to informal associates in the event of sharing, reporting and disclosing online and offline encounters.	Subjects were asked to select the appropriate response from the questions as per sharing, reporting, and disclosing online and offline SE threats and attacks.	Correct response to an answer earns 1 (one) mark.
VI	Using Facebook Media for Security Collaboration	Questions covered the abilities of the subjects to use Facebook functionalities in learning more about SE threats and tricks, posting experiences and encounters, commenting, sharing, and liking.	Subjects were asked to study their respective Facebook pages and answer some questions The questions touched on how the subjects can learn and identify threats on social media and how they can collaborate to share and prevent the threats and attacks.	Correct response to an answer earns 1 (one) mark.

However, before the Post-test was administered, content validity and reliability of the test were established.

3.14 The Content Validity

This refers to the inclusion of all the items the test supposed to cover. If the test fails to include certain variables that are relevant in answering the research questions and realizing the objectives of the study, then the test would lack content validity. This could affect the findings of the study. in order to establish the content validity of the Posttest, five professionals in the field of Education, Social engineering, Network security, Social media and mass communication, were given the drafts of the research questions and the objectives of the study for their moderations, amendments and reviews. Their views and recommendations were considered in reviewing, modifying and updating the questions in the post, thereby ensuring valid contents in the test.

3.15 The Reliability Test

Pilot and Hugler (1993) define reliability as the degree of consistency with which a test measures the attribute it is designed to measure. Apart from sufficient contents the Posttest should contained, the test should as well be able to yield the same result, if administered at different time and to different subjects. This called reliability test.

 Test reliability is significant for two reasons: In the first place, random measurement error on the participants' scores can be ascertained through reliability test. Measurement errors are factors that are unpredictable and can thus increase or lower the participants' scores. They include fatigued, ambiguous or tricky questions. In order to avoid random errors, test must be reliable.

Secondly, test reliability is a compliment to test validity. The failure of a test to assign scores consistently is an indication that the test cannot measure what is is intended for. In order to establish the test reliability in this study, Cronbach;s alpha index of test reliability was used.

The range of Cronbach's alpha is from 0 to 1.00. Values close to one indicate high reliability and vice versa. The value obtained in this research was 0.91, thereby indicating high reliability and the test was considered to have satisfied reliability test. The following formula was used in calculating the Cronbach's alpha:

Equation I: Cronbach's alpha

$$\alpha = \frac{K}{K-1}\left(1 - \frac{\sum_{i=1}^{K}\sigma_{Y_i}^2}{\sigma_X^2}\right)$$

Where, $\sigma_{Y_i}^2$ is the total variance for the total scores; K is the number of items in the exam; P_i is the item difficulty or the proportions of the candidates who answer item i correctly.

3.16 Instruments used for Data Analysis

Since the first part of the research question of this study is asking for quantitative data, statistical instrument was then appropriate for the data analysis. However, choosing the right statistical instrument could render the results valid or invalid due to right or wrong choice of the statistical tools. In order to use the right statistics, certain standard procedure must be followed to arrive to the right choice of instruments.

According to Roscoe (1969), the following flow chart guides the selection of appropriate statistics. Using the Roscoe flow chart below, I identified t-test for independent sample as the appropriate statistics to analysis the data generated from the experiment. The choice of t-test for independent sample is evidence because of the followings claims:

- The data was interval/ration type
- The question is looking for difference between groups;

3.17 The Independent Sample t-test

In a layman's term, t-test is used to determine the probability that two populations are the same with respect to the variable tested. There are a total of 80 participants, with 40 in each of the two groups. Since there are different subjects in each group, these "samples" are "independent" of one another; thereby pointing to t-test of independent sample. The research taught the experimental group the knowledge and skills of the SNS based Model for identifying and preventing of attacks that is attributed to social engineering, in WLAN.

After the treatment was given to the experimental group, the same test was administered to the two groups, at the same time. The aim was to find out if the two groups are the same or not, on the independent variable at the apha level of 0.05. The hypothesis of this research is directional. The null hypothesis is the opposite of what I hope to find. After calculating the "t" value, a decision is made as to reject or accept the null hypothesis on the basis of the size of the "t" value.

There are 8 steps in an Independent Samples t-Test:

1. Define Null and Alternate Hypotheses
2. State Alpha
3. Calculate Degrees of Freedom
4. State Decision Rule
5. Calculate the pooled variance
6. Calculate Test Statistic
7. State Results
8. State Conclusion

The Hypotheses (the null and the alternate)

The alternate hypothesis is the antithesis of the null hypothesis. Whatever H_0 (null hypothesis) is, H_1 (alternate hypothesis) is the other side of the argument. The two hypotheses are mutually exclusive, only one at a time can be true. They cannot be true at the same time. Accepting one implies rejecting the other, and rejecting one leads to the acceptance of the other.

Equation II: declaration of Null and alternate hypotheses

$$H_0; \mu_{classA} = \mu_{classB}$$
$$H_1; \mu_{classA} \neq \mu_{classB}$$

The H_0: *There is no significance difference in the performance scores of the subjects exposed to*

> *SNS based Model in the identification and prevention of a social engineering based attacks in a WLAN and those who were not exposed to the SNS based Model.*

The H_1: the subjects exposed to the SNS based Model perform better in the identification and prevention of a social engineering based attacks in a WLAN than those who were not exposed to exposed to the SNS based Model.

3.18 The Qualitative Content Analysis Method

Content analysis is about how issues are talked about**.** This is the second part of the research method that attempted to answer the second phase of the research question. Qualitative research acknowledges the contextual nature of inquiry (Glesne and Peshkin, 1992, p. 7). It has been described as "watching people in their ownterritory ... interacting with them in their own language, on their own terms" (Kirkand Miller, 1986, p. 9). According to Krippendorff (1980), Content analysis is a research method for making replicable

and valid inferences from data to their context, with the purpose of providing knowledge, new insights, a representation of facts and a practical guide to action.

Content analysis is part of the qualitative research and it is the type of research that focuses on interpretation of phenomena in their natural settings to make sense in terms of the meanings people bring to these settings (Patton, 1996). Content analysis was used to describe the behaviour of the participants while implementing the SNS based model on the social media of Facebook. This was achieved through sifting of certain words or concepts within texts or sets of texts, or images posted, commented, or shared by the participants. The research then analysed the presence, meanings and relationships of such text, images and concepts.

3.19 The Position of this Research in the Classes of Content Analysis

Content Analysis is broadly classified into two Semantic and Syntactical (Ahuvia, 2001). In semantic content analysis, content are classified into predetermined categories, ferreted out from a word, phrase or sentence, irrespective of the syntax used to establish meaning. According to Krippendorff (2004), there are three categories of Semantic content analysis.

- Designation Analysis: referring to the appearance of certain objects, things or concepts.

- Attribute analysis: refers to the reference made to characteristics of a predefined category.

- Assertion analysis: refers to the way a particular category is directly mentioned to refer to a particular category.

The second category of content analysis is the syntactic, which refers to the classification of content according to its physical properties.

3.20 Manifest and Latent Content Analysis

Manifest content analysis focuses on the coding that is manifest or obvious. Manifest content analysis uses straight forward and literal meaning while making coding decisions (Ahuvia, 2001; Holsti, 1969). Smith and Taffler (2000) refers to the manifest content analysis as form-oriented or objective. On the other hand, latent content analysis is reading between the lines to bring out the coding unit. It is how the meaning of the content is interpreted. *This research used the manifest function. This is because the research was interested in the type of contents the participants were posting. In addition, the posting on social media came with predetermined categories that made the coding obvious and straight forward thereby pointing to manifest content analysis.*

3.21 Manual Content Analysis

Manual content analysis is the use of human codes to identify the units for coding and categorization. This research used manual system of conducting the content analysis as against the computerized or intelligence system. The justification for this was, in the first place the use of coders maintained the desired reliability in the content analysis. Second: computerized or intelligence system used key word search. It is difficult to detect through Keywords search for contents embedded with social engineering statements. Moreover, as Holsi (1969) pointed out, intelligence system is ideal where the unit of analysis is the word or symbol, and inferences are to be based on the frequency with which they appear. Against this background, as this study attempts to analyse divergent contents on the social media of FB, computerized system was not considered the best fit method.

3.22 The Process adopted in conducting the Content Analysis

This study adopted the eight steps process in conducting content analysis as recommended by Weber (1990). The study also used some of the procedures of Krippendorff (2004). Figure shows the eight processes with brief description of how each step was applied in this study under the various sections.

Figure 22: The Eight Step Process to the Content Analysis

Figure: Weber (1990) Eight Step Process to Content Analysis: Used in this study
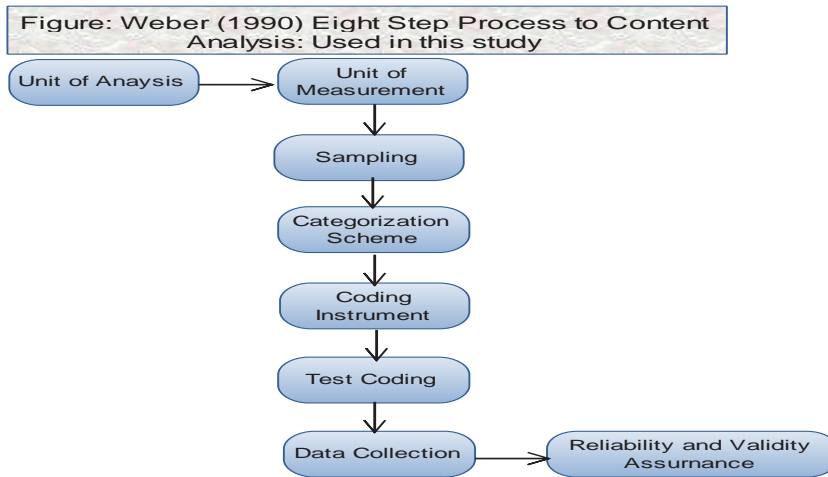
3.23 The Recording Unit

According to Holsti (1969), recording unit is the specified segment of content that is characterized by placing it in a given category. This study identified any part of the posting, comment, shared, or liked as the recording unit. The part of the recording unit was in the form of text and images. A word, phrase, sentence and paragraphs constituted the properties of the recording unit. However word was not considered as the appropriate recording unit in this study. This is because the terminologies of security threats and attacks that are based on social engineering cannot be presented directly by the divergent contents coming from the users.

However, phrases, sentences and paragraphs could point to a security terminology. For example, few users may directly mention the word "phishing," whereas majority may mention phrases, sentences and paragraphs that can categorize the content to phishing. Milne and Adler (1999) asset that in certain filed of research, the use of word cannot bring out the desirable category without the assistance of sentence or sentences.

This study therefore considered phrases and sentence(s) as the recording unit. According to Milne and Adler (1999), sentences are reliable units and can facilitate the coding system. Beattie and Thomson (2007) also supported sentences as recording unit for they assert that inter-coder reliability is more guaranteed with sentences comparison. In this study, sentence(s) that identified with the security terminologies of concern to this study were categorized accordingly. Therefore putting a sentence in the domain it belongs enhances mutual exclusiveness of the recording unit (Abeysekera, 2006).

3.24 The Theme Unit

A theme is an idea or sentence portrayed for an analysis. The theme in this part of the study is pre-existed; and the major theme is: the behaviour of the users of WLAN in implementing the SNS model on the social media of FB. This major theme was further subdivided into four themes: the users posting behaviour for security collaboration, the users' comment behaviour for security collaborations, the users' sharing behaviour for security collaborations and the user likes behaviour for security participation. The contents analysed were not complex as such the pre-existed themes facilitated the analysis.

3.25 The Measurement Unit

Since numbers were not involved in this study, this study then used communication of meaning in latent dimension as its unit of measurement. Unit of measurement in content

analysis hinges on three units: a) space /time, b) frequency and c) intensity or direction. This study used intensity or direction and measured the direction of the interactions of the users was inclining as per social network security is concerned.

3.26 The sampling Unit

Two distinct groups for the implementation of the SNS based model existed on the platform of social media of FB and collaborated side by side. The members of the first group were selected and purposely established for formal tie interactions in the implementation of the model; while the second group was formed on freewill by some members of the first group, for informal tie interactions in the implementation of the model. In other words, the first group was given the freedom to establish not more than one group with free will membership. Automatically an individual, who considered himself as not part of the group culture, may not join the second group.

However, the sole aim of the two groups was the implementation of the SNS model (security collaborations). The only difference was that the first group was formal (called formal tie interaction) and the second group was informal (called informal tie interaction), formed on freewill by some members of the formal group. The two groups in this study are called Bi-forminal ties.

3.27 The Categorization Scheme

The heart of content analysis is the establishment of predefined categories generated from reliable coded context. It is the process of fine-tuning. Such fine-tuning was necessary in reaching the level of satisfaction that all relevant distinctions about the data were achieved through the categorization system. The contextual data from the two groups FB pages were coded and similar codes were grouped into categories based on their common

properties. Phrases and sentences were analysed line-by-line for the identification of common properties for categorization purposes. Thus, the data was grouped on like with like system, messages that seemed similar or related were grouped together. However, the grouping was not done arbitrarily; decision to compare and differentiate was implicit in the grouping process. In other words, the categorization took into considerations the differences between the included and the excluded data.

3.28 The Coding Instrument

Methodology is all about systematic process. In content analysis there is the need to explain how the data capture process was done. According to Carney (1972), disclosure of how data were generated facilitates understanding and assessment of the research. This research adopted the suggestion of Boyatzis (1998) in a five factor coding considerations tools.

- Assigning a label and this comprises up of category name and code.

- Define the concern of the category or the characteristics or issues constituting the theme.

- Describe how to identify the category or how to flag a category

- Describe exclusive attributes in the identification of the category.

- Provide examples with positive and negative dimensions so as to minimize confusion while identifying a category.

This study applied the five considerations by observing coding rules of inclusiveness and exclusiveness in the data categorization system. Figure 3.4 shows the reflection in the use of the coding instrument.

Figure 23: Coding Extract format

Figure: Showing an extract of how the coding instrument was applied

Category	Operational Definition	Coding Rules	Example
Spoofing	Any form of faking and/or hiding identity to lure the user in thinking that message or identity is from known person or source. fake representation or identity hijacking are both act of spoofing. it also include any form of disguise through hoaxing, tricking or deception.	Any element not pointing or inclining to fake or disguise representation is exclusive to the category of spoofing and should either be placed in a subcategory or to the appropriate category	*"Hi guys, I came across a fellow introducing himself as new lecturer and he seemed in a hurry asking me to kindly print some document for him from his removable flash drive. I became suspicious wanted to make certain inquiries then he hurridly walke away."*

3.29 Data Collection

The social relationships and interchanges which describes the succession of actions and events in which the participants engaged on their respective groups' FB pages, constituted the data of this study. The participation of the researcher to elicit meaningful response also constituted data collection pattern. According to Ian (2009) data collection can itself be conceived as an interactive process through which the researcher struggles to elicit meaningful interpretations of social interactions and patterns of behavior.

Figure 24: Data Collection stages
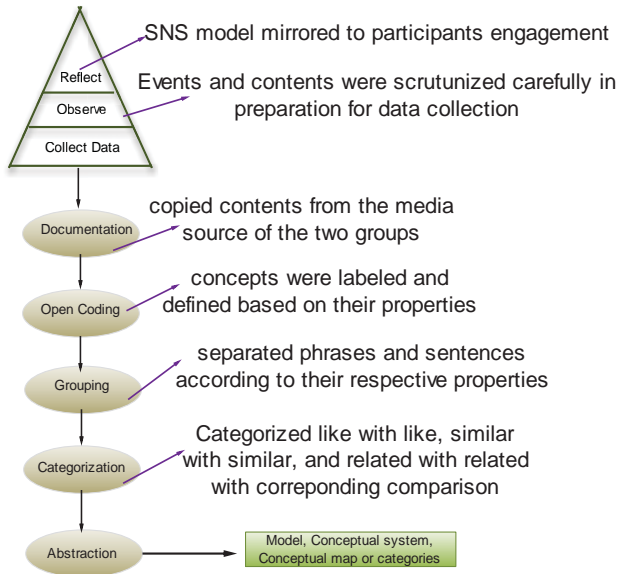
3.30 Justification for using content Analysis

The justification for selecting content analysis to address the second phase of the research question rested on the followings:

- *It is unobtrusive and non-reactive method of collecting data about phenomena (Krippendorff, 2004). In the case of other methods like interviews and focus groups, the participants may switch to a pretext mode and such habit can contaminate the data thereby misleading the conclusion of the research.*

- *For many years content analysis has been used in media and communication research (eg., Bos and Tarnai, 2004; Carney 1972; and Krippendorff, 2004).*

- *It has the quality of preserving data source (Krippendorff, 2004). Other methods may not guarantee preserving the data source.*

- *It is effective in ferreting out appearing attributes from the content (Berge, 1998). This was useful to this research in addressing the second phase of the research question.*

- *More "objective" data.*

142

- Rich with divergent data.

The research studied the contents participants were presenting on the social media of FB. The justification why content analysis was selected is because it has been used by many researchers as the appropriate method of studying social media content and communication. For example,

3.31 Reliability and Validity

Reliability is concerned with consistency over repeated measures. If consistent result is obtained over series of observations, then a level of confidence is said to have been reached to declare attainment of reliability. The more reliable the research instruments are, the more valid and convincing are the findings of the research.

To attain the level of reliability and minimize subjective interpretations, the coding was performed by professionals in qualitative research. Apart from their expertise experience, the rules of coding and the operational guided their individual coding. The use of the five coders was to ensure reliability from the coded data set produced by the analysis.

In content analysis, inter-coder reliability is widely acknowledged and is highly critical. The validity of the data interpretation is justifiable only with proper coding. The inter-coder reliability is the general consensus reached by individual coders over the characteristics of a message or artefact. According to Tinsley and Weiss (2000), inter coder agreement is needed in content analysis because it measures only the extent to which different judges tend to assign exactly the same rating to each object. Similarly Kolbe and Burnett (1991) assets that inter-judge reliability is often perceived as the standard measure of research quality. High levels of disagreement among judges suggest weaknesses in research methods, including the possibility of poor operational definitions, categories, and judge training.

Validity in content analysis refers to the extent to which the study is comprehensive enough in contents and context to measure what it is expected to measure. According to Krippendorff (2004), validity is the quality of research result that leads us to accept them as true. In this research, the validity was established right at the level of the research design and the data gathering process. Thus, the content analysis aimed to describe the behaviour of the participants of the study in the implementation of the SNS mode and the reliable formation of the categories justifies the validity of the study.

3.32 The Bi-Forminal Ties

Therefore the two groups together with the contents of their FB pages were the sample of this study. The FB pages of the two groups included all the contents of individual posts, comments, sharing, and the likes. According to Popay et al. (1998), randomness and representativeness are of less concern than relevance in qualitative research. So far the sample can produce the right type of information relevant to the understanding of the phenomena, further considerations on sampling criteria are unnecessary. This research was aware of this and in order to have fair involvement of the participants, randomization was still carried out to give each participant fair and equal chance. The figures and show the sample of the participants and the sample of the context of the implementation of the SNS model on the FB pages of the two groups.

Figure 25: The first Group (formal tie interaction) on the implementation of the SNS based model
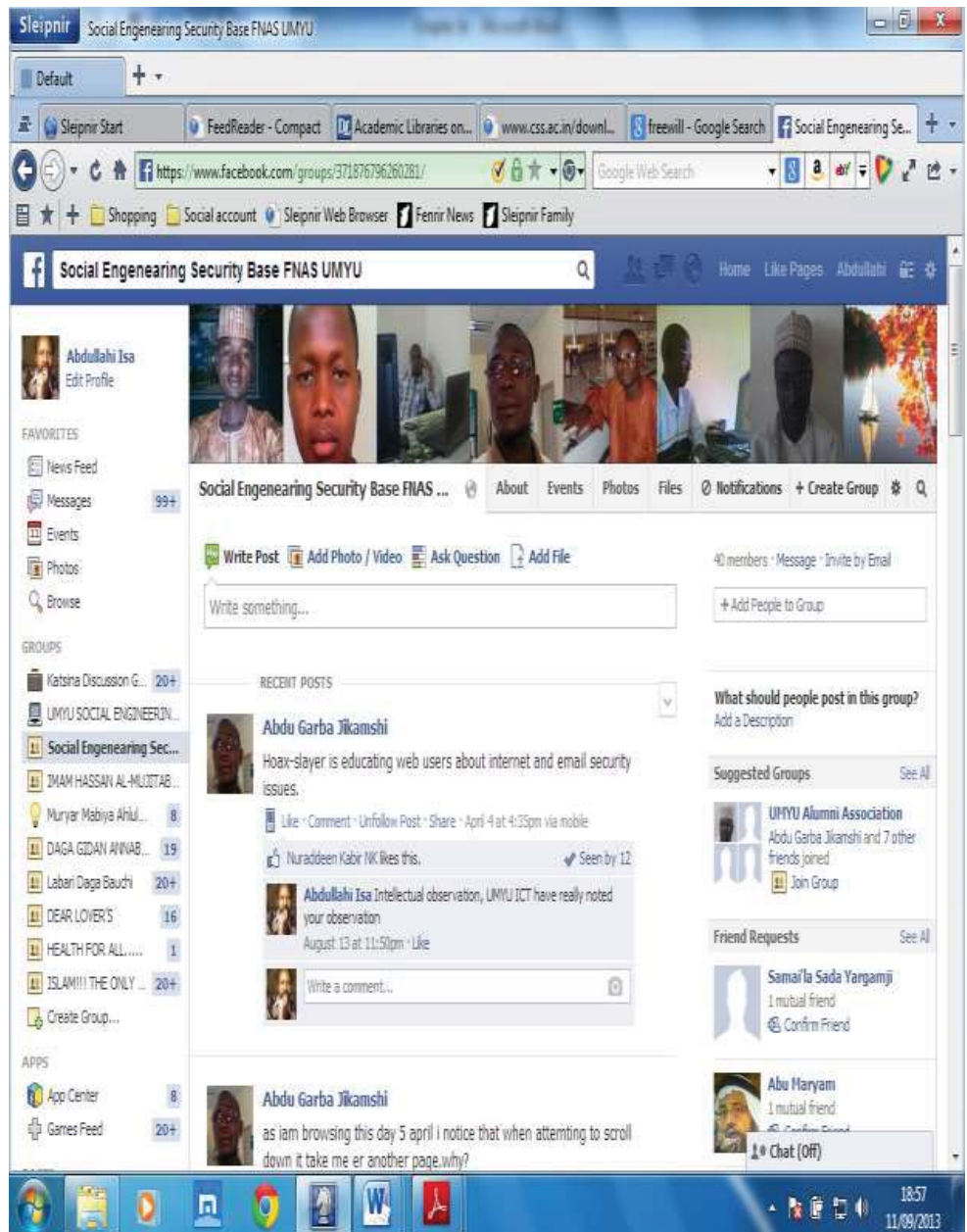
Figure 26: The Second Group (Informal tie interaction) on the implementation of the SNS based model

3.33 Summary

The purpose of this chapter was to describe the method and instruments used in designing and conducting this study. The chapter introduced experimental design as the appropriate research method to test the research hypotheses and answer the first part of the research question. The chapter also explained the procedures used to arrive at t-test for

independent sample as the statistical instrument used to analyse the performance scores of the participants. The justification for the choice of method and the instruments were also provided. Controlling measures against threats to reliability and validity were also high-lighted thereby achieving the desired quality and efficiency in the research

Therefore on the one hand, this research used experimental method to test the effect of the SNS model in the identification and prevention of social engineering based threats and attacks. Thus, the SNS model served as the treatment administered to the experimental group. On the other hand content analysis was used to analyze the behaviour of the sub-jects of the study in the implementation of the SNS model on the social media platform of Facebook. The data for the experimental methods was the test scores of the subjects of the study.

The instrument used to analyze this data was t-test for independent sample. Thus the data was quantitatively analyzed. The data for the content analysis was the social net-working (for security) activities of the subjects of the study, on the social media of Face-book. The instrument used to analyze this data was content analysis involving themes, cat-egories, and patterns.

Thus, the data was qualitatively analyzed with interpretations and schematic dia-grams. The purpose of creating categories in the content analysis is to provide a means of describing the phenomenon, to increase understanding and to generate knowledge (Cavanagh 1997). According to Tesch (1990), there is standard procedure for data analysis within qualitative research, but rather a "fluid" process of making sense of data. In this research, the data was qualitatively analysed for trends, patterns, relationships and similari-ties.

CHAPTER 4:   The Theoretical Framework

"The starting point for designing a theory of socio-technical systems is the observation that hardly anybody has a general understanding of the technical society; this applies to laypeople as well as to specialists. Particularly, engineers tend to ignore the social concerns of their work, and social scientists, on the other hand, do not know very much about technology and are reluctant to consider the artificial reality of technical objects. That is the reason why I came to systems theory; I needed a powerful tool to bring both sides together. So I take the systems model to describe both social and technical phenomena, persons and machines, the technization of society and the socialization of technology."(Ropohl, 1982).

Hereby in the current research:

TECHNICALIZATION OF USERS, and SOCIALIZATION OF SECURITY

Thus, this thesis introduced, implemented and tested SNS model in wireless environment of an organization for identification and prevention of social engineering threats and attacks. The model is socio-technical both in its structure and application. It was created from a socio-technical perspective to develop security skillful users who can learn and collaborate on security matters on real-time to complement the technical and automated system of security.

4.1   Introduction

The previous chapter three described the methodology followed in the implementation of the SNS based model; the current chapter four describes the framework from which the proposed model was developed. Irrespective of the type of research conducted, a framework in form of a model or theory is necessary in guiding the conduct of the research. Patricia and Mary (2002) define theory as set connected principles which provide a systematic view of a phenomenon. Theory set the foundation for how to describe the research work. Chinn and Kramer (1999) define a theory as an "expression of knowledge….a creative and rigorous structuring of ideas that project a tentative, purposeful, and systematic view of phenomena." Thus, a theory is akin to a blueprint used to organize a system. This research draws largely from the Socio-technical theory in the design and conduct of the

research. After discussions on the theoretical underpinnings of this research, the next is the details elaborations of the proposed SNS based model.

4.2   Conceptualizing the Socio-technical System

The origin of the Socio-Technical Theory can be traced back to the efforts of the British Coal mine to optimize work process by a joint optimization of a social and technical system. The pioneers of the theory, Trist and Bamfarth (1951) argued that a work process should not only be considered as being a technical system of plant and machinery, or a social system with work force interactions, but should rather be considered as a single two-dimensional system (the social system and the technical system), thereby making the system socio-technical. In support of the Theory in addressing the problem of the Coal mine, Fox (19951) established that the problems of the Coal mine and related Industry existed because of so much attention paid to technical aspects of production without a corresponding attention to the social structure and human requirements. This is similar to the argument of the current research that too much attention to technical solutions to security has overshadowed the social system solutions to security. Vendor solutions and Scholastic solutions to security are more on the technical (automated-software) system, thereby paying less attention to the social system (or the user); who is the weakest link to security threats and attacks.

Harvey (1994) defines ST theory as a system approach that is concerned with the interdependencies between and among people, technology and environment. While Cummings (1994) sees ST theory as a system that seeks to optimize both the social and technical domains in an organization. The ST theory draws heavily from the open system theory, which implies that an organization should be seen as a whole entity in which its parts are interrelated and a dysfunction in one part leads to a dysfunction in another part. This is

149

true of the argument in the current research in which a dysfunction in user security renders the user the weakest link, thereby rendering the network insure and vulnerable to attacks. Recalling the doctrine of the STS theory, that organizational problem can best be addressed if both the social and the technical systems are optimized together. This is confirmed by Van De Ven and Joyce (1981); and Pasmore et al (1982). The current research used such doctrine to address the social system of security that suffers neglect to the extent of rendering the user the weakest link to security threats and attacks. Thus the ST theory is a best fit in addressing issues of a social dimension within a virtual technical system. Mumford (1995) identified ST theory as being Suitable for computer-based work systems and for setting out alternative solutions in IS and ICT related issues.

Against this background, Thach and Woodman (1994) established that socio-technical basis can be customized to fit the social network of an organization. Similarly, Belinda and Brandis (2013) argue that the Socio-Technical Theory is a social network in which people (the social system) interact with each other through a virtual environment (the technical system). Chase and Susman (1986) support the use of ST theory to approach new design that could address a problem involving people and technology. Similarly, Bostrom and Heinen (1997) suggested that STS can be applied to MIS in solving IT related problems, including network security which the current research addressed with the STS.

The proposed model of the current research includes user's involvement and structural interactions for security collaborations. This design is contained in the STS theory as established by Steven (1997) that STS is the most widely conceptual and empirical work influencing employee involvement and activity design. Moreover, Hackman (1980) added that STS theory has the flexibility to be adopted with ease to almost any organizational situation. Similarly, Cherns (1986) identified the following guidelines for designing an

150

activity that is in conformity with organization's objective: that the activity design should lead to participatory process involving employees in the activity; and that the features necessary to implement the activity design should be described. This is inconformity with the current research that aimed at users' participations and their activities were specified in their respective structures and pattern of interactions.

   Similarly, Pasmore and Barko (1987) asset that employees performing similar tasks should be grouped together to facilitate sharing of information, knowledge and learning in sucha a way that bureaucratic processes are removed; thereby giving workers sense of responsibility and control in the discharge of their activities. This as well in conformity with the design of the proposed model of the current research where users were grouped according to ties (formal and informal) after being equipped with the necessary knowledge and skills, giving them the freedom of learning sharing and experiences security experiences on the platform of social media of FB.

   Similarly, the STS theory is flexible in approaching various issues, like that of security collaboration. This is supported by Cummings et al (1996) who state that implementation of STS theory is not limited to a stable work design, but it offers a continuous process to modify activities to fit changing conditions. Security issue is an evolving phenomenon and a counter measure that is proactive and real-time, such as the proposed model of the current research is the desirable fit to the evolving conditions. Thus fitting the STS theory in this regard and the STS theory justifies the framing of the proposed model. Similarly, Robbins (1994) found that organizational effectiveness was related to the "fit" between technology and structure.

   This is in conformity with the current research in which structural interactions was designed to fit virtual environment on the platform of the social media of FB, for security

collaborations. After framing the research in the sociotechnical system, yet again there is the need to provide another frame (called Blooms Taxonomy of learning) that could guide the learning process on the SNS model by the users, for successful implementation.

4.3   Theoretical Framing – The Socio-technical Theory (STS)

Socio-technical theory has proven to be a useful theoretical framework in blending people with technology for addressing organizational problems; or for solving a technical problem, through a social system and vice versa. In the field of IS and ICT, to which this research is situated, various scholars used ST theory to advance the thinking of the theory in their respective disciplines.

For example, Horton et al (2005) used sociotechnical to design human social arrangements with computers in organizational settings; Devarport (2008) used sociotechnical system to come up with IS and ICT framework within institutional condition; Day (2007) brought computing and sociology together, with the application of sociotechnical system; Scacchi (1982) used sociotechnical to develop a framework known as the web of computing, in which he described organizational computing as congruent to both technical and social elements.

Similarly, in the web of computing, sociotechnical system was advanced to STIN (Sociotechnical Interactions Networks) notably Kling (1987); McKlim (2003); and Kling et al (2003). Other researchers with sociotechnical frameworks include Wellman and Haythornthwaite (2002) on human-centric communication networks; and Monge and Contractor (2002).multimedia technologies and individuals; Participatory sociotechnical design of organizations and IS by Adam and Warren(2000); Al-Mudimigh et al (2000) with an integrated framework for software implementation; and sociotechnical perspectives in the implementation of emerging issues by Carayon et al (1997).

The focus of researches in ICT and IS has always been on the interactions of social and the technical systems of ICT. A number of scholar, notably, Cooper et al (1996); Carayon and Karsh (2000); Palvia et al (2001); have agreed that socio-technical system has been widely recognized as the pedagogical method for computer-based analysis, work design, diffusion of new technologies, and evaluation of information system.

The main principles of Socio-technical system are: Structure (people and relationships), and Technology (tasks, activities, and processes). This is contained in the sociotechnical schema as depicted in figure 27. Moreover, it is the doctrine of sociotechnical theory that all technologies that exist for everyday life settings could not be separated from the social settings. This is established by Kling (1980); Avgeror (2001); Walshan (1993); and Orlikowski (2000) that ICT, either by design and application, is aimed at improving, facilitating, and solving organizational issues.

In this regard, the implementation of a social media to create a virtual community, on one hand, and the embedment of users to participate and collaborate on the virtual community, on the other hand, is the approach adopted by this research, which is in line with the sociotechnical doctrine. The pillars that blend the sociotechnical are schematically presented in figure 27 by Bostrom et al (1997).

However, the principles were substituted with relevant constructs to the current research, without changing the meaning and philosophy of the sociotechnical principles in the schema. The views of the sociotechnical approach is that any design of a solution in an organization must aim to fit both the social and the technical system and that it is only through such joint optimization of the two systems that efficiency and successful implementation of a solution can best be achieved.

Figure 27: Schematic Representation of Sociotechnical doctrine
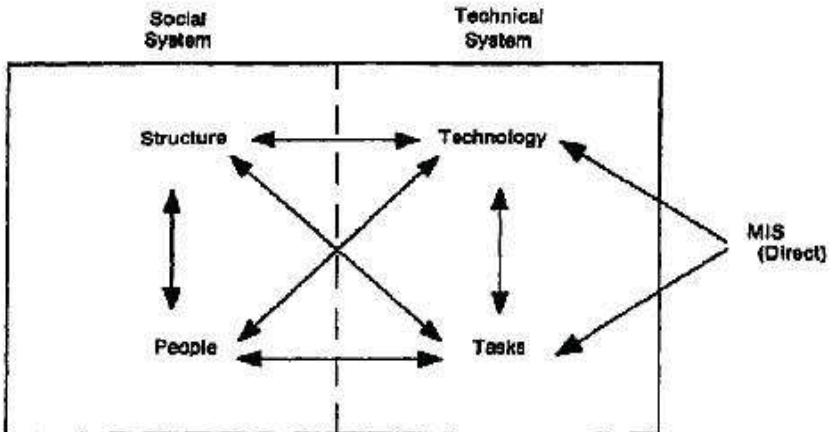
MIS Problems and Failures: A Socio-Technical Perspective. Bostrom, Robert P.; Heinen, J. Stephen. MIS Quarterly, Sep77, Vol. 1 Issue 3

4.4   The Bi-Forminal Ties (structure)

While figure 4.1 represents the original principles of the sociotechnical, the diagram that follows in figure 27 represent the modified socio-technical approach of the current study for addressing security issues in Wireless LAN by the users, for the users, and about the users of the Wireless LAN. As depicted in figure 4.2, one of the principles of soci-otechnical in the social system is group formations: self-managing, semiautonomous and autonomous groups. Since organization is a formal structure, a formal group with formal relationships was created and hereby named in this research as FORMAL TIE, to represent the formal or semiautonomous association. Similarly, in every organization or social set-tings, some individual would form relationships and interactions, based on certain ideolo-gies, interests, culture or related reasons.

Therefore this research provisioned the emergence and formation of such associa-tion and hereby named it as INFORMAL TIE. Thus, collaborations, participations, infor-

mation sharing, and social leaning is best achieved where the two ties exist and work hand-in-hand towards the common goal of security. Thus, the social system (of structure) in the sociotechnical was replaced, in this research, with Bi-forminal ties (the formal and informal ties). The emphasis of the sociotechnical theory is for people to have the capacity to be multi-structured, assign themselves into groups at will and within the prevailing circumstance.

This thesis used the Socio technical to structure users in groups on Biforminal-ties for collaborations on security on social media of Facebook. Emery and Trist (1965) found that productivity is greater where employees are structured in autonomous working groups. This is similar to the current research where the ties (formal and informal) were autonomous with little control or supervision in their social networking for security. Cummings (1981) assets that self-regulating group is one of the manor applications of ST theory. This is supported by Steven (1997), who assets that work groups is the basic building blocks for collaborative activity towards realization of the organization's objectives. Manz (1986) added that self-regulating groups are otherwise known as teams, self-leading or self-managing members, performing inter-related tasks towards common goal.

In the current research, the self-regulating groups are the formal and informal ties having autonomous interactions towards security collaborations with a sense of duty and responsibility. While self-managing teams are common in manufacturing settings, Steven (1997) argues that such team design is applicable to any situation where collaboration is required for improvement on a common goal. This has further justified the framing of the current research with the ST theory.

155

4.5   People in the Sociotechnical systems

Similarly, people (hereby in this research denominated as users) are pivotal for the deployment, usage, implementation and applications of technology. With the digitalization of office and organizational functions, today's workforce must reflect today's electronic office; in terms of ICT knowledge and skills. While majority of office workers are ICT literate, being the trustees of data and information, they must have some level of security knowledge and skills relevant to their human capability in order to actualize the trust; and thus maintain the confidentiality, integrity, and availability objectives of security.

This coincides with the assessment of workforce by David et al (2003) who asset that in today's workplace, employees must perform new roles that can protect their work from challenges that could render them off duty. The lack of network availability due to DoS attacks could halt jobs and render an employee off duty. The side of the social systems in the modified sociotechnical appeared in figure 5.2, schematically depicts the structure and people as discussed in the previous paragraphs.

The SNS based model of this research addressed SE based intrusion into Wireless LAN. The social system of ST theory aims to design a system that involves workers in an activity. Likewise in the SNS model users can identify and take countermeasures to SE threats and attacks on real-time.

A social system can be actualized as Harvery (1994) pointed out, through organization's communication patterns as well as through a network of social relationships. The current research used social networking to promote the communication patterns and the social interactions for security collaborations, with knowledge acquisition and competency as advocated in the ST theory by Pasmore and Barko (1987).

Figure 28: Modified Schematic Representation of Sociotechnical doctrine

Schematic Diagram of Socio Technical Theory:
modified to frame the study

Social System groups individuals into teams

Semiautonomous Group   Self-managing Group

Formal ties   **Informal ties**   *here modified to fit group formation in the Social Network*

Bi-forminal ties

Social Network reflects the Socio Technical system, where workers form relationship to interact within the (social system) in a virtual (technical system).

Social System	Technical System
Bi-forminal ties	Social Media
User Competencies *Knowledge base of IP in SE*	Social Networking

SNS
Social
Network
Security

4.6   Technical System (the social media)

Social media is akin to communication channel. It offers the platform and the facilities for users to communicate and interact virtually. The biggest shift since industrial revolution is the activities on the web, or the social media. Visiting social sites is now more popular online than checking personal email. Social media is the fast growing technology that revolutionizes, more significantly, the communication system. It proliferates in every part of human and organization's activities. For example, individuals and companies and organizations have FB profiles. Among the social media technologies, is the Facebook (FB).

The popularity, simplicity, and ease of use of social media of FB facilitate the engagements and collaboration of users to stimulating, real live debate and discussions,

157

thereby turning users into real live and proactive security intelligence. FB is the leader in the way people connect to one another and share information. If FB were a country, it would be the third largest country on the planet. It has more than 800 million active users. An average user spends not less than an hour every day on FB. Over five hundred thousand (500,000) businesses have a presence on FB. Access to FB is promoted with smartphones and other internet enabled BYOD (Bring Your Own Devices) at the workplace.

Organizations that are deeply and widely engaged in social media significantly surpass their peers in both revenue and profits. Since social media can actualize a so difficult task as revenue and profit increase, then it is an appropriate technology to deploy for security system that is for the users, by the users, and of the users. Thus sociotechnical system has offered us the insight to deploy this popular technology for a shift in organizational approach to security.

Thus, the technical system in the modified sociotechnical principles in figure 4.2 consists up of social media and social networking. There is significant attention on social media in sociotechnical researches. Researchers such as Monge and Contractor (2003) argued that social media is becoming the bringing (and platform) technology between people and interactions.

4.7   The Technical system (the social networking)

The tasks or activities under the technical system are hereby in this research modified to mean virtual activities (or social networking). This coincide with   sociotechnical researchers, Chaw and Chan (2008) who claimed that knowledge sharing as a fundamental premise of sociotechnical is effective and successful through social networking. This is also collaborated with the claim of Mumford (2000) who asserts that workforce tasks is increasing-

ly becoming virtually executed, online and real-time. Moreover, Castells (1996) argues that in the era of electronics of things, organizations are moving away from hierarchies to networks, and from paper based tasks to paperless tasks through networks. Similarly, Pasmore (1985) argues that work system should be seen as a set of activities contributing to an integrated whole and not a set of individual jobs. Although this assertion was made long before the arrival of social networking, but one can deduce that it implicitly advocating networking system for tasks execution. This has justified the adaptation of social networking as tasks users should engage for security affairs on their network.

Ravi (2009) sees socio-technical as interactions involving individuals interacting with (a) *technologies,* and (b) *other individuals.”* Social networking uses virtual community on a social media to connect users together for interactions, debate, discussions and learning on security issues. This is made possible through the facilities of the social media of posts, comments, like, sharing, blogs, and instant messaging. With the facts that tasks are becoming networked, processed and disseminated, then incorporating social networking for security (as an added user task), is an appropriate simplified adaptation. That is why some organizations have an intranet system for communications and collaborations for tasks execution. Thus, the social networking tasks contribute to creation of contents and knowledge, which is one of the key tenets of the sociotechnical system.

4.8   Blooms Taxonomy of Learning

The relevance of using Blooms taxonomy of learning in this research is because for the subjects of the study to be able to identify and prevent social engineering threats and attacks in the implementation of the proposed SNS based model, the following domains must be involved:

d. Imparting of knowledge;

e. Developing of skills;

f. Developing of competencies;

The applications of the above three domains are suitable and appropriate with the blooms taxonomy of learning. Blooms Taxonomy of learning is a classification of learning levels that maps the way learning is designed and information is processed. Thus it is the categorization of learning objectives and goals in the course of imparting knowledge to learners. It was proposed in 1956 by team of educational psychologists led by Benjamin Blooms; and it was revised by Anderson (2001).

Bloom was an American educational psychologist who made influences to the classification of educational learning objectives and to the concept of mastering learning. Blooms divided the educational learning objectives into three areas or domains: Cognitive, Affective, and Psychomotor. The goal of Blooms' Taxonomy is to motivate educators to focus on all the three domains while preparing the learner for a more functional education. The cognitive domain is divided into six categories or layers, with each layer presenting increasing complexity: Remembering, Understanding, Applying, Analyzing, Evaluating, and Creating.

Figure 29: Bloom's Taxonomy used to implement the SNS model

Cognitive Domain	Affective Domain	Psychomotor Domain
Remembering	Receiving	Perception
Undersanding	Responding	Set
Application	Valuing	Guided Response
Analysis	Organizing	Mechanism
Evaluating	Characterizing	Overt Response
Creating		Origination

KNOWLEDGE	ATTITUDE	SKILLS

USER SECURITY COMPETENCE - PREVENT INTRUSION
(Identify/Counteracts - threats & attacks)
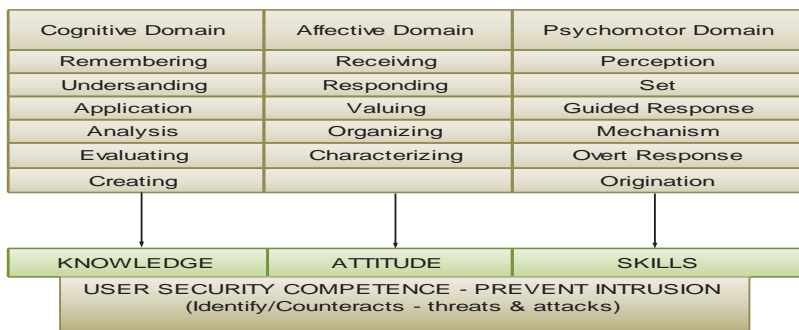
These levels are arranged in hierarchy from lower level to the higher and more complex, as depicted in figure 29. Remembering is maintaining basic knowledge through root learning or memorization. Understanding is the ability to restate the information in one's own words by constructing meaningful ideas explanations that make sense. Application requires the learner to put into use what has been learned in the previous levels. Application is the ability of the learner to make connections to prior knowledge in order to solve a problem. It involves transfer of abstract ideas into practical situations.

Analyzing is the ability to break the knowledge into components so as to illustrate relationships to one another in order to recognize unstated assumptions and identify relevance information. Evaluating is the ability of the learner to judge, criticize or assess information using current or prior knowledge so as to make decisions and support one's ideas or concepts. It encompasses critical thinking with profound understanding of specific concepts or discipline. Creating is the highest level in which learner combines the learning elements to form a coherent or functional knowledge. Creating requires learner's originality in thought and inventiveness. This is the highest level that brings all previous level together for theorizing, designing, and testing knowledge or concepts.

The Blooms Cognitive domain is applied by an orderly and systematic follow of the six categories with examples in each category on how each level should be implemented. Table 12 is the exact replica of the Bloosm's table of cognitive domain, with the terminologies and wordings modified to fit the current research. Sousa (2006) established that Bloom's Taxonomy is widely known and accepted pedagogical taxonomy, and is widely applicable to any discipline that aims at developing an individual in a particular discipline.

Table 10: Bloom's Taxonomy for Intrusion Prevention User Competencies

Category	Example and Key Words (verbs)
Knowledge. Recall Knowledge of Security domains: Tricks and Techniques of Social Engineering	Examples: Recite security goals. Quote online and offline various forms of tricks and techniques. Know the threats signs and behaviours. Define key terms: Malware, phishing and other related terms and the types under each; and Memorize the steps and process of both online and offline SE. Key Words: arranges, defines, describes, identifies, knows, labels, lists, matches, names, outlines, recalls, recognizes, reproduces, selects, states.
Comprehension: Understand the meaning, translation, interpolation, and interpretation of instructions and problems. State a problem in one's own words.	Examples: Rewrites the types of SE. Explain in one's own words the steps for performing user manipulations both online and offline. Translates online and offline anomalies into SE approach. Explain how various SE tricks and techniques work, and attempt to give your own types of examples with countermeasures. *Key Words: comprehends, converts, defends, distinguishes, estimates, explains, extends, generalizes, gives an example,* infers, interprets, paraphrases, predicts, rewrites, summarizes, and translates.
Application: Use a concept in a new situation or unprompted use of an abstraction. Applies what was learned in the classroom into novel situations in the work place; surfing the web and other online-offline encounters.	Examples: Use prior knowledge to identify and prevent suspicious requests both online and offline. Apply human factor authentication to evaluate the genuine of access requests by online and offline objects. Show how you can identify both online and offline SE tricks and use the same instances in different websites and online encounters. Key Words: applies, changes, computes, constructs, demonstrates, discovers, manipulates, modifies, operates, predicts, prepares, produces, relates, shows, solves, uses.
Analysis: Separates suspicious anomalies from genuine behaviours in web browsers, websites, and social networking sites from normal and expected behaviours and distinguish the variations in each.	Examples: Troubleshoot a potential threat by using logical deduction. Recognize logical fallacies in reasoning. Gathers information from ties and differentiate your analysis. Key Words: analyzes, breaks down, compares, contrasts, and diagrams, deconstructs, differentiates, discriminates, distinguishes, identifies, illustrates, infers, outlines, relates, selects, and separates.
Synthesis: Builds a structure or pattern from divergent views, social learning, and prior knowledge. Put parts together to form a whole, with emphasis on creating a new meaning or structure from the whole experience, blogs, posts or comments.	Examples: post, share and discuss experience and encounters. Take action or recommend immediate stpes. Integrates ideas from several sources to solve a problem. Revises and process to improve the outcome. Key Words: categorizes, combines, compiles, composes, creates, devises, designs, explains, generates, modifies, organizes, plans, rearranges, reconstructs, relates, reorganizes, revises, rewrites, summarizes, tells, writes.
Evaluation: Make judgments about the value of ideas or materials encountered, received, or discovered in the virtual community.	Examples: Select the most effective solution. Apply and implement the chosen solution. Explain, share and justify your action. Key Words: appraises, compares, concludes, contrasts, criticizes, critiques, defends, describes, discriminates, evaluates, explains, interprets, justifies, relates, and summarizes, supports.

Adapted from Anderson et al (2001)

4.9   Conclusion

In developing the proposed SNS based model with its implementation strategy, the research draws largely upon the Sociotechnical theory; and modified by substitution, the constructs of the theory in order to fit the socio-technical design of the current research. In addition, the Bloom's Taxonomy of learning was followed in developing the subjects of the research, on the use, application and implementation of the proposed model. Numerous scholars have outlined the way sociotechnical principles can be implemented. Albert Cherns (1976) enunciated a set of sociotechnical design principles and these were updated by Chris (2000) to encompass the new Internet based ICT. The current research used the doctrines of sociotechnical system to design, conduct and implement the proposed SNS based model.

CHAPTER 5:   The SNS based Model

5.1   Introduction

A model is a representation of something that describes a blueprint relevant for the achievement or attainment of a purpose or project. Steinmuler (1993) defines a model as information on something with contents and meaning, created by someone (the sender), for somebody (the receiver), and for some purpose (usage context). Thomas (2005) defines model as a description of something; and Bezivin (2001) defines model as "simplification of a system built with an intended goal in mind. The model should be able to answer questions in place of the actual system." Irrespective of the terminologies used to define a model, one thing is clear that a model is like a roadmap to execute or achieve a goal on specific issue or phenomenon.

The uniqueness of this model is that it does not focus only on security approach, but it enhances and improves security; secondly, it is not a copy of an existing security model. Thus, it is not the outcome of a choice among models, nor an extension of a particular security model. It was created (through sociotechnical framework). Thirdly, it was tested through an experiment (with experimental and control groups) and found to have served the purpose it was created. Thus, the proposed model of this research was aimed at developing Wireless LAN users with knowledge, skills, and competencies that would enable them to identify and prevent intrusion (threats and attacks) that are based on social engineering, through a collaborative system of social networking on the platform of social media of FB. The interdependency of the technical aspect and the social aspect of an organization is desirable for successful implementation of a system or model that address organizational problem on security issues.

5.2   Network and Information Security Goal and Objectives

Security is all about protecting assets (data and physical) from threats and attacks by intruders (persons and objects). All security issues are built on CIA triads: Confidentiality, Integrity, and Availability. These three fundamental security pillars could not be achieved without a user who is knowledgeable and skillful in the escalating rate of social engineering threats and attacks. The user is often described as the weakest link to security controls as a result of user lacking the functional knowledge and skills in the current trend of attacks through social engineering. Any or all of the CIA triads can be compromised through the user. The SNS model serves as a foundation for the CIA triads on user platform.

Figure 30: The CIA Triads
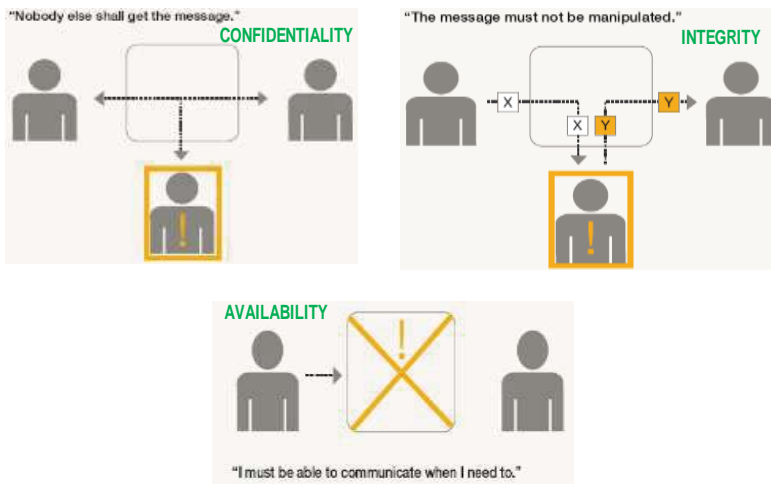
Confidentiality refers to secrecy of data at input, process or transmission levels. The user must ensure that at the input stage, data either electronically or through conversations with

colleagues, is not disclosed to unauthorized person either by responding to online requests or through eavesdropping in conversation. Allowing unauthorized person to access sensitive information and the network or its resources, amounts to intrusion; and any attempt to deny access amount to preventing the intrusion. Most users, because an application sounds good, without authenticating its source and credentials, click "OK" almost every time a user is warned that "this application can use the internet to track your locations, utilize other phone and data resources." A user may click a link or open a mail attachment and such actions are similar to granting indirect access to information to unauthorized person. The unguided and rampant use of BYOD in the workplace also contributes to confidentiality compromise.

Such devices like iTouch, and iPad, bring malware into the network; and through these devices, sensitive data is stolen or leaked. Apple admits that there is no way to guarantee an iTouch or iPhone does not contain malware. Google also admit there is no way to guarantee an Adroid application does not contain malware; and Blackberry devices have 9 known CVEs (Common Vulnerabilities and Exposure).

Integrity refers to safeguarding the accuracy and completeness of information in the input, process, storage, and transmission sessions in such a way that the information is not modified, changed, altered, deleted, or substituted. A user allowing unauthorized person or objects to spoof information and network resources is by that action allowing intrusion; the knowledge of spoofing and applying the knowledge to safeguard the network is prevention against intrusion. A user filling online form requested by an unsolicited source or downloading free software and applications, may as well compromise the integrity of the network resources.

Availability refers to the accessibility of the information and network resources when and at the time requested, with minimum delay, and with service reliability. The opposite of these issues is referred to as Denial of service. It includes Account lockout, CPU resource consumption, Buffer Overflows and improper packet handling. In today's digital office, where interactions and job processing are electronically performed, delay and service time out may lead to job stoppage. This may in turn bring a lot of consequences some of which may not be bearable to an organization. Thus reliable and uninterrupted connectivity is crucial to the survival and efficiency of today's e-of-things organizations.

There are some malwares that occupies the system resources of the user or the whole network system. These types of malware activate only with the intervention of the user. Attempt to activate them by clicking a pop-up window means facilitating the intrusion; and knowledge of them and timely application of the knowledge means preventing the intrusion. The availability of connectivity means the survival of the organization, and the survival of the organization means job protection, and job protection means user being security protective and thus needs the application of the SNS model so as to protect the network resources from being compromised.

5.3 Overview of the SNS model

The way a burglar follows to break into a physical system is quite the same way a hacker follows to exploit and attack information and network resources. The only difference is that a burglar uses physical means whereas a hacker uses bits and bytes. However, with the sophistication of the technical solutions to security and successful exploitation becoming harder, threats and attacks evolved to a social system known as Social Engineering (SE). the model is designed not only to provide insights into the methods used to break

into a network system, but also aimed at developing Wireless LAN users who are proactive in security:

- Users who anticipate security breaches and understand how they are caused.

- Users, who can on real-time, report, share and take action on what appears suspicious or wrong on their network and physical Wireless infrastructures.

- Users who are conscious of potential threats on their network infrastructure and suggest improvements on security issues and share their experience and knowledge on the SNS model.

- Users, who can intelligently monitor, observe, respond, and control situations that seem to compromise the security objectives of the CIA.

- Users who consider ownership in security, thereby considering security of the users, by the users, and for the users with sense of accountability.

- A model that engage users to take responsibility of protecting their Wireless LAN so that security is of the users, for the users, and by the users so that human vulnerabilities to exploit are blocked or kept to minimum.

Figure 31 is the diagrammatic presentation of the SNS based model. The model is designed to ensure that security was collaborated in such a way and manner that any suspected object, event or process, whether offline or online, was reported, alerted and exposed on real time, on the social network. Users were made to be vigilant and alert, using their visual and sensory on people, process and activities. Every user was made to understand that he/she is a node and attacking him/she (a node) means attacking all the nodes in the network. Just like a node (PC) infected by virus in the network system, infects other nodes (PCs). The user was also made to understand that protecting the network and information resources is a responsibility that is linked to job security and survival of the organization.

This was further emphasized by making user to understand that compromising the security objectives of the network and information resources implies attacking the reputation, survival and existence of the organization, which is crucial and important to the user's job security, professional growth and development. With this introduction, the Bloom's Taxonomy of learning was applied in exposing the components of the model to the participants – the experimental group.

The model is socio-technical both in its structure and application. It was created from the socio-technical perspective to develop security skillful users who can learn on real-time through the social networking platform, to identify SE threats and attacks; and collaborate on real-time to counteracts the SE based threats and attacks. Thus it serves as complement to the automated, software and technical security controls. Figure 5.2 depicts the schematic diagram of the model with the subsequent sections explain each part of the model.

Figure 31: The SNS based Mode: diagrammatic presentation
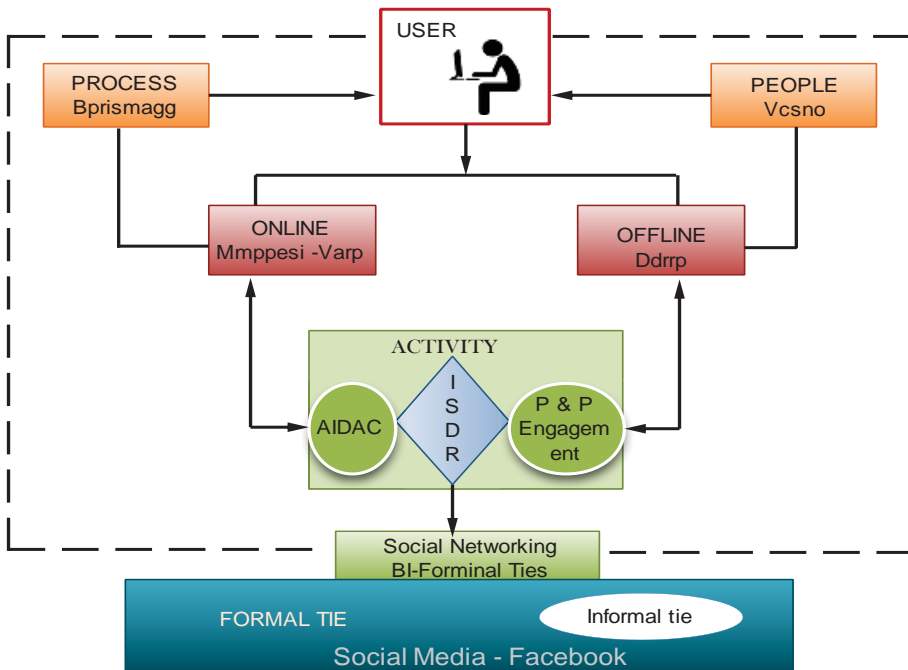
As can be seen in the SNS model, the user is confronted in the front with processes that expose him/her to online social engineering based threats and attacks. It is the same at the back of the user. The only difference is that while in the front interactions is with computing devices, the interaction at the back is with people (or potential social engineers). The subsequent sections describe the each of the segments in the SNS model.

5.4   The User: A Component of Wireless LAN

As a result of digitalization and expansions of office functions and activities, wireless networks are increasingly deployed in organizations. Wireless is the type of communication that takes place over the air. People and devices can communicate with each other through electromagnetic waves, which include radio waves, infrared waves, microwaves,

visible light, ultraviolet rays, and gamma-rays. The proliferation of Wireless LAN is rapidly replacing the wired networks, due to low costs, conveniences, and increase in employee productivity.

Wireless LAN genetically called WiFi that provides higher data speed within a building, campus, or environment of an organization. It is license within the spectrum of the Wireless LAN. With the original specifications of IEEE 802.11, it improved in data rate/speed of 54 Mbps and presently goes up to 1.3Gbps; and within the frequency of 2.4 GHz and now 5.5GHz is also used.

The concern of this research is on Wireless LAN Infrastructure type. The infrastructure type is made up of: The radio signal, the client devices, the access point, and the user. Yet again, the user is the concern of the current research. The infrastructure mode is depicted in figure 5.3 below.

Figure 32: Wireless LAN Infrastructure type
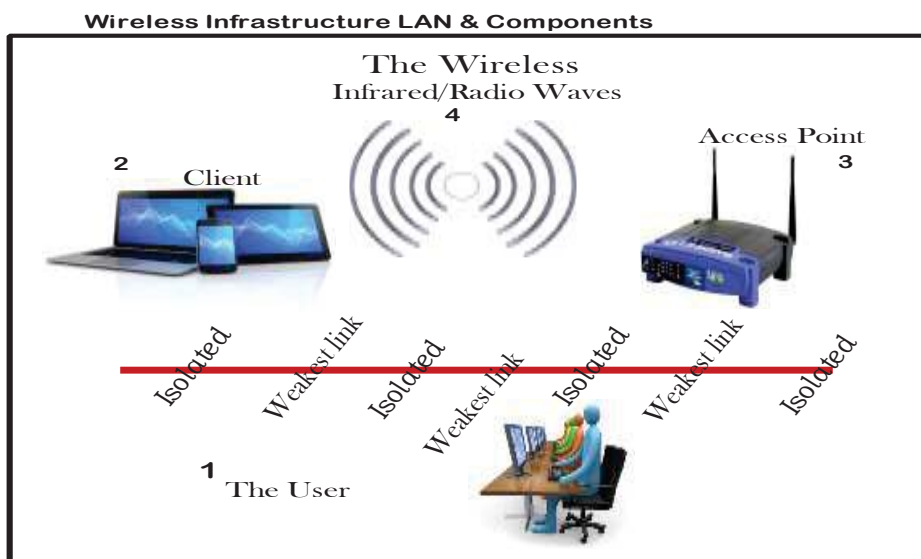
In all the components of the Wireless LAN, user is the weakest link, not the technology. Who clicks the links? Who interacts with the systems? Who uses smartphones, notebooks, with unencrypted data? Who uses the most popular passwords (easy to remember)? All the answers are the user. Security starts at the childhood with basic instructions by parents and elders on the does and don'ts for environmental safety and hazards.

Unfortunately, as a person matures and submerged into job activities, security at the workplace become a relegated and a "not my concern" issue. User should have the security habits and knowledge of threats, vulnerabilities and mitigating controls. The previous and current paragraphs exposed the participants to why the user should implement the model; and the subsequent paragraphs described what they should implement and how they should implement the model. Lack of desirable user security system, exposes the user and the organization to various threats and attacks that are based on social engineering, both offline and online. If the user understands the implications and what is critical as per network and information security is, the user can do the best to protect himself, his job, and his/her organization from the SE based attacks.

5.5 The Process (Bprismagg) Segment of the Model

The process refers to the interactions the user has with various elements in the course of input, process, storage, and transmissions of data and information on the system and over the network. Thus in the process of browsing, phone calls, registrations, social networking, installations, messaging, gaming and device operations, the user come across various threats and attacks. Each of these has certain peculiarities that user can observe and detect some abnormalities that could be a threat or attack. The browser could be displaying unwanted toolbars, redirecting the user to another website slightly different from the one re-

quested, strange Google search results may appear; system hanging, slowing and flashing a warning of infection.

Through phone calls determined attacker informs a victim that there is an infection on the system. For example, the hacker may ask the victim to confirm the infection by locating a file on the system. After brief explanation of how to locate the file, the victim soon located the file and the hacker repeat the name of the file and immediately the victim confirmed the correctness of the long file name. Then the hacker confirmed the infection; whereas the file was common systems file that every computer has. Another example may be where the attacker asks the victim to download a program to provide remote access to the victim's system.

Similarly, in the process of online registrations of any kind and filling application forms, various kinds of information are required. The information provided may be used for unknown purposes that may compromise privacy. At the end of the registrations, terms of agreement bottom must be checked for the registration to continue. This implies that any purpose to which the information was utilized was with the consent of the user. Likewise in the installation of some programs and software, which is often a daily routine among users in today's software assisted tasks. Here again user has to accept to incomprehensible and longer terms of use over which the user has no control.

Through instant messaging, various forms of social engineering take place which in most cases are unknown to the user. Instant messaging (IM) is a software application that enables interactions with others on user's device, just like texting messages on the cell phone. There are many IM services and providers like AIM, Yahoo, talk, icq, and Microsoft messenger. Most of these applications are not secured. They are open means of

communication, sending plain text without encryption. The contents can be intercepted and read by anyone monitoring the user's traffic as it moves across the internet.

In the process of playing online games, users encounter social engineering, in most cases unknown to the user. Apart from social networking, online game is highly social and popular way of pastime and entertainments. Most of the social attacks through gaming are downloading driven. Most of the information passed and shared on the online game is plain text, without encryption.

A lot of tricks are exercised by hackers to convince or lure user into downloading some software that enhances the game experience, or a user may reach a thrilling part of the game, but would not proceed without downloading some code or components of the game that would complete the thrilling part. Online games often interact with the user's privacy and in the process, Trojan, phishing, infections, spyware, adware, and malicious software are installed on the user's machine.

Figure 33: Social Engineering in Action
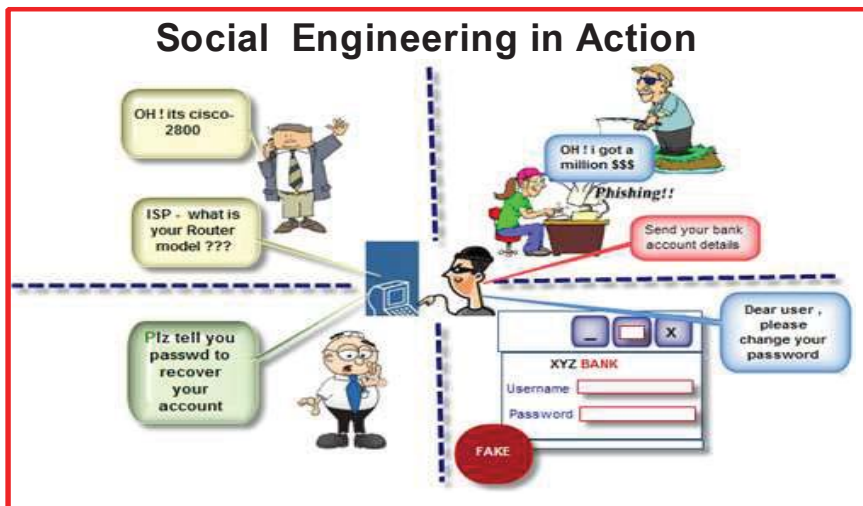
Similarly, through the process of social networking, users encounter various forms of tricks that deceive them in being proxy attackers. Thus with the increasing popularity of social networking, hackers write malware programs and rely on users to spread and install the malware. Hackers convince the user to install the application and the motive is identifying theft and spread of malware. On the Facebook there are various applications that may look interesting, appealing, and enticing user.

For example, there is an application that invites the user to see the number of people that have visited his/her profile. At the current time on Facebook, there is no application that offers such services. This type of application once installed by the user, it will send directed messages to user's friends inviting them to install similar application. The application will continuously send messages to its creators about the online activities of the victims that installed it. The information collected will be used to spoof the profiles of user's friends to launch targeted attacks.

5.6   The People (Vcsno) segment of the model

The user is a social being who cannot run away from interactions with various categories and caliber of people in the course of discharging day to day office functions. People come to user's workplace with different motives and intentions. While some motives are good and favourable, some motives are bad and unfavourable. In today's world of electronic dependency, hackers using social engineering may physically appear before a user and attempt to take advantage of user vulnerabilities in human attributes so as to obtain sensitive information; or manipulate user in doing something that can provide access to the attacker in the network and information resources of the organization. An understanding of peoples' motives of interactions is a step forward to identifying and preventing social engineering based threats and attacks.

Among the categories of people that interact with the user on a daily basis are Visitors, Casual workers, Service Professionals, Neighborhood, Impersonated colleague. Each of these classes of people may represent a social engineer in disguise. The previous sections have explained how the user can encounter social engineering both from the front and the back aspects of his/her work interactions. This therefore leads to the two forms of social engineering: online and offline, which are described as the next segments of the SNS model.

5.7   The Online-Offline SE threats and attacks

Social engineering refers to the manipulation of computer user through tricks and techniques in order to obtain information from the user, or to cause the user to do something on behalf of the person or objects putting the request. Thus hackers and attackers use tricks, disguise, and persuasion to deceive computer user to assist in gaining illegal access or the use of computer and network resources, through online confrontation or personal interactions. The online social engineering are the various manipulations the user encounters while using the computing devices (including the OS, the browser, and the network services). The offline social engineering are the various manipulations the user encounters with determined attackers in the day to day discharge of official functions. Figure 34 depicts the classification of SE.

Figure 34: offline online social engineering
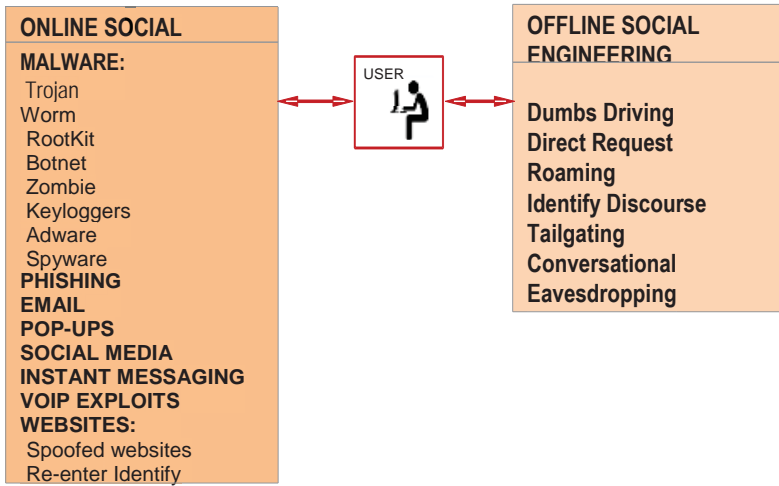
Figure 34 depicts the two classifications of social engineering confronting the user both in the computing activities and the social interactions. Each of the elements in the online SE is attempting to gain illegal access to the network and information resources through the user. Instead of spending a tedious process and long time trying to crack into a security system, hackers nowadays use the wetware or the human elements to launch attacks. User is vulnerable and can be compromised. No matter how secure a system is, there is always a way to breakthrough. The human elements of the system are the easiest to manipulate and deceive. Social engineering is the creation of panic, using influence, manipulation tactics, or causing feelings of trust are all methods used to compromise the victim. The social engineer always attempts to get the trust of the victim or throw a fear in the victim. The user is deceived by hackers through malware social engineering. Figure 35 describes how hackers use the user to activate malware.

Figure 35: social engineering malware
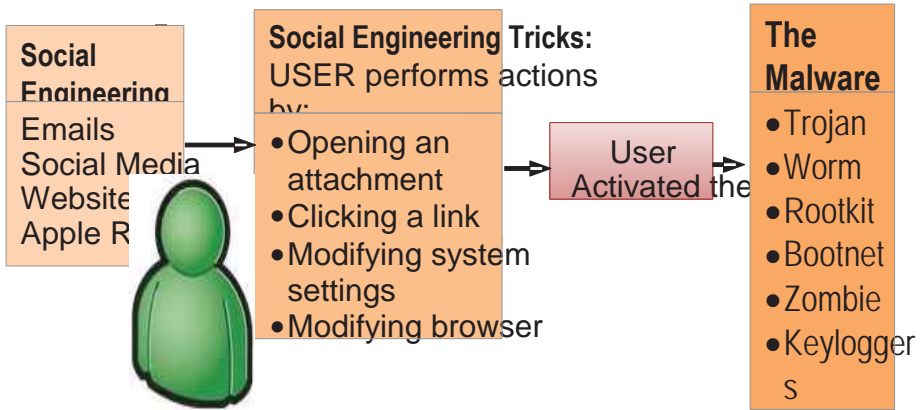
Malware are blended threats of malicious software written to cause havoc and compromise the security system. Each malware is designed to cause a specific havoc. For example, a virus is designed to infect files on the disk and can spread autonomously from device to device. However, the action is triggered by the user opening an infected email attachment. Similarly, email worms require the action of the user in order to spread. A Trojan masquerade as a useful program and the user may go ahead download them with that expectation, whereas they are meant to cause havoc and compromise security.

A user visiting a compromised webpage can also be infected with a Trojan referred to as drive by download. Keyloggers records every key pressed with the aim of finding out the user's password, login details, and other sensitive information. Botnet is used by cyber-criminals by combining the functionalities of virus, worms, and Trojans to launch denial of service attacks. The user's computer may be a victim that is connected with several infected computers thereby forming a network of infected computers. The network will be sending spam emails in thousands thereby causing distributed denial of service attack (DDoS),

perhaps on the user's network or organization. Adware is software attached with adver-

tisement and it is driven by download and installation of software. Adware often has em-

bedded spyware that tracks and monitors user's online activities and also forward user's

computer files to its creator. Adware always displays unsolicited advertisements on the

user's screen and modify the start page of the web browser thereby making it difficult to

change in the normal browser settings.

5.8   Other elements in the online SE

The other components of the online social engineering are:

- Malicious Websites
- Pop-ups
- Phishing
- Emails
- Social Media
- VoIP Exploits
- Pharming

Malicious websites are sites that have either been compromised or designed to spread mali-

cious contents. Legitimate sites that have been hacked are also used to spread malware. A

site can be mimicked or modified to lure the user into interacting with the site with confi-

dence. The knowledge of mimicking a website was exposed to the user because websites

has been the gateway for accessing and interacting with online resources. The following

descriptions of URL and spoofing techniques reveal how a user can easily be deceived.

Figure 36: URL name indicator
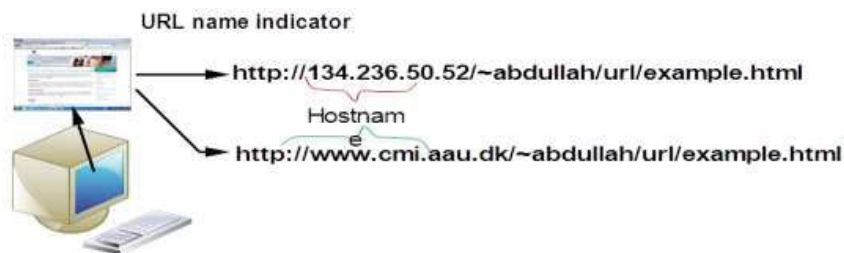
While the user only knows the website name by letters, the system only knows the website by numbers, or the IP address. However, every computer or the local network has what is called DNS: Domain Name Server that translates the letters to numbers and vice versa, for the convenience and application of both the user and the system. In short it maps the domain names to IP address. Social engineers use DNS hacking to direct users to unsolicited website. If a user type in the domain name, instead of going to the actual website, the user is then directed to hacker's website (similar to the requested website).

Phishing attack is then executed by deceiving the user into typing username and password, which would return with an error message; whereas the details have been captured. The user may also be redirected to a website that loads user's computer with spyware, adware, keyloggers, etc. As the user types a domain name, the keeps on looking for the domain name resolution, first from the host file, then the local DNS and finally to the public DNS. Therefore once the host file is changed, through malicious software asking the user to install or run on his computer, it can then modify the host file to redirect the user to the determined site; or a user may click a link on a website, and the link may contains malicious scripts that will add all the bogus websites on the user's computer. Clicking the "Yes" bottom, automatically changes the host file. The subjects of the experiment in this research were exposed to this type of deception.

5.9 Website spoofing

Users often receive an email, or while browsing come across unsolicited message requiring urgent attention by login onto a website; where a link is conveniently provided for the user to click. The motive is to redirect the user to a similar website to extract or track user's online activities. Most users, unknown to this trick, go ahead to click the link and ended up giving away surname and passwords. Users are deceived into trusting a website by hiding

the contents of the spoofed website through various techniques. Irrespective of the techniques used, the user can humanly check for spoofing attacks through the status bar matching. Thus, on the left bottom corner of the screen, there is a little status bar area that is usually blank; but when a mouse is hovers on a link, the actual site the link will take the user, is revealed. If does not match with the clickable link, then a spoof attack is obvious.

Spoofed anchor

In HTML, a href indicates the subsequent page to go on clicking a hyperlink. For example, in the two links below, the second link is supposed to be the genuine link, but when the user click on it, the page takes the user to site in the first link.

 www.abdullah.com

Moreover, anything that comes before the @ symbol in a URL, browser overlooks it. For example, www.abdullah.com@wwwmusa.com: the second page after the @ is the page the browser will recognize. Similarly, one or more letters may be changed in such a way that may not be easy for the victim to detect the bogus website. For example, www.abdullahi.com, may be modified to look: www.abdullahl.com. Users who are not able to identify and recognize the deception in the website address, may fall victim to the deception. The experimental group was exposed to this type of deception.

Bogus SSL certificate

For secure HTTP connection, SSL (Service Socket Layer) is used for information encryption and identification. Thus, HTTPS is Hypertext Transfer Protocol Secure. Encryption and Identification are the most significant attributes of SSL. Bothe the browser and the web server rely on SSL to create secure channel for communication over the internet. However, hackers create both their own HTTPS and Certificate, to lure user into trusting a website intended to collect sensitive information from the user. Figures 37 and 38 respectively

show how user who is conscious of the security lock is deceived by the bogus padlock icon.

Figure 37: Browser padlock

Browsers Padlock security indicator
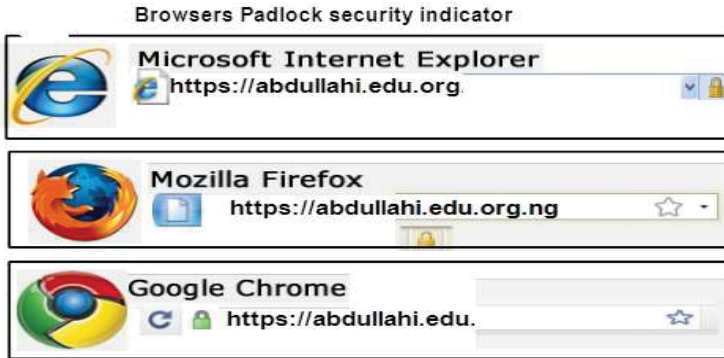
Figure 38: Padlock and HTTPS security indicator

Padlock & HTTPS security indicators

The user who knows the padlock icon, on seeing it, has a calm posture mentally created. A user connects to a secure site, some security features appear in some parts of the browser. A clocked icon appears in the status bar of IE; and the web address must start with HTTPS. The digital certificate is sent to the user's browser, which checks the validity of the certificate in its settings. If the certificate is not valid, the browser raises an alarm, but due to user security habit, such an alarm may not be taken seriously. What users must know is that the appearance of security pad lock is not an indication that the website is not malicious. The idea is that the padlock means that the communication is done on secure channel.

5.10 Pop-up Windows

Pop-up is a graphical user interface that appears in small window and is used in social en-
gineering to deceive users into installing malware either by clicking the window bottom or
attempting to cancel the pop-up window. The best way to get rid of them without activating
their hidden contents is to close them by using the "Red X" in the top right corner, as
shown in figure 39

Figure 39: Pop-up threats

However, some pup-ups appear with double red X or a "fake red X" to trick the user into
clicking the wrong one. The outer red X should be the one to click. The trick is shown
below in figure 40. In the day-to-day interactions with online activities, users cannot avoid
encoutners with pop-up windows. The exposure of users to pop-ups windows is ideal for
user knowledge and skills in the indetification and prevention of social engineering based
threats and attacks.

Figure 40: Double Red X deception

Double Red X deception

However, some pop-ups hide the Red X by turning to grey so as to prevent the user from using it. This is evident in figure 41.

Figure 41: Greyed Red X

Greyed Red X

In this case, the user can open Taks Manager (Ctrl-Alt-Del) and select "Application" then click and end the offending browser window. Sometimes it may warrant going to the process to close the browser completely. Other examples of pop-ups that deceive user to perform some actions for malicious purposese are depicted in figure 42.

Figure 42: Various pop-ups demanding user action

Some pop-ups deceive the user with an offer, but conditioned to provide personal information before proceeding to the rest part of the offer. Similarly, some sites issue a message on pop-ups that before using their resources (videos, musics, software, or documents), the user must install a software, and the pop-up will urge the user to "click to install", messate. The trick is to install adware, spyware, or keylogger on the user's machine.

5.11 Phishing

Phishing is the second name for social engineering. Phishing is very much like eavesdropping, but in electronics form. Receipt of electronic mails or message from unexpected sources may be a trick to get the user to disclose personal or other sensitive information. Thus a hacker is casting his net hoping the fish (the user) to take the bite and respond. Many phishing messages and related sites not only attempt to get sensitive information, they may also attempt to install malicious code on the user's devices.

5.12 emails

e-mail, an electronic mail, is the most common and popular means of communication for both individuals and orgnizagtions in today's electronic and digital society. Similarly email

is one of the most commonly used methods by criminals to lauch an attack on information and network resources. Phishing and emai attacks go hand in hand because the contents of the email is conined in such a way that the user is so enticed that he/she may not reist the temtation of responding to the message, clicking the link or opening the attachement. The exposure of the subjects of the experiment to email phishing is necessary because email is one of the most favourite attack vector used by hackers in deceiving users to comply and compromise security objectives of confidentiality, integrity and availability.

Figure 43: Email social engineering

Emails are cleverly crypted to trap the user into performing actions advantageous to attacker but disastrous to the user, the organization and the network resources. Emai being the easiest and convenience way to communicate is incrasingly facing various forms of attacks targeted at the user. Figure 43 show more examples of targerted email attacks. The more information a hacker is able to obtain from determined targets, the easier it is to hack the network and information resources of an organization. Email is one of the easiest and best ways of getting information from victims by hackers.

The phishing emails sent by hackers ask for username and password, or direct the victim to a phishing website. Email phishing is favourable hackers' tool for it is very easy

to attack hundreds of thousands victims at a go. The script can be tied to email database so that it can keep on looping throughout the script, sending emails to everyone. Thus email phishing attempt to trick users into revealing username and password either of their network login or profile account on credit card. The obvious signs of phishing emails include unanimous salutation (dear account holder) and the clickable link in the email is not corresponding with the URL on the bottom of the browser. Table 13 shows the different kinds of tones used by hackers to lure users into believing the mail and demand immediate action from the user.

Table 11: Phishing emails

Wadwa, Semrin [semrin.wadwa@starwoodhotels.com] Actions 31 October 2013 19:47 Your Account Will be Closed Within 24 Hours. This is to inform you that your mailbox has exceeds its storage limit, you will be unable to receive and send emails. To re-set your Account Space on our database, prior to maintain your INBOX from 20G to 20.9G. CLICK HERE to Activate. CLICK HERE <https://mail.aau.dk/owa/redir.aspx?C=_18oENzqH0qCNZNh6Ph9m2tcvdwbqtAI_rW6bsXcMI4UlkDdyHmWqiVyvDOrEGQw2SY9IXrI-2w.&URL=http%3a%2f%2fsocial.eng4u.cn%2f%2femailupgrade%2f> Warm Regards, System Administrator. This electronic message transmission contains information from the Company that may be proprietary, confidential and/or privileged. The information is intended only for the use of the individual(s) or entity named above. If you are not the intended recipient, be aware that any disclosure, copying or distribution or use of the contents of this information is prohibited. If you have received this electronic transmission in error, please notify the sender immediately by replying to the address listed in the "From:" field.	From: XXXXXXXXXXXXXXX Date: Wed, Sep19, 2013 To: XXXXXXXXXXXXXXXXSubject: Commercial Litigation Subpoena Through this document we hereby inform you of the Litigation process started by XXXXXX Marketing LLC against the company you represent. You are required to produce the originals of all docu-ments and other items which are responsive, in whole or in part, to any description set forth in this "Subpoena Schedule," regardless of where located, that are in your possession, custody, or control, or in the possession, custody or control of any of your partners, associates, employees, agents, representatives, accountants, or attor-neys, along with all copies of any such document which differ from the original by virtue of any addition, deletion, alteration, notation, or inscription on any part of the document, includ-ing its back. The complete list of the required documents can be found at: <http://www.officialarticles.com/subpoena_files/> as well as the number of the complaint against your company placed for copyright infringement on 12.21.2010 by the legal representative of XXXXXX Marketing LLC. Failure to produce and present the requested documents can display in fines dictated by the court. XXXXX XXXXXXX Senior Attorney XXXXXXX Law

CLICK HERE<http://aucoinduluth.com/2/adminupgrades-/>
IT Service Des
2013.
This electronic message transmission contains information from the Company that may be proprietary, confidential and/or privileged. The information is intended only for the use of the individual(s) or entity named above. If you are not the intended recipient, be aware that any disclosure, copying or distribution or use of the contents of this information is prohibited. If you have received this electronic transmission in error, please notify the sender immediately by replying to the address listed in the "From:" field.

One obvious sign users can use to verify the genuines of the email is to hover the mouse over the link, and if the link name does not match with the expected receipient sending the email, then it may be a phishing email. Malicious attachements, fake links, and benefits/threats are the common attributes of phinsing emails.

5.13 Social networking

Users frequent more of social media sites than they log into their emails. Social media of facebook enhances and facilitate virtual communication among people of common interest. The media is rich with enticing communication channels, such as chat, instant messaging, posts, comments, likes, vieo and photo sharing. This makes the amount of inforamtion shared on the media to be enoumous. Thus, exposing the user to data mining by criminals who would use the harvested information to intrude into personal privacy and lauch various forms of attacks. Morever, social networking websites provide applications developed by different parties in order to provide better entertainment and more funcions for usrs. However, most of th applications are developed by vicious attackers. Users who exucute the applications will fall victims of various malware attacks. Impersonation and profile spoofing is also common in social networking media thereby using the channel to send spam messages as traps. A sppofed Facebook page may also ask user to adjust privacy settings, and also a comment may appear from a known friend with a request to click a URL for an enticing story or video.

5.14 The AIDAC Component

Social engineers, whether knowingly or unknowingly, use the AIDAC principles to per-suade, convince, and manipulate users to comply with their requests. The letters means: Attention, Interest, Desire, Action, and Compliance. Attention is anything that draws the

eyes and the cognitive perception, be it on the website, telephone call, email, or pop-ups. This follows with an interest that evokes the emotions of the user for the necessity of the message. That is followed by desire which is an appeal to the emotions of the user pointing a benefit or threats for the user. The Action then elicits prompt action in the user to click, sing up, open an attachment, or respond to the request. The compliance then committed user to do other further things that if not done the benefits or threats may actualized or the threats may not be subverted. Thus, AIDAC is a powerful communication tool that per-suades, convince, and emotionally provoke a target to take positive action regarding the message's content. A thorough analysis of social engineering message contains all or com-binations of the AIDAC formula. Figure 5.5 is the graphical presentation of the AIDAC principles.

Figure 44: Social Engineering AIDAC Identification Clue

The user can compare the content of the message encountered with any of the elements of the principles to determine an attempt of manipulation. Although marketing and advertising companies use the AIDA principles often, it is easy for the user to know if the persuasion is customer based.

5.15 The Offline Ddrrpp

As social engineering takes place online, so also offline. The most common elements in the offline SE are: Dumps driving, Direct request, Road apple, Roaming about, and Prompt rescue. In dumps driving, the determined criminal search for any leading information in the trash of the office or organizations; or deliberately throwing, within the premises, pamphlets and fake flyers that contain enticing offers on some websites. Road apple is also similar to dumps driving where a malware laden USB or any removable media is left unattended in the most frequently visited area of the organization. A person may confront a user with direct request for computing and network services.

The person may appear in an impersonated character. For example wearing a suite may trigger the thought to assume an important personality; and since the thought have been conditioned that way, any request by the hacker may not be likely rejected. Similarly, a social engineer may be roaming about the premises and even attempt to gain access to restricted areas through Tailgating, which is following an authorized person too closer through a restricted area to avoid security scrutinizing. Three things are the target of such a roamer social engineer: a user to engage in psychological maneuvering, an unattended device, and eavesdropping to gather sensitive information. Eavesdropping is another means a social engineer can obtain information that can be used to access network resources. Users must be aware of the environment in which conversation is taking place and who is around the environment. In the offline SE, the operation must be quick and immediate; as such a

direct request without giving the victim a thought of reflection or rejection of the request advanced to the user.

5.16   Personal and Professional engagements

For the offline SE to be successfully executed, the social engineering is either on the platform of personal or professional engagements. The personal engagement is where the attacker initiated and engaged the user into personal interactions through remarks and utterances that are similar to the ones listed in Table 5.3. The professional engagement is also similar to the personal engagements but differs in the style of the interactions with authoritative and businesslike manners. A social engineer may come in the personality of a distinguished figure in professional field; say pretending to be one of the Microsoft regional agent, or IT hardware technical specialist from a fictitious company or organization. Assuming the role of professional engagement is brief and requests the victim to hasten in meeting the demands of the impostor.

Table 12: SE – Personal and Professional Engagement

PERSONAL ENGAGEMENT *The Friendly Approach*	PROFESSIONAL ENGAGEMENT *WITH AUTHORITY*
• 1st to Give instant recognition • Giving Compliment (Flattery & Appreciation), making the target feels important • Asking Simple questions • Looking helpless and creating an atmosphere of coming to his/her rescue • Encouraging the target to say more about himself, environment, current affairs or situations. • Showing interest in what is of importance to the target. • Creating a relaxed atmosphere with a sense of Humor • Artificial Glamour, to create liking • **Pretexting - Creating a fake scenario**	• **Trappings of Role** • **Credibility** • **Alter casting (forcing the target into a role)** • **Distracting from Systematic Thinking** • **Momentum of Compliance (one more thing)** • **Glamorization** • **Attribution** • **Propaganda and Fear (hostility situation)** • **Reactance** • **Familiarity Exploit**

The user equipped with the knowledge of the two approaches to offline SE engagements, can easily identify and prevent the threats and the attack from happening.

5.17 Socio-Technical Balance in Security

The argument that security has both a social system and a technical system has been well advanced. Social networking is revolutionizing all aspects of human and enterprise activities. In an increasing, globalized and digital world, embracing social networking into the workplace for a particular interest is not just a nice frill, but a necessity. As more and more workers are joining social networks, enterprise must turn such trend to opportunity and advantage.

Social Networking brings people together through a platform of social media, for the purpose of interactions, participations and engagement on various issues and activities.

It is a form of virtual relationship. Social Networking is not new in the history of human socializations. Since the early existence of human beings on earth, people have been coming together to participate and contribute on issues that are of concern and importance to them. An individual is naturally a social being. Any form of technology or opportunity that offers social engagement to people is embraced and uphold with enthusiasm and delight.

Figure 45: Facebook Social network platform

Although FB is not the only social media, however its popularity and vulnerability to social engineering threats and attacks make it the suitable platform for the implementation of the model of this research. Similarly, the Facebook platform under which social networking is conducted is easier, simple, well known and popular among users in the computing world. The platform was made up of two groups named as Formal tie and Informal tie. The formal tie was actual employees with roles and responsibilities, officially recognized by the organizational structure.

However, only those participants of the research in the experimental group were considered as the formal tie. In the formal ties, relationships and interactions exist based on culture and personal interest. Hence the members were asked to voluntarily create one additional group to be named as the Informal ties. A member in the formal ties can as well be a member of the Informal ties, depending on personal preferences and choice of a member.

Each of the two ties share information, experiences, and security encounters both online and offline on real time.

5.18 The Contributions of this Thesis

This thesis has contributed to theory and knowledge as follows:

a) Modification of the Socio-technical theory to include social networking for optimization of both technology and people (users) to collaborate on security issues. The modification is clearly seen in Chapter 4: **Figure 31**

b) Introduced, implemented, and tested SNS based model and was found to be effective in developing users, who can on real-time, learn security skills on one hand and on the other hand collaborate on security controls in their organization. Thus, the model was able to create a security system that is of the users, for the users and by the users, in the identification and prevention of social engineering threats and attacks on their network and information resources. The SNS model appeared in pages 160 – 186 of chapter 5.

c) Contributed to Network and Information security through the implemented and testing the SNS in an organization (in University setting), and result was found to be effective in the prevention of social engineering based intrusion on Wireless LAN in an organization. The complete SNS model is depicted in Chapter 5: **Figure 27**

d) Added to the understanding of Social engineering tricks and techniques through AIDAC strategy, which does not exist in the literature of Social engineering, hitherto to this study. AIDAC appeared in Chapter 5: **Figure 5.7**

e) Contributed to the proper understanding of social engineering threats and attacks for both on line and offline user interactions, by the addition of professional and personal engagements, which does not exist in literature, prior to this study.

f) Contributed to Technical security skills in the literature of social engineering with the introduction of Human Factor Authentication system as shown below (**Figure 46).**

Figure 46: Human Factor Authentication
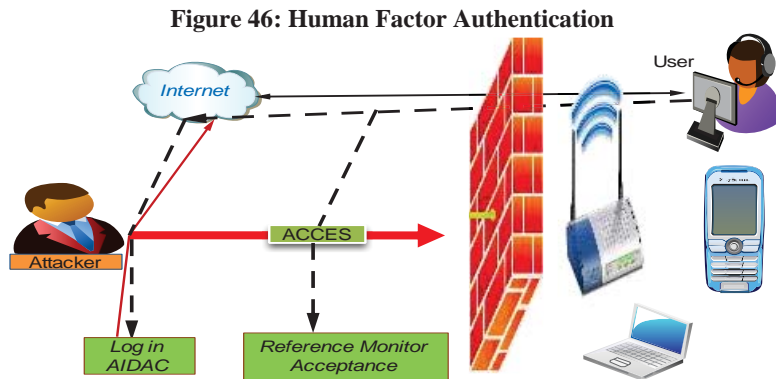
g) *Contributed to the proposal of extending the popular CIA triads to include Css (Cyber security skills). Thus, CIA plus Css shall be pronounced "SAYAS." (CIA-Css). In today's digital society and electronic organizations, the actualization of the CIA triads could not be attainable without a user who is knowledgeable and skillful in cyber security skills. The absence of such a user could lead to compromising the CIA triads.*

h) *Contributed to the development of a framework for teaching and learning cyber security skills specific to user-centred and social engineering. The continued bias showed to social system of security, or user negligence, is one of the factors promoting threats and attacks in social engineering. The SNS model address this bias and could serve as a reference re-source for the development of curriculum and frameworks for teaching and learning social engineering based cyber security skills.*

5.19 Summary

The socio technical system originated from work organization, emphasizing the optimization of both the technical system and the social system for efficiency and better work performance. The digitalization of works coupled with e-of-things has made network and internet resources vital tools and materials for the modern day workforce. For better work performance and higher productivity, availability of network services must be maintained through mechanism for denial of service (DoS) attacks; and the data/information creation, processing and dissemination must be confidential through authentication. Similarly, the integrity of the data/information must be protected through encryption.

Thus the control to the CIA (Confidentiality, Integrity, and Availability) of network and Information resources is inclined to favour the technical control. Thus, the users (the social system) of the network and information resources are not optimized with the technical control for a balanced security system. The socio technical system is used by this research as a framework to provide a system of security that is socio-technical, in which both the technical control and the social systems are optimized for better security. As shown in figure 4.1, the constructs of the socio-technical system was modified to substitute a social networking platform that provides users with the technical skills for collaboration on security.

Thus, as users continuously interact with technology for the day-to-day discharge of organizational tasks, users should equally, on a social network platform, continue to acquire the knowledge, skills, and competences necessary for real-time identification and prevention of threats and attacks obstructing effective job performance and productivity.

Humanism and technology must be linked in order to provide a balanced system of security with the socio-technical system of security augmenting automated/software system

of security. The views of the sociotechnical approach is that any design of a solution in an organization must aim to fit both the social and the technical system and that it is only through such joint optimization of the two systems that efficiency and successful implementation of a solution can best be achieved. Albert Cherns (1976) enunciated a set of sociotechnical design principles and these were updated by Chris (2000) to encompass the new Internet based ICT.

5.20 Conclusion

This chapter identified and described socio-technical theory as the suitable framework for this research. The description and analysis of how the theory fit the research was provided. Bloom's taxonomy of learning was described and adopted as teaching-learning strategy for exposing the participants to the SNS model. The schematic diagram of the model was presented, and each part was described and explained. An implication for each segment of the model in social engineering was highlighted. The traditional way of securing the WLAN is the head of Network security or security administrator installing and putting in place all the vital software and policies that could protect the network from virus, threats and attacks. With the expansion of office activities and the digitalization of office functions, the number of hardware and software tools used in the office is as well increasing. This adds up to the existing numerous and tedious work of security on the IT office, thereby causing administrative and cognitive overloads. The consequences of this is that certain vital aspects of security tasks may be missed or overlooked, like updates, patches, monitoring and analysis.

The argument that security has both a social system and a technical system has been well advanced. Social networking is revolutionizing all aspects of human and enterprise activities. In an increasing, globalized and digital world, embracing social networking into

the workplace for a particular interest is not just a nice frill, but a necessity. As more and more workers are joining social networks, enterprise must turn such trend to opportunity and advantage. Hackers and cybercriminals are taking advantage of social networking to practice their trade through online social engineering.

Paying scrupulous attention to turning social networking to an opportunity will be a significant way for enterprise to fight escalating attacks on WLAN.The way a burglar follows to break into a physical system is quite the same way a hacker follows to exploit and attack information and network resources.

The only difference is that a burglar uses physical means whereas a hacker uses bits and bytes. However, with the sophistication of the technical solutions to security, threats and attacks evolved to a social system known as Social Engineering (SE). The SNS based model develops Wireless LAN users who are proactive in security:

- Users who anticipate security breaches and understand how they are caused.
- Users, who can on real-time, report, share and take action on what appears suspicious or wrong on their network and physical Wireless infrastructures.
- Users who are conscious of potential threats on their network infrastructure and suggest improvements on security issues and share their experience and knowledge on the SNS model.
- Users, who can intelligently monitor, observe, respond, and control situations that seem to compromise the security objectives of the CIA.
- A model that engaged users to take responsibility of protecting their Wireless LAN so that security is of the users, for the users, and by the users so that human vulnerabilities to exploit are blocked or kept to minimum.
- Users who can see, detect, and take appropriate action on real-time and prompt.

- Users who regard the network and information resources as vital raw material for the discharge of their day-to-day functions.

- Users who actively responsible for protecting their network and information resources from being compromised in Confidentiality, Integrity, and Availability.

CHAPTER 6: Empirical Presentation of Findings
(Data Presentation, Analysis and Discussions on Findings)

6.1 Introduction

While using the Wireless LAN of an organization to visit web sites and the internet, users encounter unknown social engineering threats and attacks that compromise their network and information resources. The SNS model imparted the knowledge of social engineering threats and attack only to the experimental group of the study. They were tested together with their counterparts – the control group, on how to identify and prevent social engineering based threats and attacks. The test covered both online real-time activities and offline environmental activities. The subjects were also tested on how they use the social media of Facebook as a platform for counteracting the threats and attacks, through non-compliance to the social engineering threats. Similarly, the subjects were tested on using the social network platform to report, discuss, share and inform the social network about suspicious events and threats experiences. The test scores were computed statistically to test the hypotheses of the research. The activity of the users on the social media platform of Facebook was also analyzed qualitatively and interpreted so as to give meaning to the implication of the activities.

Thus, this chapter is not repeating the research methodology and the designed used in data collection. However it is focuses on the examination of the collected data with a view to establishing meaning towards testing the hypotheses and answering the research question. In this regard, the analysis of the data is in two phases. In the first phase, the data collected through the experiment were analyzed quantitatively. In the quantitative analysis, the statistical results of the data were pronounced and described to prove the various hy-

potheses postulated in chapter one of this research. The results of each variable tested were presented in tables, graphs, and followed by textual descriptions. In the second phase the data collected on the implementation of the model on the platform of social media of FB was analyzed using affinity diagram. In other words, the attitudes of the participants were assessed from their activities on their respective groups. These activities are wall posts, comments, likes, and sharing.

Therefore, this chapter is structured to accomplish the following stages:

The quantitative part of this chapter was first addressed as thus:

- The results of the processed raw data was presented in tables and graphs;

- The results were analyzed by statistical interpretations and textual explanations;

- Implications of the findings to the objectives of the study were briefly mentioned and expounded in the section of the discussions on findings.

The qualitative part of this chapter was addressed as thus:

- The raw data was presented in tables and diagrams;

- The data was described and explained textually;

- The data was interpreted diagrammatically, using empirical findings in the literature review of chapter two, to support the interpretations.

- The interpretations, discussions on findings and implications of the findings to the research objectives as stated in chapter, were concurrently discussed.

The discussions on findings

- Discussing the revelation of the findings;

- Relating the findings to similar empirical results, so as to validate the findings of the current research; chapter two – the literature review was used to find similar results that support findings in the current research;

- Discuss the implications of the findings with the stated objectives in chapter one.

6.2 Data Collection

Data collection refers to the application of the research design to obtain information focusing on the research question. To answer the research question of this study, the first part of research question required quantitative data and the second part of the research question required qualitative data. Therefore the first phase of this research used pre-test/post-test design to collect the data, which was an interval/ratio data type. After the experimental group was exposed to the SNS model, both the experimental and control groups were tested and the scores of the test were put to statistical analysis for testing the hypotheses of the research. The quantitative data was used to compare the two groups of the study on the independent variable to determine its impact on the dependent variable. The t-test of independent sample was used to analyze the test scores of the participants.

On the other hand, the second part of the research question was answered through qualitative data. Qualitative data was collected from social media of Facebook, which was the platform used to implement the SNS model. Thus, Content analysis was the method used to collect the data. Content analysis is a research technique for the systematic classification and description of communication content according to predetermined categories (Wright, 1986). The predetermined categories were the Facebook functionalities of post, comment, share, and like that were examined and extracted the behavior of the participants on what they were posting, what and how they were commenting; what they were sharing

and how they were sharing; and the interpretation of the liking mode of the participants. Appropriate codes, themes, categories, and patterns were identified with the involvement of five coders thereby establishing the reliability of the qualitative data.

6.3   Data Analysis

Raw data is meaningless and carries no sense for understanding and using it to make decision. Data analysis is the process of establishing meaning and making sense out of the raw data leading to a logical conclusion and dependable decision. Although there are different ways and procedures for data analysis, yet irrespective of such differences, the type of data (quantitative or qualitative) will determine the appropriate procedure to follow.

The procedure used to analyze the quantitative data involved statistical test, which are tools that distinguish between chance results and results that cannot be associated with chance. One of such statistical test is the t-test, which was used by this research to analyze the quantitative data. Details for the choice of t-test for this research are found in chapter three (methodology).

On the other hand, the qualitative data of this research were results of content analysis of social media of Facebook, which was the platform used to implement the SNS model. The procedure used to analyze and/or understand the qualitative data involved assigning code, theme and seeking pattern on the subject matter of the SNS model, under the platform of the social media of Facebook. Thus, qualitative analyzing and/or understanding the content followed the format below:

Table 13: Example of the coding pattern

Text/image	Code	Theme
Statement, context, image, or acknowledgement posted, commented, shared or liked.	**Label** to an information extracted from text/image	Unifying idea that is a recurrent element. Is sets of 'like' information

Five coders were involved in arriving to reliability and validity was achieved through consistency checks of data reduction. Details of coding procedures and reliability/validity are found in the methodology, chapter three. The results obtained were presented in diagrams and tables. Analytical induction coupled with literature review was used to interpret the result through discovering patterns and sequence of events. Patterns were identified through intensity, direction and process of interactions.

The pattern for the presentation and analysis of the quantitative data analysis is as follows:

- *Statistical/graphical presentation and analysis of the overall Pretest performance for both the Experimental and the Control groups;*
- *Statistical analysis of the dependent variables in the pretests of the Experimental group;*
- *Statistical/graphical presentation and analysis of the Experimental group Pretest-Posttest overall performance;*
- *Statistical analysis of the dependent variables of the Experimental group on the pretest-Posttest performance;*
- *Statistical/graphical presentation and analysis of the Control group pretest-Posttest overall performance*
- *Statistical analysis on the dependent variables of the Control group pretest-Posttest performance;*
- *Statistical and graphical presentation and analysis of both the Experimental and the Control groups on the Posttest performance.*

6.4   The Variables Tested at the Pre-test

The following six variables were used in testing the two groups at the pre-test level.

1. Ability to distinguish between genuine and fake:

    - Pop-up Windows
    - Emails
    - Window messages
    - Websites
    - URLs
    - Advertisements
    - Software offers
2. Ability to humanly authenticate authorized object or person attempting to access the Wireless LAN or its environments and infrastructures.
3. Ability to take countermeasures to anomalies or suspicious events.
4. Ability to use the formal structure to interact and collaborate on security issues.
5. Ability to use the informal structure to interact and collaborate on security issues.

6. Ability to use social networking on the platform of Facebook to collaborate on security issues.

6.5   The Variables Tested at the Post-test

The variables tested are: the ability to identify both online and offline social engineering based tricks and techniques; how to humanly authenticate online and offline encounters that are potentially a threat or an attack; ability to prevent and take countermeasures for potential and identified tricks and attacks; ability to interact with formal tie for sharing and collaboration on security issues; ability to interact with informal ties for sharing and collaboration on security issues; ability to use social networking on Facebook platform to collaborate with formal and informal ties on security issues. Performance in any of these variables implies the ability to identify and prevent social engineering based threats and attacks on the Wireless LAN.

Table 14: Summary of t-test analysis of Experimental and Control groups on overall Pretest on the identification and prevention of SE based threats and attacks.

PRETEST	N	M	SD	t-value	
				Calculated Value	Table Value .05
Experimental	40	9.15	2.248	0.98	1.664
Control	40	9.65	2.315		

Table 16 presents the mean score of experimental group as 9.15 and 9.65 for the control group. The calculated t value was less than the critical t value at 0.05 level of significance. Therefore, there is no significance difference between the two groups in terms of the over-

all performance in the use of knowledge of the model to identify and prevent social engi-
neering based threats and attacks. This shows that the two groups are almost equal as can
be seen in the bar graph below:

Figure 47: Overall Pretest Results

Figure 47: Overall Pretest Results
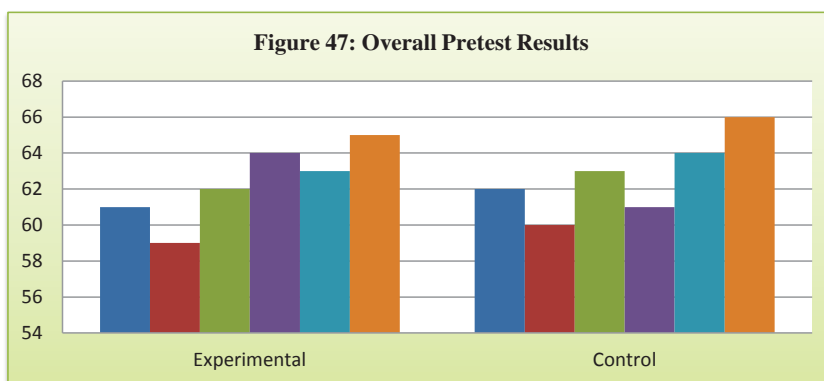
The six bars represent the variables tested in the two groups. The variables tested are high-
lighted in section 6. 4. As can be seen in the bar graph, the performances of the two groups
is almost similar. While they differ slightly in some of the variables, statistics revealed that
such variation was not significance. Thus, the two groups are statistically qualified to be
used for an experimental design which applies to the current research.

**Table 15: Summary of t-test analysis on Pretest – tricks and techniques of social engi-
neering based threats and attacks.**

PRETEST	N	M	SD	t-value	
				Calculated Value	Table Value .05
Experimental	40	1.525	0.751	0.26	1.664
Control	40	1.575	0.931		

Table 17 shows the results of the knowledge of social engineering based tricks and techniques as highlighted in section 6.4. The mean score of the experimental group was 1.525 and that of the control group was 1.575. The calculated t value was 0.26 which is less than the critical t value of 1.664 at the significance level of 0.05.

Therefore, there is no significance difference between the two groups in terms of knowing the tricks and techniques of social engineering. This shows that the two groups are almost equal in terms of the knowledge tested, as can be seen in the bar graph below:

Figure 48: SE Tricks and Techniques
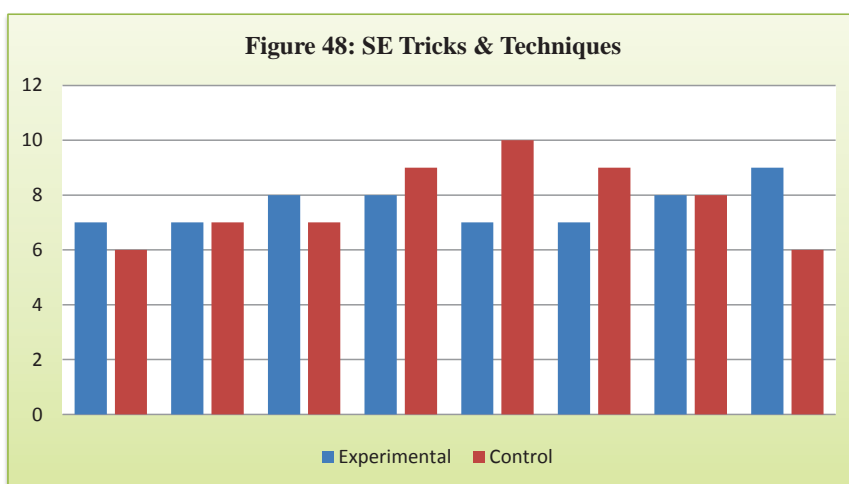
The bar graph in figure 48 clearly revealed that as per the test result on SE Tricks and Techniques, the two groups are almost equal. Although the performance of the groups differ in some of the variables, the overall statistical analysis as described in table 17 revealed no significance difference between the two groups.

Thus, the two groups deserved the condition of being appropriate for the experiment. The next analysis is on the human authentication mode.

Table 16: Human Factor Authentication Mode

PRETEST	N	M	SD	t-value	
				Calculated Value	Table Value .05
Experimental	40	1.475	0.640	0.30	1.664
Control	40	1.525	0.847		

Table 18 shows the result of the two groups on the test of human factor authentication mode. The mean score of the experimental group was 1.475 and that of the control group was 1.525. The calculated t value was 0.30 which is less than the critical t value of 1.664 at the significance level of 0.05. Therefore, there is no significance difference between the two groups in terms of the knowledge tested. The two groups are said to be equal as can be seen in the bar graph of figure 49. Thus, the ability of the subjects to distinguish between genuine request and fake request through clickable links and URL has really demonstrated the effectiveness of the model in having users authenticate web contents before committing and accepting any request and terms.

Figure 49: Human Factor Authentication

Figure 49: Human Factor Authentication
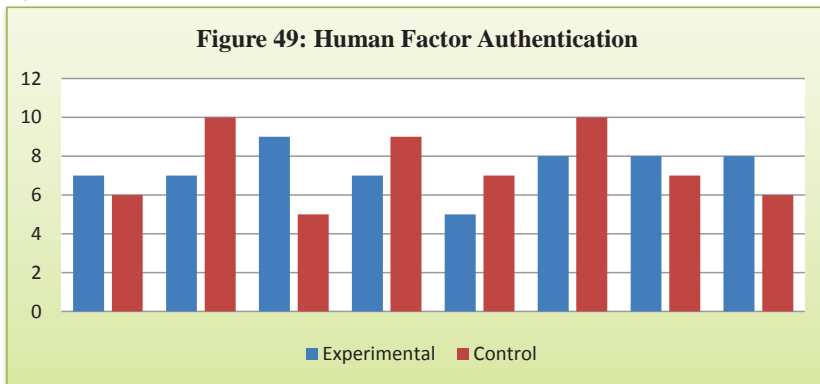
It is obvious from the graph in figure 49 that the two groups are almost equal as per their performance in the test of Human Factor Authentication. The two groups are said to be equal in terms of variable tested (human factor authentication mode); and therefore considered suitable and qualified for the experiment.

Table 17: Summary of t-test analysis on Pretest – countermeasures to SE based threats and attacks

PRETEST	N	M	SD	t-value	
				Calculated Value	Table Value 0.5
Experimental	40	1.375	0.847	0.29	1.664
Control	40	1.625	0.903		

Table 19 shows the result of the two groups on the test of knowledge of social engineering threats and attacks. The mean score of the experimental group was 1.375 and that of the control group was 1.625. The calculated t value was 0.29, which is less than the critical t value of 1.664 at the significance level of 0.05. Therefore, there is no significance difference between the two groups in terms of the knowledge tested, as can be seen in the bar graph below:

Figure 50: Counter Measures to SE based Threats and Attacks
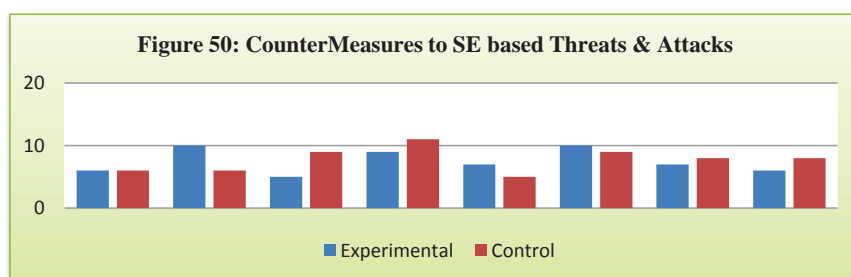
It is obvious from the graph in figure 50 that the two groups are almost equal as per their performance in the test of counter measures to social engineering threats and attacks. Thus, no one group is said to be superior to the other in terms of such knowledge; thereby satisfying the condition of equality for participation in the experiment.

Table 18: Summary of t-test analysis on Pretest – Formal tie connection

PRETEST	N	M	SD	t-value	
				Calculated Value	Table Value .05
Experimental	40	1.55	0.628	0.35	1.664
Control	40	1.625	0.011		

Table 20 shows the result of the two groups on the test of sharing experience on strong tie connection. The mean score of the experimental group was 1.55 and that of the control group was 1.625. The calculated t value was 0.35, which is less than the critical t value of 1.644 at the significance level of 0.05.

Therefore, there is no significance difference between the two groups in terms of sharing experience on strong tie connection. This shows that the two groups are almost equal in terms of the knowledge tested. The groups are said to be equal as can be seen in the bar graph below:

Figure 51: Formal Tie Connection

Figure 51: Formal Tie connection
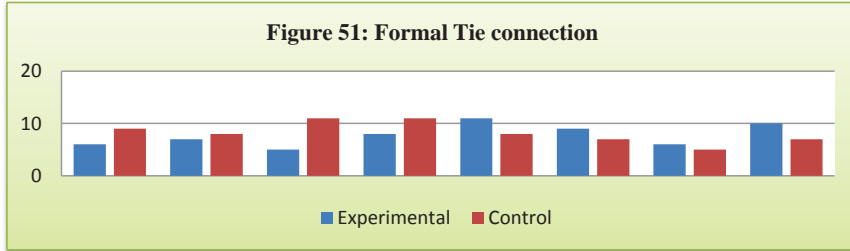
It is obvious from the graph in figure 51 that the two groups are almost equal as per their performance in the test of social networking security collaborations with formal tie connection. Thus, no one group is said to be superior to the other in terms of such capability; thereby establishing equality in performance in terms of the variable measured. This indicates compliance to the conventional way of interactions in an organization that is facilitated through formal organizational structure.

Table 19: Summary of t-test analysis on Pretest – Informal tie connection

	N	M	SD	t-value	
PRETEST				Calculated Value	Table Value .05
Experimental	40	1.5	0.736		
Control	40	1.65	0.816	0.80	1.664

Table 21 shows the result of the two groups on the test of sharing experience on weak tie connection. The mean score of the experimental group was 1.525 and that of the control group was 1.65. The calculated t value was 0.80 which is less than the critical t value of 1.664 at the significance level of 0.05. Therefore, there is no significance difference between the two groups in terms of sharing experience on weak tie connection; thus two

groups are almost equal in terms of the knowledge tested. This is obvious in the bar graph

below:

Figure 52: Informal Tie Connection
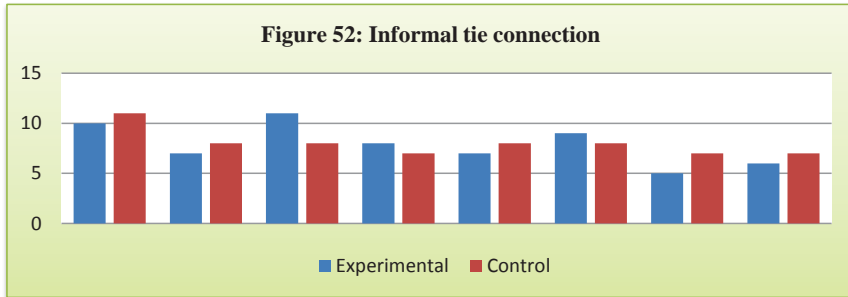
It is obvious from the graph in figure 52 that the two groups are almost equal as per their

performance in the test of social networking security collaboration with informal tie con-

nection. Thus, no one group is said to be superior to the other in terms of the variable tested

on the ability to use formal tie interaction to share and collaborate on security issues. The

equality in performance is desirable for achieving the validity of the research findings. The

pre-test results served as a measure to determine the extent to which any change that oc-

curred at the end of the post test is attributed to the treatment to the experimental group. In

this research, the treatment is the SNS model exposed to the experimental group.

Table 20: Summary of t-test analysis on Pretest – Using Facebook functionalities for security Collaborations

	N	M	SD	t-value	
PRETEST				Calculated Value	Table Value .05
Experimental	40	1.5	0.736		
Control	40	1.65	0.816	0.80	1.664

Table 22 shows the result of the two groups on the test of knowledge of using Facebook functionalities for security collaborations. The mean score of the experimental group was 1. 5 and that of the control group was 1.65. The calculated t value was 0.80 which is less than the critical t value of 1.664 at the significance level of 0.05. Therefore, there is no significance difference between the two groups in terms of knowledge of the knowledge tested; thus the two groups are almost equal in terms of the knowledge tested.

Figure 53: Facebook functionalities

Figure 53: Facebook Functionalities
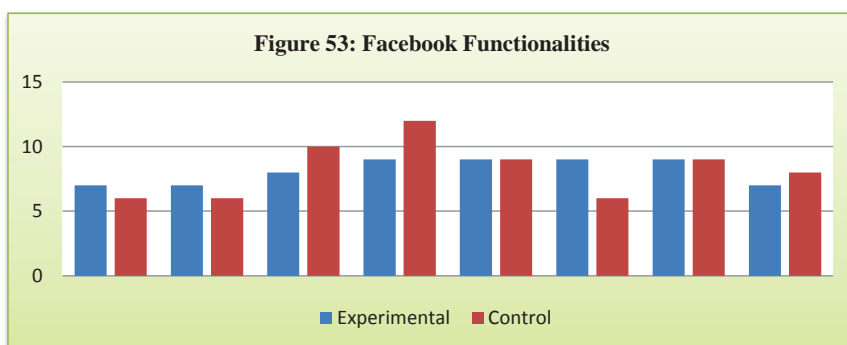
It is obvious from the graph in figure 53 that the two groups are almost equal as per their performance in the test of the use of FB functionalities to identify, prevent and collaborate for SE based threats and attacks on the platform of FB. Thus, no one group is said to be superior to the other in terms of such capability; thereby establishing the equality in performance as per the variable tested. This further revealed that any changes occurred at the end of the posttest is attributable to the treatment given to the experimental group.

6.6 Experimental Group t-test analysis on Pretest and Posttest

The analysis that follows shows the t-test of the Experimental group on both pre-test and posttest. Table 23 and Figure 24 below, represent and display the findings on the research hypothesis 1:

H0: there is no significance difference in the performance scores of the subjects exposed to the SNS based Model in the identification and prevention of social engineering based intrusion on WLAN and those subjects who were not exposed to the SNS based Model.

H1: *the subjects exposed to the SNS based Model perform better in the identification and prevention of social engineering based intrusion on WLAN than those subjects who were not exposed to the SNS based Model.*

Table 21: Summary of t-test analysis of Experimental Group on the overall Pretest-Posttest

Experimental	N	M	SD	t-value Calculated Value	Table Value .05
Posttest	40	35	2.792	45.61	1.664

Table 23 shows the result of the experimental group on the overall knowledge of the model on both pretest and posttest. The mean score of the pretest was 9.5 and that of the posttest was 35. The calculated t value was 45.61, which is greater than the critical t value of 1.664 at the significance level of 0.05.

Therefore, there is difference after the experimental group was exposed to the treatment – the SNS based model. This could be seen clearly in figure 4.8.

Figure 54: Experimental Group Overall Posttest-Pretest Result

Figure 54: Experimental Group Overall Posttest-Pretest Result
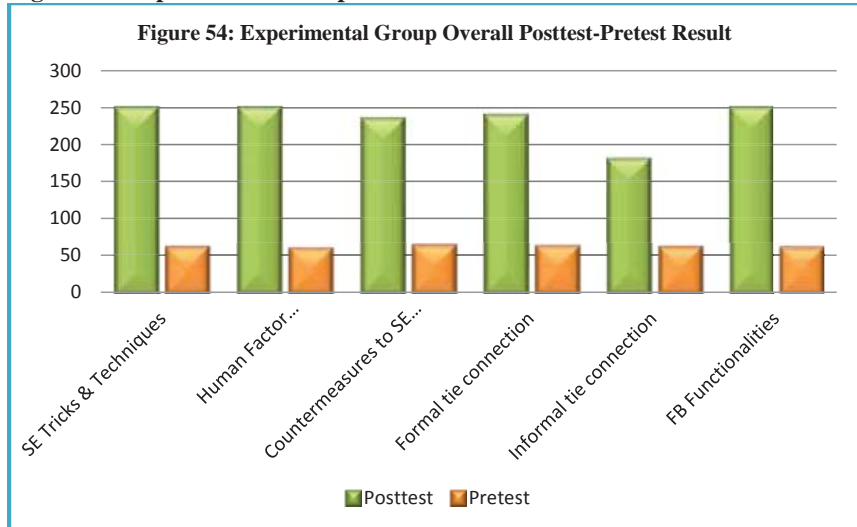
It is obvious from the bar graph in figure 6.8 that there was sharp difference after the experimental group was exposed to the SNS based model. Their performance rose sharply not as they were at level of the pretest. This is true in all the variables tested as can be seen in the graph. This implies that the SNS model is effective in the identification and prevention of SE based intrusion on their WLAN.

Table 6.10 and Figure 54 below, presents and displays the findings on research hypotheses two:

H1:   There is no significance difference in the performance scores of the subjects exposed to the SNS based model on tricks and techniques of SE and those subjects who were not exposed to the SNS model.

H0   *The subjects exposed to the SNS based mode perform better in the tricks and techniques of SE than those subjects who were not exposed to the SNS based model.*

Table 22: Summary of t-test analysis of Experimental Group on Pretest-Posttest - tricks and techniques of social engineering

Experimental Group	N	M	SD	t-value	
				Calculated Value	Table Value .05
Posttest	40	6.225	1.000	23.78	1.664
Pretest	40	1.525	0.751		

Table 24 shows t-test of the Experimental group on tricks and techniques of social engineering for both pretest and posttest. The mean score of the pretest was 6.225 and 1.525 for the posttest. The calculated t value was 23.78, which is greater than the critical t value of 1.664 at the significance level of 0.05. Therefore, there is difference after the experimental group was exposed to the treatment – the SNS based model. The difference is clearly seen in figure 55

Figure 55: SE Tricks and Techniques, Pretest-Posttest Experimental Group

Figure 55: SE Tricks & Techniques, Pretest-Posttest Experimental Group
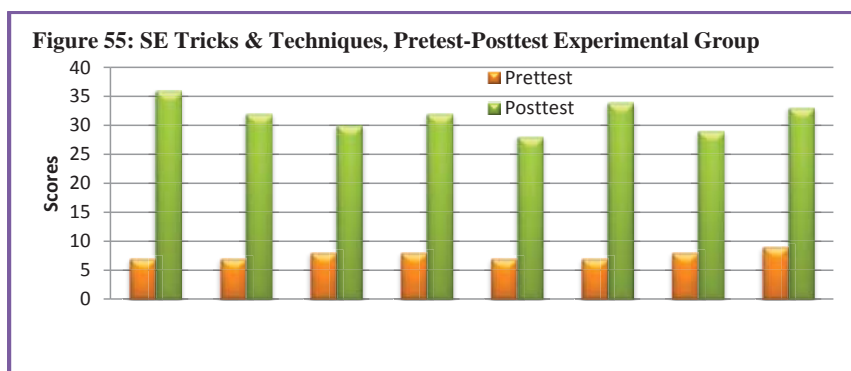
It is obvious from the bar graph in figure 55 that there was sharp difference after the experimental group was exposed to the SNS based model. Their performance on the tricks and techniques of SE rose sharply not as they were at level of the pretest. This implies that the SNS model is effective in the identification and prevention of SE based tricks and techniques for intrusion into their WLAN.

Table 25 and Figure 26 below, presents and displays the findings on research hypotheses three:

H0:   There is no significance difference in the performance scores of the subjects exposed to the SNS based model on the Human Factor authentication mode and the subjects who were not exposed to the SNS based model.

H1:   *the subjects exposed to the SNS based model perform better on Human Factor authentication mode than the subjects who were not exposed to the SNS based model.*

Table 23:Summary of t-test analysis of Experimental Group on Pretest-Posttest – Human factor authentication

Experimental Group	N	M	SD	t-value	
				Calculated Value	Table Value .05
Posttest	40	6.225	0.751	22.59	1.664
Pretest	40	1.475	1.165		

Table 25 shows the t-test of the Experimental group on authentication mode for both pretest and posttest. The mean score of the pretest was 1.475 and that of the posttest was 9.15.

The calculated t value was 22.59, which is greater than the critical t value of 1.664 at the significance level of 0.05. Therefore, there is significance difference after the experimental group was exposed to the treatment – the SNS based model. The difference is clearly seen in graph figure 56.

Figure 56: Experimental Group Pretest-Posttest Human Factor Authentication

Figure 56: Experimental Group Pretest-Posttest Human Factor Authentication
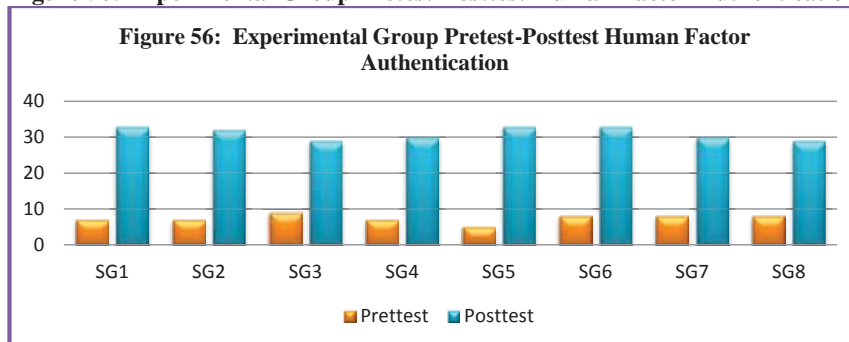
It is obvious from the bar graph in figure 56 that there was sharp difference after the experimental group was exposed to the SNS based model. Their performance on the test of human factor authentication rose sharply not as they were at level of the pretest. This implies that the SNS model is effective in making the user to authentication both online and offline intrusion techniques.

Table 27 and Figure 57 below, presents and displays the findings on research hypotheses four:

H0:   there is no significance difference in the performance scores of the subjects exposed to the SNS based model on countermeasures to threats and attacks of SE and the subjects who were not exposed to the SNS model.

218

H1:   *the subjects exposed to the SNS based model perform better on countermeasures to threats and attacks of SE than the subjects who were not exposed to the SNS based model.*

Table 24: Summary of t-test analysis of Experimental Group on Pretest-Posttest prevention of social engineering threats and attacks

Experimental Group	N	M	SD	t-value	
				Calculated Value	Table Value .05
Posttest	40	5.85	0.903	18.78	1.664
Pretest	40	1.575	1.250		

Table 26 shows the t-test analysis of the experimental group on prevention of social engineering threats and attacks for both pretest and posttest. The mean score of the experimental group was 35.85 and that of the control group was 1.575. The calculated t value was 18.78, which is greater than the critical t value of 1.664 at the significance level of 0.05. Therefore, there is significance difference after the experimental group was exposed to the treatment – the SNS based model. This indicates the effectiveness of the model as an intervention that brought the changes in performance between the two groups. Thus, the experimental group was able to counteract social engineering threats and attacks better than their counter part, the control group.

**Figure 57: Experimental Group Pretest-Posttest SE Intrusion
Countermeasures**
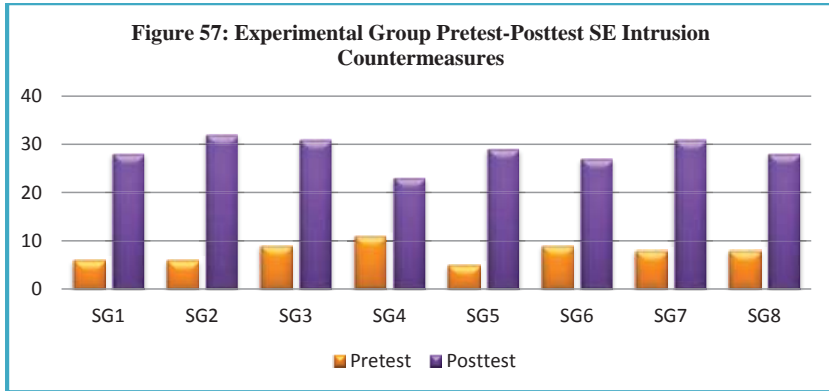
It is obvious from the bar graph in figure 57 that there was sharp difference after the exper-
imental group was exposed to the SNS based model. Their performance on counter
measures to SE based intrusion rose sharply not as they were at level of the pretest. This
implies that the SNS model is effective in making users to counteract SE based intrusion on
their WLAN.

Table 27 and Figure 58 below, presents and displays the findings on research hypotheses
five:

H0:   there is no significance difference in the performance scores of the subjects exposed
         to the SNS based model regarding forminal tie security collaborations and the sub-
         jects who were not exposed to the SNS model.

H1:   *the subjects exposed to the SNS based model perform better on forminal tie security
         interactions than the subjects who were not exposed to the SNS model.*

Table 25: Summary of t-test analysis of Experimental Group on Pretest-Posttest (formal tie connection)

Experimental Group	N	M	SD	t-value	
				Calculated Value	Table Value .05
Posttest	40	5.975	1.250	17.40	1.664
Pretest	40	1.55	1.011		

Table 27 shows the t-test analysis of the experimental group on sharing experiences through strong tie connection for both pretest and posttest. The mean score of the pretest was 5.975 and that of the posttest was 1.575. The calculated t value was 17.40, which is greater than the critical t value of 1.664 at the significance level of 0.05. Therefore, there is significance difference after the experimental group was exposed to the treatment – the SNS based model. This is obvious in the bar graph appeared in figure 58.

Figure 58: Experimental Group Pretest-Posttest Formal tie Connection

Figure 58: Experimental Group Pretest-Posttest Formal tie Connection
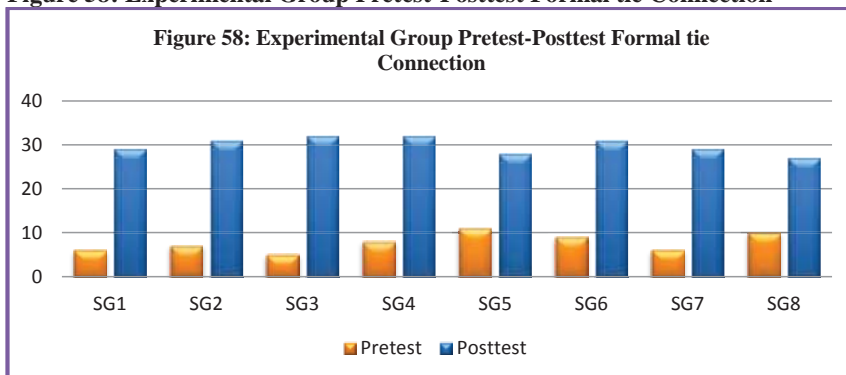
It is obvious from the bar graph in figure 58 that there was sharp difference after the experimental group was exposed to the SNS based model. Their performance on the test of social networking for security collaborations with formal tie connection rose sharply from the level they were at the pretest. This implies that the SNS model is effective in collaborating with formal ties to share SE security experiences for the prevention of SE based intrusion into their WLAN.

Table 28 and Figure 59 below, presents and displays the findings on research hypotheses six:

H0: there is no significance difference in the performance scores of the subjects exposed to the SNS based model regarding informal ties security collaborations and the subjects who were not exposed to the SNS model.

H1: *the subjects exposed to the SNS based model perform better on informal ties security interactions than the subjects who were not exposed to the SNS model.*

Table 26: Summary of t-test analysis of Experimental Group on Pretest-Posttest (Informal tie connection)

Experimental Group	N	M	SD	t-value	
				Calculated Value	Table Value .05
Posttest	40	4.5	1.525	14.70	1.664
Pretest	40	1.013	0.784		

Table 28 shows the t-test analysis of the experimental group on sharing experiences through weak tie connection for both pretest and posttest. The mean score of the pretest was 4.5 and that of the posttest was 1.013. The calculated t value was 14.70, which is greater than the critical t value of 1.664 at the significance level of 0.05. Therefore, there is significance difference after the experimental group was exposed to the treatment – the SNS based model. The difference is clear in the bar graph below.

Figure 59: Experimental Group Pretest-Posttest Informal tie connection

Figure 59: Experimental Group Pretest-Posttest Informal tie Connection
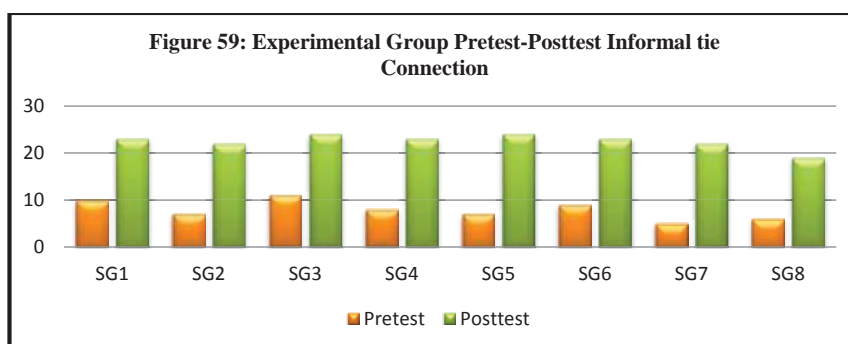
It is obvious from the bar graph in figure 59 that there was sharp difference after the experimental group was exposed to the SNS based model. Their performance on the test of social networking for security collaborations with informal tie connection rose sharply from the level they were at the pretest. This implies that the SNS model is effective in collaborating with informal ties to share SE security experiences for the prevention of SE based intrusion into their WLAN.

Table 28 and Figure 60 below, presents and displays the findings on research hypotheses seven:

H0: there is no significance difference in the performance scores of the subjects exposed to the SNS based model on the use of Facebook functionalities for security collaborations and the subjects who were not exposed to the model.

H1: *the subjects exposed to the SNS based model perform better on the use of Facebook functionalities for security collaborations than the subjects who were not exposed to the SNS based model.*

Table 27: Summary of t-test analysis of Experimental Group on Pretest-Posttest (using Facebook functionalities for security collaborations)

Experimental Group	N	M	SD	t-value	
				Calculated Value	Table Value .05
Posttest	40	6.225	1.165	21.00	1.664

Table 29 shows the t-test analysis of the experimental group on using Facebook functionalities for security collaborations for both pretest and posttest. The mean score of the pretest was 1.5 and that of the posttest was 6.225. The calculated t value was 21.00, which is greater than the critical t value of 1.664 at the significance level of 0.05. Therefore, there is significance difference after the experimental group was exposed to the treatment – the SNS based model. Thus the experimental group was able to use social networking on the platform of Facebook for collaboration on security issues, better than their counter part, the control group. The difference is clear as depicted in figure 60.

Figure 60: Experimental Group Pretest-Posttest FB Functionalities

Figure 60: Experimental Group Pretest-Posttest FB functionalities
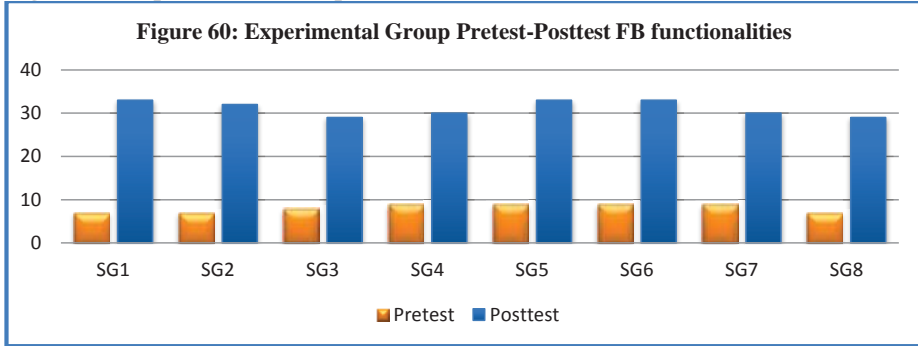
It is obvious from the bar graph in figure 60 that there was sharp difference after the experimental group was exposed to the SNS based model. Their performance on the test of the use of FB functionalities to identify, prevent and collaborate for SE based threats and attacks on the platform of FB, rose sharply from the level they were at the pretest. This implies that the SNS model is effective in using FB platform to identify, discuss, share and prevent SE based intrusion into their WLAN.

6.7   Control Group t-test analysis on Pretest and Posttest

The following table shows the t-test analysis of the Experimental group on both Pretest and Posttest.

Table 28: Summary of t-test analysis of Control Group on overall Pretest-Posttest

Control Group	N	M	SD	t-value	
				Calculated Value	Table Value .05
Posttest	40	9.7	1.539	0.11	1.664
Pretest	40	9.65	2.315		

Table 30 shows the t-test analysis of the Control group on the overall pretest and posttest. The mean score of the pretest was 9.65 and the posttest was 9.7. The calculated t value was 0.11, which is less than the critical t value of 1.664 at the significance level of 0.05. Therefore, there is no significance difference in the performance of the control group after posttest on the SNS based model. The difference is clear in the bar graph - figure 61.

Figure 61: Control Group Overall Pretest Posttest

Figure 61
Contro Group Overall Pretest Posttest

	SE Tricks & Techniques	Human Factor Authentication	Countermeasures to SE threats & attacks	Formal tie connections	Informal tie connections	FB functionalities
Pretest	63	61	65	65	66	66
Posttest	60	55	69	68	69	67
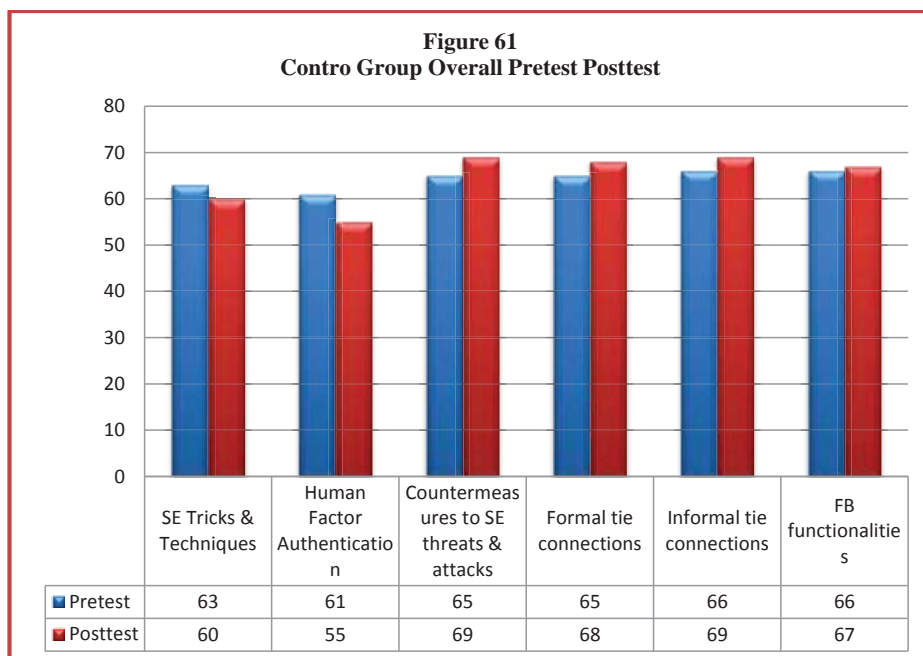
It is obvious from the bar graph in figure 61 that there was no any improvement in the performance of the control groups after the pretest. This is obvious from the fact that denying them the treatment of the SNS based model was responsible for such no difference performance. This implies that the SNS based model has effect on the identification and prevention of SE based intrusion into WLAN. The subsequent t-test analysis further revealed the performance of the control group on the six variables contained in figure 62.

Table 29: Summary of t-test analysis of Control Group on Pretest-Posttest (tricks and techniques of social engineering)

Control				t-value	
Group	N	M	SD	Calculated Value	Table Value .05
Posttest	40	1.5	0.641	0.42	1.664
Pretest	40	1.575	0.931		

Table 31 shows the t-test analysis of the Control group on both pretest and posttest for tricks and techniques of social engineering. The mean score of the pretest was 1.575 and the posttest was 1.5. The calculated t value was 0.42, which is less than the critical t value of 1.664 at the significance level of 0.05.

Therefore, there is no significance difference in the performance of the control group after posttest on the tested variable. The experimental group, however, showed improved performance on the posttest as compared with their performance in the pretest. The difference or the changes that occurred in the posttest performance of the two groups is attributed to the exposure of the experimental group to the SNS model.

Table 30: Summary of t-test analysis of Control Group on Pretest-Posttest (Human factor Authentication)

Control				t-value	
Group	N	M	SD	Calculated Value	Table Value .05
Posttest	40	1.375	0.838	0.80	1.664
Pretest	40	1.525	0.847		

Table 32 shows the t-test analysis of the Control group on both pretest and posttest for human factor authentication. The mean score of the pretest was 1.525 and the posttest was

1.375. The calculated t value was 0.80, which is less than the critical t value of 1.664 at the significance level of 0.05. Therefore, there is no significance difference in the performance of the control group after posttest on the tested variable.Table

Table 31: Summary of t-test analysis of Control Group on Pretest-Posttest (prevention of social engineering based threats and attacks).

Control Group	N	M	SD	t-value	
				Calculated Value	Table Value .05
Posttest	40	1.725	0.816	0.61	1.664
Pretest	40	1.625	0.628		

Table 33 shows the t-test analysis of the Control group on both pretest and posttest for prevention of social engineering based threats and attacks. The mean score of the pretest was 1.625 and the posttest was 1.725. The calculated t value was 0.61, which is less than the critical t value of 1.664 at the significance level of 0.05. Therefore, there is no significance difference in the performance of the control group after posttest on the tested variable, the prevention or countermeasures to social engineering based threats and attacks.

Table 32: Summary of t-test analysis of Control Group on Pretest-Posttest (Formal tie connection for collaboration on security issues)

Control Group	N	M	SD	t-value	
				Calculated Value	Table Value .05
Posttest	40	1.7	0.648	0.42	1.664

Table 34 shows the t-test analysis of the Control group on both pretest and posttest strong tie connection in sharing experiences. The mean score of the pretest was 1.625 and the posttest was 1.7. The calculated t value was 0.42, which is less than the critical t value of 1.664 at the significance level of 0.05. Therefore, there is no significance difference in the performance of the control group after posttest on the tested variable, which using formal tie connection to collaborate on security issues.

Table 33: Summary of t-test analysis of Control Group on Pretest-Posttest (weak tie connection on sharing experiences)

Control Group	N	M	SD	t-value	
				Calculated Value	Table Value .05
Posttest	40	1.725	0.751	0.45	1.664

Table 35 shows the t-test analysis of the Control group on both pretest and posttest for weak tie connection in sharing experiences. The mean score of the pretest was 1.65 and the posttest was 1.725. The calculated t value was 0.45, which is less than the critical t value of 1.664 at the significance level of 0.05. Therefore, there is no significance difference in the performance of the control group after posttest on the tested variable.

Table 34: Summary of t-test analysis of Control Group on Pretest-Posttest (Using Social networking on Facebook platform for collaborations on security issues)

Control Group	N	M	SD	t-value	
				Calculated Value	Table Value .05
Posttest	40	1.675	0.736	0.14	1.664
Pretest	40	1.65	0.797		

Table 36 shows the t-test analysis of the Control group on both pretest and posttest in using Facebook functionalities for security collaborations. The mean score of the pretest was 1.65 and the posttest was 1.675. The calculated t value was 0.14, which is less than the critical t value of 1.664 at the significance level of 0.05. Therefore, there is no significance difference in the performance of the control group after posttest on the test of social networking on the platform of Facebook, for collaborations on security issues.

6.8   Experimental and Control group's t-test analysis on Pretest and Posttest

Table 37 shows the t-test analysis of the Experimental and Control groups on Pretest and Posttest.

Table 35:Ssummary of t-test analysis of Experimental and Control Group on Pretest-Posttest (overall elements of the SNS model)

Group	N	M	SD	t-value	
				Calculated Value	Table Value .05
Experimental	40	35	2.792	50.19	1.664
Control	40	9.7	1.539		

Table 37 shows the t-test analysis on the overall pretest and posttest of both Experimental and Control groups. The mean score of the experimental group was 35 and that of the control group was 9.7. The calculated t value was 50.19, which is greater than the critical t value of 1.664 at the significance level of 0.05. This shows that there is significance difference between the performance of the two groups in the knowledge of the model for the identification and prevention of social engineering based threats and attacks. Thus, the experimental group was able to perform better in the test of all the variables that constitute the knowledge and skills of the SNS model. Ability to perform better in all the variables is

an indication that the model is effective for the purpose it was proposed to identify and counteract social engineering based threats and attacks on the Wireless LAN in the organization. The bar graph in figure 62 reveals the obvious difference.

Figure 62: Experimental and Control Groups: Overall Pretest-Posttest
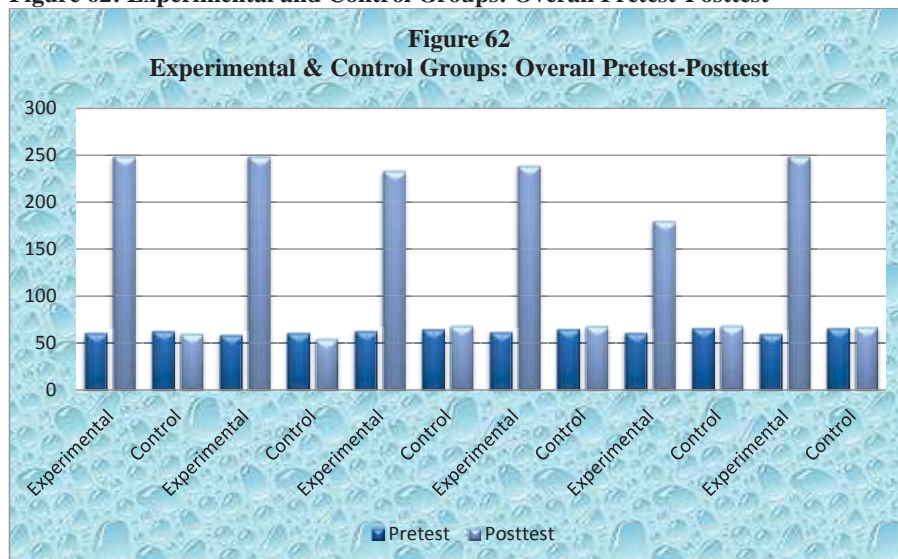
It is obvious from the graph in figure 62 that there was sharp increase in the posttest of the experimental group, while the performance of the control group remained the same as it was in the pretest performance. The height of the bars represents the increase in performance in variables tested as highlighted in section 6.4. The reason for the difference in the posttest performance is as the result of the exposure of the experimental group to the SNS based model. Thus, the model is proved to be effective in the identification and prevention of SE based intrusion into WLAN. The tables and graphs that follow further present the results of the individual variables.

Table 36: Summary of t-test analysis of Experimental and Control Group on Pretest-Posttest (tricks and techniques of social engineering)

Group	N	M	SD	t-value	
				Calculated Value	Table Value .05
Experimental	40	6.225	1.000	25.17	1.664
Control	40	1.5	0.641		

Table 38 shows the t-test analysis on pretest and posttest of both Experimental and Control groups, on the tricks and techniques of social engineering. The mean score of the experimental group was 6.225 and that of the control group was 1.5. The calculated t value was 25.17, which is greater than the critical t value of 1.664 at the significance level of 0.05. This shows that there is significance difference in the performance of the two groups in the knowledge of tricks and techniques of social engineering for the identification of social engineering based threats and attacks. The difference is attributed to the treatment or the exposure to the SNS based model to the experimental group.

Figure 63: Experimental Control Groups Pretest-Posttest SE Tricks and Techniques

Figure 63: Experimental - Control Groups Pretest-Posttest SE Tricks & Techniques

It is obvious from the graph in figure 63 that there was sharp increase in the posttest of the experimental group in the test of tricks and techniques of SE; while the performance of the control group remained the same as it was in the pretest performance. The height of the bars represents the increase in the performance of the two groups. The reason for the difference in the posttest performance is as the result of the exposure of the experimental group to the SE tricks and techniques. Thus, exposure to tricks and techniques of SE is effective in identification of intrusion through SE into WLAN.

Table 37: Summary of t-test analysis of Experimental and Control Group on Pretest-Posttest (human factor authentication mode)

Group	N	M	SD	t-value	
				Calculated Value	Table Value .05
Experimental	40	6.225	1.165	21.37	1.664
Control	40	1.375	0.838		

Table 39 shows the t-test analysis on pretest and posttest of both Experimental and Control groups, human factor authentication mode. The mean score of the experimental group was 6.225 and that of the control group was 1.375.

 The calculated t value was 21.37, which is greater than the critical t value of 1.664 at the significance level of 0.05. This shows that there is significance difference in the performance of the two groups in humanly authenticating an object or event attempting to access or intrude into the network or online and offline resources.

Figure 64: Experimental Control Groups Pretest-Posttest Human Factor Authentication

Figure 64: Experimental - Control Groups Pretest-Posttest Human Factor Authentication
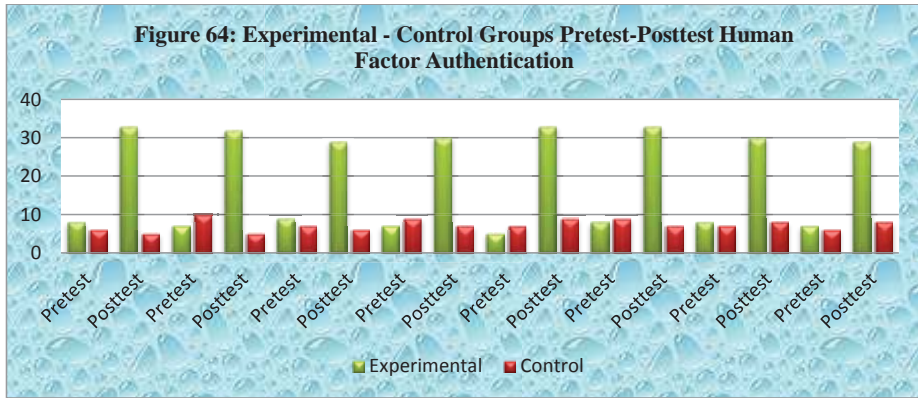
It is obvious from the graph in figure 64 that there was sharp increase in the posttest of the experimental group in the test of Human factor authentication; while the performance of the control group remained the same as it was in the pretest performance. The height of the bars represents the increase in performance in the variable tested on the two groups. The reason for the difference in the posttest performance is as the result of the exposure of the experimental group to human factor authentication. Thus, exposure to human factor authentication is effective in the prevention of intrusion by SE into WLAN.

Table 38: Summary of t-test analysis of Experimental and Control Group on Pretest-Posttest (prevention of social engineering based threats and attacks)

Group	N	M	SD	t-value Calculated Value	Table Value .05
Experimental	40	5.85	1.122	18.80	1.664
Control	40	1.725	0.816		

Table 4000 shows the t-test analysis on pretest and posttest of both Experimental and Control groups, on knowledge for preventing social engineering threats and attacks. The mean score of the experimental group was 5.85 and that of the control group was 1.725. The calculated t value was 18.80, which is greater than the critical t value of 1.664 at the significance level of 0.05. This shows that there is significance difference in the performance of the two groups in the variable tested.

Figure 65: Experimental - Control Groups Pretest-Posttest Countermeasures

Figure 65: Experimental - Control Groups Pretest-Posttest Countermeasures

It is obvious from the graph in figure 65 that there was sharp increase in the posttest of the experimental group in the test of counter measures to SE; while the performance of the control group remained the same as it was in the pretest performance. The height of the bars represents the increase in performance in variable tested on the two groups. The reason for the difference in the posttest performance is as the result of the exposure of the experimental group to counter measures to SE. Thus, exposure to SE counter measures is effective in the prevention of intrusion by SE into WLAN.

Table 39: Summary of t-test analysis of Experimental and Control Group on Pretest-Posttest (formal tie connection)

Group	N	M	SD	t-value Calculated Value	Table Value .05
Experimental	40	5.975	1.250	19.19	1.664
Control	40	1.7	0.648		

The table shows the t-test analysis on pretest and posttest of both Experimental and Control groups, on using social connection of strong tie to share experience. The mean score of the experimental group was 5.975 and that of the control group was 1.7. The calculated t value was 19.19, which is greater than the critical t value of 1.664 at the significance level of 0.05. This shows that there is significance difference in the performance of the two groups in the use of social connection of strong tie to share experience. Sharing of security experience to appropriate as in the formal structure is desirable for mitigating any anomalies and suspicious events identified through online and offline interactions. The difference in the performance of the two groups is depicted in the graph below:

Figure 66: Experimental - Control Groups Pretest-Posttest Formal tie connection

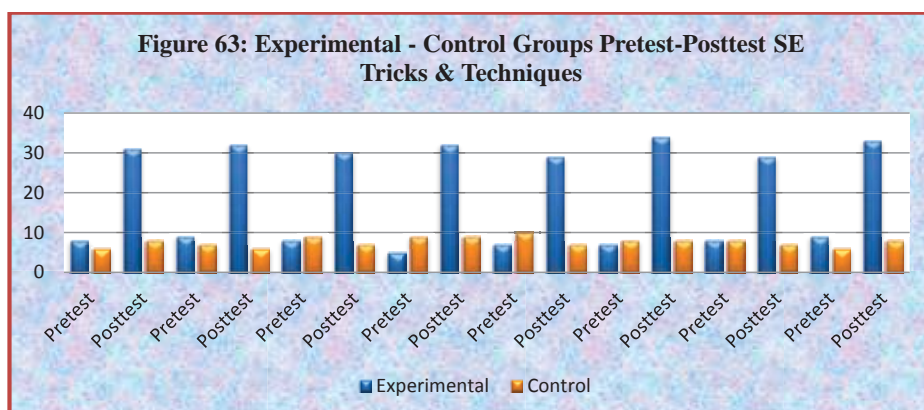Figure 66: Experimental - Control Groups Pretest-Posttest Formal tie connection
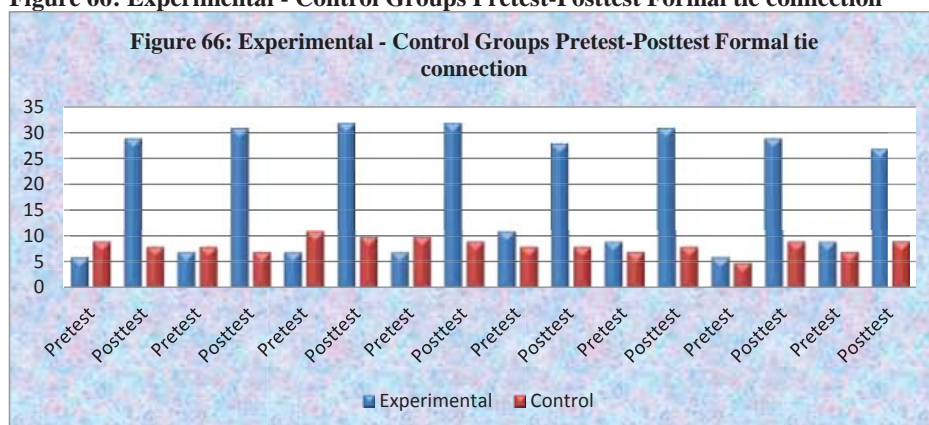
It is obvious from the graph in figure 66 that there was sharp increase in the posttest of the experimental group in the test of collaboration with formal tie connection for security on the WLAN. The performance of the control group remained the same as it was in the pre-test performance. The height of the bars represents the increase in performance in variable tested on the two groups. The reason for the difference in the posttest performance is as the result of the exposure of the experimental group to pattern of collaboration by formal ties connection. Thus, exposure to social networking for security with the formal tie connection is effective for security collaboration.

Table 40: Summary of t-test analysis of Experimental and Control Group on Pretest-Posttest (Informal tie connection)

Group	N	M	SD	t-value	
				Calculated Value	Table Value .05
Experimental	40	4.5	1.013	13.92	1.664
Control	40	1.725	0.751		

Table 42 shows the t-test analysis on pretest and posttest of both Experimental and Control groups, on the using social connection of weak tie to share experience. The mean score of the experimental group was 4.5 and that of the control group was 1.725. The calculated t value was 13.92, which is greater than the critical t value of 1.664 at the significance level of 0.05. This shows that there is significance difference in the performance of the two groups in the use of social connection by informal tie to collaborate on security. The difference is more obvious in the graph below:

Figure 67: Experimental - Control Groups Pretest-Posttest Informal Connection

Figure 67: Experimental - Control Groups Pretest-Posttest Informal Connection
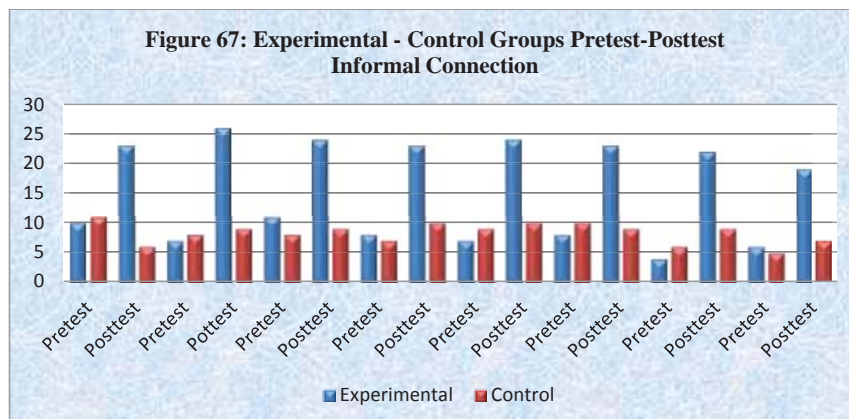
It is obvious from the graph in figure 67 that there was sharp increase in the posttest of the experimental group in the test of collaboration with informal tie connection for security on the WLAN. The performance of the control group remained the same as it was in the pretest performance. The height of the bars represents the increase in performance in variable tested on the two groups. The reason for the difference in the posttest performance is as the result of the exposure of the experimental group to pattern of collaboration by informal tie connection. Thus, exposure to social networking for security with the informal tie connection is effective for security collaboration.

Table 41: Summary of t-test analysis of Experimental and Control Group on Pretest-Posttest (using Facebook functionalities for security collaborations)

Group	N	M	SD	t-value	
				Calculated Value	Table Value .05
Experimental	40	6.225	1.165	20.38	1.664

Table 43 shows the t-test analysis on pretest and posttest of both Experimental and Control groups, on using Facebook functionalities for security collaborations. The mean score of the experimental group was 6.225 and that of the control group was 1.675. The calculated t value was 20.38, which is greater than the critical t value of 1.664 at the significance level of 0.05. This shows that there is significance difference in the performance of the two groups in the use of Facebook functionalities for security collaborations. The difference is more obvious in the graph below:

Figure 68: Experimental - Control Groups Pretest-Posttest Facebook functionalities

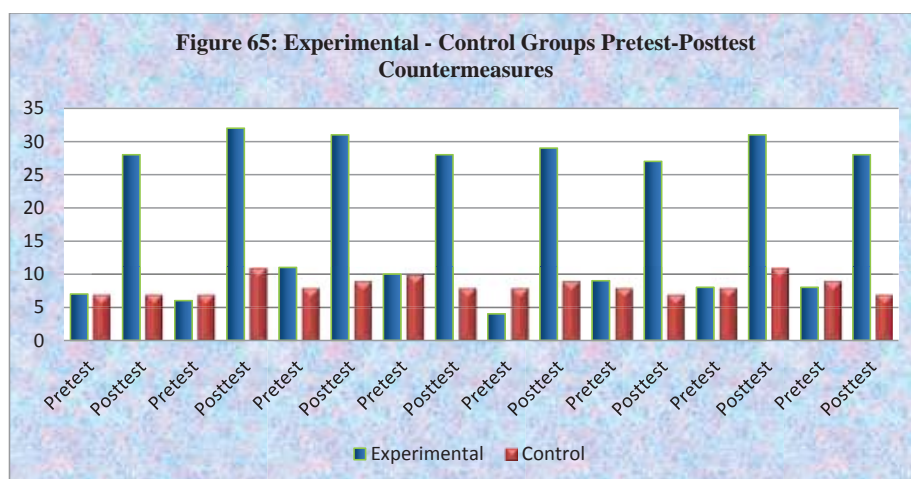Figure 68: Experimental - Control Groups Pretest-Posttest Facebook functionalities
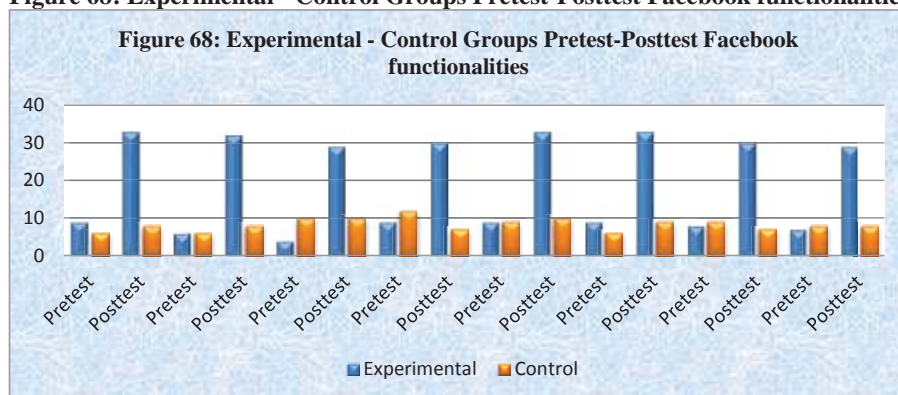
It is obvious from the graph in figure 68 that there was sharp increase in the posttest of the experimental group in the test of social networking on the platform of FB to collaborate for SE based intrusion prevention on the WLAN. The performance of the control group remained the same as it was in the pretest performance. The height of the bars represents the increase in performance in variable tested on the two groups. The reason for the difference in the posttest performance is as the result of the exposure of the experimental group to the use of FB platform to collaborate for intrusion prevention on the WLAN. Thus, exposure to social networking for security on the platform of the FB is effective for security collaboration.

239

6.9 Presentation and Discussions of findings from Qualitative Content Analysis on the implementation of the SNS model

The purpose of this section is to present, describe, interpret, and discuss the behavior of the participants as qualitative data collected from the content analysis of social media of Facebook, being the platform for the implementation of the SNS. The choice of concurrent discussions with the presentation of the findings in this section is to keep coherency with the diagrammatic interpretation of the findings. A content analysis was conducted from June 2013 to August 2013 of two groups hereby called Bi-forminal ties made up of 40 members with formal ties in one group and 67 members with informal ties in the second group. The aim was to describe the behavior of the experiment participants in the implementation of the proposed SNS based model.

The qualitative data collection involved the use of codes, themes, and patterns, to systematically view and interpret the data. Details of the methodology were outlined in the methodology chapter. The pattern of the presentation was guided by the research question (*what is the behavior of the Wireless LAN users in the implementation of the SNS model?*). In answering this question, four predefined themes were used as unit of analysis. The contents of the four pre-existing themes: uses' wall posts, users' comment on posting, users' likes, and users' sharing mode were used to bring out the categories of the data. The data was described, presented and interpreted in tables and diagrams.

The interpretation indicates patterns of behavior in relation to each theme and respective categories. Thus, the content analysis examined activities (in terms of social networking) of the research participants on the platform of Facebook. The activities of the participants reveal the extent to which the collaboration is for and about security issues.

Figure 69: The content data analysis process
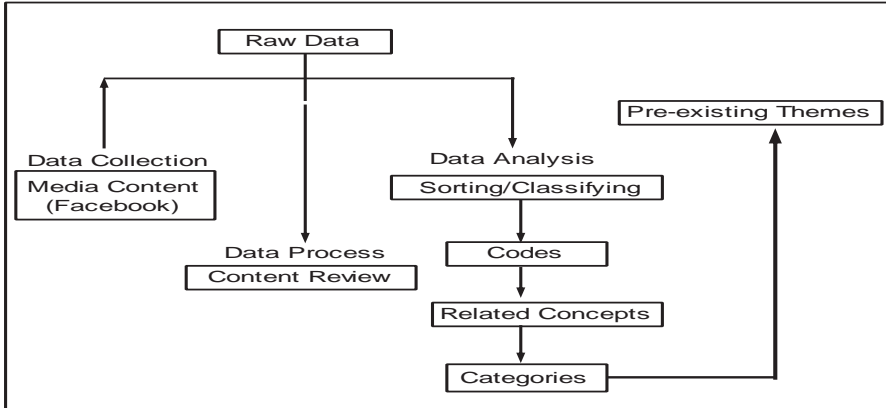
Figure 69 illustrate the process of analyzing the qualitative data generated from the contents of the users' activities on the platform of the social media of FB in the implementation of the SNS model. As already mentioned in the introductory part of this chapter, the themes were pre-existed and out of each theme categories were identified based on the contents of the theme. The themes with their corresponding categories were analyzed, one after the other, as depicted in figure 70.

Figure 70: Users' posting behavior on the SNS model *(extracted from Table 44).*
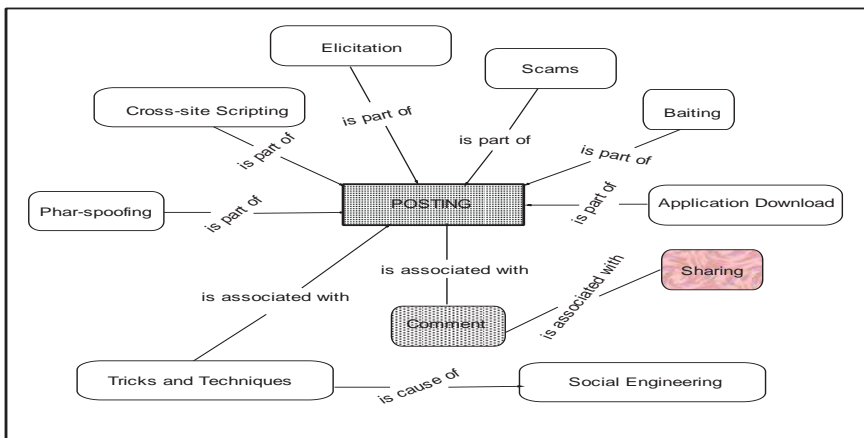
Figure 70 indicates the patterns of Posting. Users posted different contents ranging from online to offline tricks and techniques of social engineering. The posting nature was associated with tricks and techniques of social engineering. The posting also generated comments that were also a form of sharing experiences among members. Users experienced one form of trick or another in their online and offline activities. The contents in the diagram indicate that users were security proactive in their network. Thus, it was clear that users were actively implementing the model for security collaborations. The findings have revealed that the posting behaviour of the participants is centred on the tricks and techniques used to lure users into facilitating access to their network and information resources. This is in line with the findings of Sherly et al (2010) who found that user's intervention is required before malicious code are executed on the network.

The interpretations of the findings were in line with the findings of Ira et al (1995) that user's discussions on the context of SE threats lead to awareness and sharing of experiences. This is supported by the findings of Gutner (2013) that online user behaviour is surrounded with various tricks and techniques of SE. Posting in one of the Facebook functionalities that gives users the opportunity to describe their feelings, attitude, concern, or experiences in such a way that viewers of their social network can digest, comment, and discuss the subject matter with a view to supporting, criticizing, or adding more substances on the issue posted. This is collaborated by the study of Selwyn (2009) who found that posting on the group's wall added valuable means of information exchange among peers, thereby identifying their identity and satisfying the expectations of the group.

Posting reflect the users' conduct on the implementation of the SNS model for the identification and prevention of social engineering threats and attacks on their Wireless LAN. Table 4.30 below shows the conduct of the users regarding posting. The table shows

that users were posting contents that related to issues and activities that have some conse-

quences to their network and online affairs. Each of the content in the posting was a point-

er to manifestation of security habit.

Table 42: Theme I: posting behavior of users on the SNS model.

CATEGORY	DATA
Phar-Spoofing	*Now, let's discuss this on a serious note. If hackers have taken over facebook, what do we do? Leave it, perhaps? This evening someone used the account of a very senior female lecturer in UDUS to send me messages. The facebook account had her name and picture. The hacker told me he/she is in heavy traffic and need to call home, and asked me for recharge card. Immediately, I called the female lecturer and she told me she is not even near a computer or handheld device. I told her what happened and she was shocked. This is very embarrassing. So, whats facebook turning into?* *I cant access some websites like www.nouroun.edu.ng, www.goal.com* *As I was trying to log into our home page login, I noticed as If it is not the same home page I used to log in. Did anybody witnessed such suspicions?* *I recently log into our home log into our web logging, but I was asked to renter my password, whereas I entered the correct password. I later knew that our home page never asked for re-entering password. We should be aware of this and take note.* *I received the following website http://us-mg5.mail.yahoo.com/neo/launch?.rand=7sqmfovn2qrvm* *And is asking me to share it. Another form of social engineering?* *Urgent!! Your network in on upgrade. Disable all security features and submit your log in details to the following mail for verification, and then restart your system for the new verification to take effect.* *In case for a forgetting password and maintenance system that can protect your details from being lost, immediately send your login details to the link below for safe keeping. Just click here and enter your details* *Accounts are being hacked. They take your profile picture & your name & create a new FB account. Then they ask your friends to add. Your friends think it's you, & accept. From that moment , they can write whatever they want under your name. Please do not accept a 2nd invitation from me. Copy this on your wall so your friends can see & be warned!*
Cross-site Scripting	*I received a notification to log into www.simpuk.com and claim175,000 air time......from transfer......don't u think it's not true ? 419 right ?(BAS)* *I recieve a massage on hw to do my facebook setting using my cellphone...all i hv to do is to click on 'see how' and gat trap by 419 ..pple be careful on the links u see on social netwok it's too dangerous !* I will lyk to inform u that Aliyu *Danjuma (a.k.a Class rep, food director, no food no man, Ali D) just release his latest track featuring sodikoko, tittle "owo ni koko" "money* *is* *inevitable"* *u can also download other tracks like Umukitess, rainfall, jekajo, yarinya. from the* *below* *web* *site:* *www.hulkshare.com/ali_d*

243

CATEGORY	DATA
	you can also like his fans page: *http://m.facebook.com/profile.php?id=214779065331856&refid=5* *UMYUKITESS always makes a difference. we are naturally blessed with talents...* *http://www.facebook.com/l.php?u=http%3A%2F%2Fwww.netcontacts.com.ng%2F&h=2AQE0RtAm* *i visited the link and i been required to like the Link and even to share it to many people- this rely is kind of Threats* *The cursor stand still and when refresh the system hooks and state Restore to Previous Session or Start Session again* *There is a link were they ask me to click to update my online banking security which I did not am afraid of what will happan the moment I click on the link what make me suprise is I don't have account with First Bank and they sent me the message through my email address not my phone number so due to these reason I just ignore it.* *have received a text now from the sender 'TRANSFER' that my number have been assigned =N175,000 Airtime. for my line to be loaded now, Login to: www.simpuk.com. My Login PIN is 3232. I have 18 hours left* *A friend of mine found this in his inbox. I believe there is going to be problem opening the link.* *The subject matter was: Smartphone Upgrade: click here to visit the home page. This is was the message I have been receiving. Thanks to the Aalborg researcher, I would have gone for it and ended up in the website of social engineering attackers.* *Attention,* *We have unauthorized reset of our Wireless login password* *Please ignore this notification if your password was reset by you.* *We implore you to make sure your account was not compromised due to this error. Click to reset it to default, restart your computer and then create your own password.* *Reset To Default* *We are sorry for any inconvenience this may have caused.* *Sincerely,* *The network security* *Attention!* *Your system is at risk and may not see the network, secure it now by clicking the*

CATEGORY	DATA
	link *http://netnyurl.com/pdrukgd and complete the form attach to this message.* *Thank You.* *Dear Customer,* *Your First Bank account was recently updated with a new security enhancement. For your security, we have temporary suspended your account.* *Online banking Log on* *Please complete your online verification* *Privacy Department.* *2013 First Bank Nigeria plc* **Password Reset** *For security reasons, we have noticed constant account compromised and is necessary to change your login password to access the network and other services. This is carried out once! You have only 85 seconds left. Failure to do it within the stipulated seconds could log you out and you cannot be able to connect and be online. The automated software cannot entertain after event complaint, so act now! Click here.* *Dear Customer,* *Your First Bank Online security is still not active.* *Please Login below to activate your Online Banking security.* *Online banking Log on* *Please complete your online verification* *Privacy Department.* *2013 First Bank Nigeria plc*
Browsing/ connectivity	*subhanallah my system is hanging* *My system is hang and the network is interrupted.* *there is a prob of IP adress.* *My system is hang and the network is interrupted.* *the net is reporting that there is an errow visitinga particular website* *now am able to login, bout so many pop ups* *I was trying to open UMYU website, but my browser is unable to open it and my network strength is good.* *the net is very poor..could'nt lonch a brouser.* *as iam browsing this day 5 april i notice that when attemting to scroll down it take me er another page.why?* *Tried to access the apple itunes website https://itunes.apple.com/app/delicious-*

CATEGORY	DATA
	official-app/id580295142 and got an error message of " Connection Timeout".
	i tried refreshing the itunes site and the browser came up with the following error message. XML Parsing Error: unexpected parser state *Location:* *jar:file:///C:/Program%20Files/Mozilla%20Firefox/omni.ja!/chrome/toolkit/content/global/netError.xhtml* *Line Number 312, Column 50: <div* *id="ed_netReset">&netReset.longDesc;</div>*
	I tried to get access with daily trust, but site was blocked requiring certain information
	I open the page browsing page by the time I was about to continue with my browsing the browser autimatically close itselfs.
	I notice many abmornal behaviours by the time am browsing my browser was very slow the page I was trying to open was not open sometime the browser haked but by the time I close the page and re-open again I got a little changes
	Alert!
	YOUR SYSTEM HAS BEEN FLAGGED AS ONE OF THE NUMEROUS THAT NEEDS TO BE PATCHED. *The main reasons for this action are:*
	* hidden malicious code in your system. ** Invalid log on attempts by a suspected third party user.*
	Back up your login details, including your network connection password to the following folder and restart your system.
	Online maintenance Log on
Scams	*I don't have account with First Bank but they sent me this message through my email address what do u think "Dear Customer,Your First Bank Online security is still not active.Please Login below to activate your Online Banking security.Online banking Log onPlease complete your online verificationPrivacy Department.2013 First Bank Nigeria plc*
	have received a text now from the sender 'TRANSFER' that my number have been assigned =N175,000 Airtime. for my line to be loaded now,
	Please take this very seriously. People *have been receiving* *international calls from +375602605281* *or any number starting from* *+375 number one ring & hang up. If you...*

CATEGORY	DATA
	call back it's one of those Numbers that are charged N150-N200 *per minute and they can copy ur contact* *list in 3* *sec & if u have bank or credit card details* *on your phone, they can* *copy that too...But I don't know abt stealing data from mobile.... But* *call is confirm...Becau se I have got **it*** *also..* *Don't answer or call back. Please* *forward this to your friends and* *family* *Salaam every1. I received a mail notifying to complete the creation of my face-* *book account. I didn't initiate to create any new account so it has to b social engi-* *neering. It is asking me to click a link and enter a confirmation code.* *Warning!!!!!!* *PLEASE ADVISE AS MANY PEOPLE AS* *POSSIBLE: You will receive an SMS from a* *number similar to the... one that you get bank notifications* *from. The SMS will indicate a problem on your* *account and a 'consultant' will contact you.* *When the 'consultant' contacts you he/she will start* *confirming all your details and your account number* *Please let everyone know about this* *very big scam Plz pass it to others!!!!* *I received this message today from one Miss Earling Patrick, despite the fact that* *i never ever had any contact with her before.* *"Hello,* *how are you over dear in your country i hope all is* *fine am Earleen i will like to be your friend i hope* *you will not be angry with that i wait to read from* *you soon. I think this is social engineering, or how do you see guys*?
Application Download	*I visited a particular website and was required to run an online PC scanning for free. I don't feel comfortable running it because I may fall victim of one threat or the other.* *I visited a webpage and I was encountering a pop-up window asking me to down-load application for speeding up my internet connection, I resisted because I con-sidered it a trick to social engineering.* *On our University website I encountered a pop-up window asking me to download an application that upgrade the system network. When I clicked the link, I was asked to fill a form with IP address, my login password to our network, I then considered it as another social engineering.* *On my Facebook account I often encounter very interesting software applications to download but I always resist the temptation.*

CATEGORY	DATA
	Experiencing slow network and tired of frustrating waiting? Just download the speed the network application and get super speed in seconds. Log on *Download here to change your registry settings for unwanted junks, malicious codes, and many other hidden scripts that could lower the speed of your computer and network.* *Tired of being long on your system? Download these applications that could be gaming to refresh you and your system. If your download could not start automatically, please sign up to get the login code for your download.* *My friend suggested to me to watch some music online, on hailing to his advice, I was asked download upgrade version of certain unknown software, I later abandoned the site thinking it may exploit may network with the downloaded software.*
Baiting	*Hey, fals, I came across a gentleman asking me to assist him print his CV which he was to submit to the registry department.* *Yeah, I came across similar chap, but this one said he would like me to browse his flash drive to see if one of is file was there, for he was about to make a presentation to students, and he doubt whether he copied his presentation to the flash drive.* *I saw a removable device, a CD plate in its single jacket labeled "500 books and 150 music." I looked around but I could not see anybody whom I could talk to about the I picked up. So I went to it to my office and attempted to open it, then I remembered the social engineering session we had. That stopped me opening it on our corporate system, but when I reached home, I opened it on a different computer but the CD did not contain what was labeled on it, instead it contains some applications and unknown software.* *I found similar CD within our department at the far corner of the stairs leading to the library I examined it carefully, and then I said to myself this is another plant of social engineering – ready for harvesting by unknown victim. I said to myself again, well, the PhD guy had educated us enough to know this. So I did not even try to satisfy my curiosity by opening the CD, I just smash my fool on it and broken it to pieces.* *Three students-like came to my office in a rush requesting me to help them print 3 pages for them because at that moment their lecturer was busy collecting their assignments and they did not print their own earlier. I first of all asked them about their ID card to confirm they were students but none of them had an ID but said to me they all forgot their ID but next time they would be carrying them. I refused to do the printing and dismissed them.*

CATEGORY	DATA
	A visitor looking like a lecturer came into my office holding a laptop and he was talking to himself, then later turned to me complaining that he tried to login the network portal but it seemed there was problem. I asked them to see the IT people. While he was about to leave my office, he turned again said to me whether I could help him to login because there was an urgent mail he wanted to read. I said I could not help him, he turned and walked away. If it was before I would have assisted him, but now with social engineering, I am afraid. *Time without number, I have been coming across removeable devices within our premises but I either ignored them or destroyed them instantly, without exploring their contents.*
Elicitation	*I often met group of students who engaged me in conversation that inclined towards network and logging information* *Yeah, I experienced similar incidence where someone like a student kept on asking me questions upon questions on getting a free internet service within the campus so that he can be doing his assignments. I dodged his questions by asking him to go to the IT department for such network service.*

It was also discovered from the contents posted that personal affairs were not included. This further revealed commitment attitudes towards security issues. The contents came in overlapping categories from different users. For example, different users posted contents related to hoax email; and other contents followed the same pattern.

6.10 The comment conduct

The comment theme attracted divergent opinions, point of views, responses and moderations on what was posted or on existing comments. The members' comments emerged from the zeal and enthusiasms to collaborate, contribute and participate on the on-going deliberations affecting security issues. Each member of the group felt obliged to contribute a comment so as to feel responsible and committed. This was established from the studies of Gerolimos (2011) and Glazer (2012) that comment creates a sense of engagement and commitment to the maker of the comment. The five categories emerged from the

comments implied collaborations, responsibility as well accountability. These three implied attribute, though not explicitly manifested, they are however confirmed to be associated to comments as could be seen in the discussions of findings.

Figure 71: Users' Comment behaviour on the SNS model
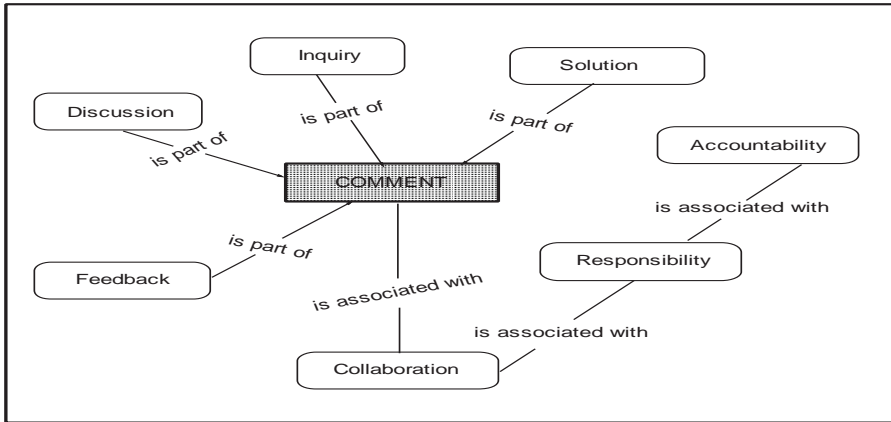
Figure 71 shows the subjects matter of the comments made by users. Four major categories were predominant in the comment. The comments made by members attracted feedback which generates discussions, and in the process of the discussions inquiries were made. The final element of the comment received solutions to the issue that attracted the comments. From the studies of Gerolimos (2011), Glazer (2012), Chester (2011), and Gray (1992), comment as depicted in figure 6.25, is attributed to responsibility, accountability and transparency. and collaboration was considered as part of user responsibility to contribute towards the security issue under deliberations. This is justified by Porter and Chester (2001) who assert that collaborations lead to responsibility, and responsibility is linked to accountability. This is further supported by Gray (1992) who claims that transparency is bonds group together for collaborative pursue that results to responsibility and accountability. The work of Velasquez (2001) is also in conformity with the interpretations

of the findings in which Velasquez found that members' contributions to an issue create collaborations that lead to responsible commitment and accountability. Further justification of the basis of this interpretation is found in the section of the discussions of findings. The following, table 6.31, shows the textual context of the comments made by users.

Table 43: Comment categories and their description

CATEGORY	DATA
Feedback	*While am trying to visit the below address, my network connection was reset*
	I go through the link and I found it to be very much informative. Many people have been misled using such tricks. Thank God that I now know something about such tricks.
	i visited the link and i been required to like the Link and even to share it to many people- this rely is kind of Threats
	I observed that the signal is too low now. But when I firt log on, it was very good.
	Hahahaha we are all aware of that we were educated on all that kind of attack i wil avoid it.
	Yes. I guess even d name sells it out
	Facebook is only one of many that have been successfully been attacked by hackers. You took best decision by contacting the lecturer before giving out the money. You seemed to be moved from unknown to known.
	From unknown to known, right?
	That is right! I used to come across such links. Sometimes I spend my time reading them, and sometimes I just deleted them.
	thankyou Sir, could have end up in the hands of terroriest,419, e.t.c....without your help....thankyou once again.
	Thank you for the info
Inquiry	*Can we try to open the link? @Malam*
	If, I received such mails can I contact their email addresses?
	Is there a maintenance upgrade on our network that requires login details?
	Pls do you know something about this? I messaged you on circle the local network. Get the app: http/discovercircle.com/ download?Sms1

CATEGORY	DATA
Discussion	*This simpleology 5.0 account is so funny. People think they can easily cheat online. It is not that SIMPLE-ology* *@ Abubakar ..ok now we r being threatain by wht i think u know, don't u think we should just let it go ?*
Solution	*This is also one of them..if u ever try it u will end up in the hands of 419 pple..believe me it's real...am telling u this by xperns ...take note* *Never try site like this is too dangerous....419 site be careful!* *Please members we need to know how we can tackle certain issues we posted that seemed complicated or disturbing.* *When I get messages saying I've won a competition or lottery I always ask myself, "How can I win when I've never taken part in it?"* *It surprises me how many people really believe they've won without taking part & excitedly respond, falling straight into the trap.* *Beware or scams.*

As could be seen in table 45, the feedback category generated comments that were centered on security issues about social engineering. The inquiry category was questions raised by users on certain security issues that needed action or further clarifications. The discussion category was opinions and analysis of users on the subject matter under review. The solution category offered advice, caution, direction or action that could be taken to avoid a threat or recognize similar encounter. The responses to comment category were acknowledged through likes, as could be seen in figure 6.26 below.

Figure 72: Users "Like" behaviour on the SNS model
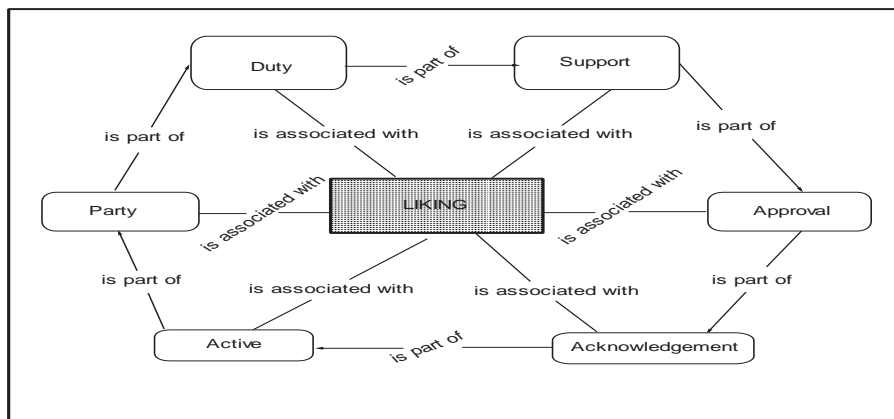
Figure 71 shows the theme: "liking" with six categories associated to it. The categories were in the pattern of relational dependency on one hand; and cause-effect relationship on the other hand. Although the categories were not explicitly emerging from the theme "like", they were implicitly deducted from the literature review on the word "like." as highlighted in the subsequent paragraph. The relational dependency could be viewed as follows: in figure 5.26, the category "party", is associated to liking, which is considered part of a "duty" to like.

In other words a member or user liking a comment or post was an indication that the user was a party to that comment or post; and being a party to comment or post indicated sense of duty. The duty in turn led a member to offer assistance where needed. The support led to approval, and acknowledgement was as a result of approval; and acknowledgement shows that a member was active. The interpretations of the above diagrammatic presentation of liking was supported by Christofides et al (2009); Lee (2012); Mattingly et al (2010); Pelachette and Kark (2010); Pampek et al (2009); Dominic (2013; Peter (2013); and Rocael et al (2012) all have interpreted like to mean various self-concept attributes.

253

On the other hand, the cause-effect relationship shows that the theme "liking" was the cause to the six categories in figure 5.26 In other words, the six categories occurred and were said to be associated to "liking". A member liked a comment or post to show that the member was active; a member liked a comment or post so as to be reciprocated, to show appreciation or approval on the subject matter under discussions. **Chien-Kuo and Buo-Han (2013) and Glazer (2012) have all agreed that the work Like is part of self-concept and associated with self-identity.**

Figure 73: Users' Sharing behavior on the SNS model
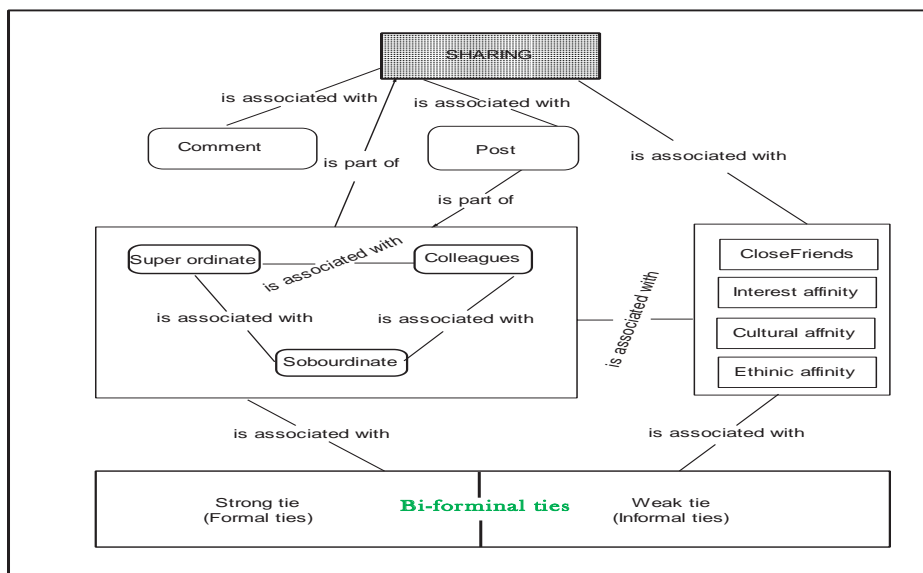
Figure 73 interpreted the sharing behavior of users on the SNS model. Sharing was the theme that was associated with two main categories: the comment and the post. In other words, users were sharing comment and post, which were shared with superiors, colleagues and junior staff; as well as to members of informal ties. This pattern of sharing is in con-

formity with the findings of Thomas et at (1998) who found that sharing is influenced by conformity or interest group influence. This is also supported by **Vygostky (1978)** who claims that sharing is a function of relationship, subjective norms, and expected relationship. Furthermore, Albrecht (1979); Jablin (1980); Falcione and Kaplan (1984) have all established sharing of information to be attributed to both the formal ties and informal ties in an organization.

This group of people was associated with strong tie. Each of the three subcategories of the strong tie were sharing comment and post to any or all of the subcategories of people who were not directly linked to the users' defined group of social network. This autonomous group was the weak tie (known in this research as informal tie). The pattern of sharing comment and post indicated that both ties (known in this research as Bi-forminal ties) feed one another, thereby enriching the contents of what was shared.

6.11 Discussions on Findings

This study found that if users are trained on SE tricks and techniques with taxonomy of learning, and structured to collaborate for security control in Bi-forminal ties, on a platform of social media of FB that facilitate social learning with encounters to SE threats, then they can be able to identify and prevent threats and attacks that are SE based either by online or offline approach. Thus, the findings rejected the first hypothesis that: *there is no significance difference in the performance of the subjects exposed to the SNS based Model in the identification and prevention of social engineering based intrusion on WLAN and those subjects who were not exposed to the SNS based Model.* The work of Jeffery et al (2005) supported the findings of this study in which their work developed an end-user security taxonomy, which maps technical knowledge with user behavior to motivate security attitudes. The test on the taxonomy revealed that a user equipped with the technical

knowhow on security coupled with desirable attitudes to security, will have intrinsic motivation to apply and comply with security policies. This is also similar to the findings of Kerry-Lynn (2006) who found with appropriate infusion of information security culture in users; security habits then become second daily activities among employees. The proposed model of this study was designed in such a way that it permeates into the interactions of users in such a way that desirable security habits are acquired and practiced. This is also supported by Helen et al (1996) who discovered that participatory approach to security is significant in supporting the technical aspect of security that is indicating weaknesses due to constant reported cases of threats and attacks. The acceptance of the alternate hypothesis that: *the subjects exposed to the SNS based Model perform better in the identification and prevention of social engineering based intrusion on WLAN than those subjects who were not exposed to the SNS based Model*.

This is inconformity with the findings of with the findings of Fin et al (2009) who developed an IS model that fit in a socio-technical system where technology, users, and managerial strategies play a role in the provision of effective security to network and the information system. Similarly, Veiga et al (2009) discovered that security implementation is only successful when user is included in security issues. This is further supported by Clifford (2006) who established that organizations should embark on more user-centred security training, that bring all onboard. The model of John (2003) which improved user security behaviour through awareness and conformity also support the findings in the alternate hypothesis that user's collaborative behaviour to security enhances security awareness and preventive measures. The findings in the first hypothesis also conformed to the findings of by Eirik et al (2010) who found that democratic – involvement of users for security

attitudes transformation through dialogue, participation and collective reflection, enhanced proactive security among users.

With regard to the second hypothesis of this study, the findings revealed that tricks and techniques of SE strategically imparted to users (as implemented in the model of this study), threats and attacks from SE were identified and counteracted. Prior to the exposure to the tricks and techniques of SE, both participants were not able to distinguish between SE threats and attacks. This collaborated the study of Furnell (2007) who studied 179 participates who were exposed to 20 latent phishing messages, and found that users failed to distinguish between genuine and fraudulent messages. However, the posttest of this study accepted the alternate hypotheses that there was a significant difference exist between the performance of the experimental group and the control group in the identification and prevention of SE threats and attacks. In other words, the strategic training yielded positive results by enabling the experimental group to identify SE threats and have taken preventive measures. This is in conformity with the study of Sheng et al (2007) who found positive effect after exposure to phishing cues among participants. In their study, participants were exposed to 20 websites without prior exposure to phishing techniques. In the middle of the presentation, the participants had a break; and during the break the group divided into three groups: one group played anti-phishing game, the second group read anti-phishing tutorials, and the other group did a different thing unrelated to phishing. The result revealed that the game group performed remarkably well in identifying phishing so also the reading group, but not as much as the game group. The study of Wright et al (2010) is in conformity with the findings of the second alternate hypothesis of this study. They found that knowledge base, experience and personality traits account for the reason why users are able to detect phishing camouflage. However, the study of Jakobsson et al (2006) contradicted

the results of the second hypothesis of this study. Their study found that 11 percent of users still went ahead to read spoofed emails, click a link, and enter their login details. This study attributed such failure to non-strategic implementation of the learning system. Again in support of the findings of this study under the second hypothesis, Kumaraguru et al (2010) developed an e-mail-based and anti-Phishing education system called "PhishGuru" and an online game called "Anti-Phishing" that teaches how to use cues in URLs to avoid falling for Phishing attacks. In the implementation of their teaching-learning model, they used instructional principles in the learning of science. They found the method effective in teaching users to identify fraudulent websites and emails, thereby coinciding with the findings of the current research.

The third hypothesis on human factor authentication was rejected thereby leading to the acceptance of the alternate hypothesis that users exposed to human factor authentication are better in the assessment of both online and offline based intrusions. With the exception of password user habits, the variables embedded in this research with respect to human factor authentication were few in the previous literature. However, the findings are similar to the authentication decision of Bezuidenhout et al (2010) in their attack detection model. Users were able to authenticate suspicious events with decision algorithms which is similar to the findings of the current research. The current research findings revealed that the experimental group performed better in authenticating intruding events, deliberately enforced by the research but appeared suspicious to the experimental group and attempted to scrutinize the request before granting access through user intervention to download software and to render assistance to a USB visitor. Username and password request through SE was turned into a human factor authentication that tested the experimental group how they approach such requests; and the revelation was the experimental group performed better than

the control group, who yielded to the request without any follow up of the request for confirmation. The findings is in line with the findings of Ka-Ping (2006) who developed log in tools and found users were cautious in password user habit in their browsing sessions.

The fourth hypothesis tested the claim of using Bi-forminal ties in sharing security experiences and encounters with either the formal or informal ties and cross-wise. The result revealed that the performance of the experimental group was better as a result of their structured interactions in the Bi-forminal ties. Thus, a Bi-formal tie has an effect on the effectiveness and successful collaboration identification and prevention of SE based intrusion on the WLAN. The findings of Olaf (2008) confirmed the results of these findings, where Olaf found that informal ties within the formal tie work relations, contributed significantly to the successful implementation of a project. The findings of Grund (2000) that network density and intense interactions between individuals increase team performance, also collaborated the findings of this study under hypothesis four. Similarly, the findings were also in conformity with the findings of Prasad and David (2013) who found that team task performance and viability are higher where teams are configured with densely interpersonal ties. It should be recalled that the findings in hypothesis four, revealed that the participants were able to perform well in collaborations for security when they are structured in Bi-forminal ties. The findings were supported by the findings of Jay (2013) that intergroup interactions promote intellectual tasks. Thus the findings in hypothesis four emphasize the need for Bi-forminal ties for successful user security collaborations for the identification and prevention of network intrusions that are SE based. This is supported by the findings of Siyuan and Jonathan (2013) that centralized critical knowledge structure have negative relation to executive-related team performance. In other words, if one formal structured is used in the collaborative efforts, the performance would not yield func-

tional results. This is supported by Kelman (1958) who found that people's actions and thoughts are influenced by the group they attached to. Thus the significant of the findings in the Bi-forminal ties is the more users are structure into Bi-forminal ties, the more they enthusiastically and passionately collaborate for security controls.

With regards to the use of FB functionalities to interact and socialize for security collaborations, the findings revealed that experimental group performed better in the use of the functionalities to identify and prevent SE based intrusion on their network. This findings is in conformity with the findings of Arjan et al (2008); and Evans et al (2009), who found that the use of social media FB (functionalities) improve knowledge creation, collaborations, feedback and sharing of resources. Similarly, the findings of Similarly, Chien-Kuo and Buo-Han (2013) supported this finding where they found that the use of FB functionalities generated live discussions among their study participants and thus most members were active and participatory to the project of their study. The findings thus confirmed the use of FB for collaboration with ease and simplicity as confirmed by the findings of Ractham and Daniel (2011), who found that using FB functionalities, learners leverage social networking with knowledge creation, discussions, and sharing learning experiences. The findings in using FB functionalities have revealed knowledge facilitation and improved security awareness among users. This is confirmed in the findings of Terence et al (2009), who found that the use of FB functionalities improve learners' communication skills and awareness. Likewise the studies of Rocael et al (2012) found that the use of FB functionalities enhanced their learning process through sharing and scaffolding knowledge. The finding in this study is significant in the provision of collaborative tools that create a system of security for the users, by the users, and of the users. This is in conformity with

the findings of Daniel (2011) that FB functionalities made learning and collaboration easier and created sense of ownership and belongings among their study participants.

With regards to the findings on the attitudes of the participants on the use of the SNS based model, the participants exhibited the expected conducts in the identification and prevention of SE based intrusion into their WLAN. Their postings, comments, sharing, and "likes" all contained and indicated SE threats, issues, and actions as countermeasures. The significance of this finding is that transparency in security collaborations is exhibited through the implementation of the SNS based model. For instance, the various comments made by participants were centred on SE security issues and the implication of this finding is that live and active implementation of security measures is achieved. This is in line with the findings of Yan et al (2013) who found that online collaborative activities build and sustain a community of live and active participants. This is indeed how security is supposed to be on the social aspect. The findings on the attitudes of the users also indicated unified efforts to contribute to security with enthusiasms and interest, unlike issuance of security policies to users that makes users dormant and noncompliance. The findings are conformity with the findings of Kelman (1958) that the quest for identity intrinsically motivate and extrinsically drive an individual to participate and contribute to collaborative actions.

The implication of the findings on the attitudes of the participants while implementing the SNS model has supported that the claim of this research that when users participate on a social media platform to collaborate on SE based security measures for their network, the collaborations will support the technical system of security, thereby enhancing and balancing security approaches from both the technical and the social system. This is supported by the claim of Mortorolla (2012) that security is a social system and should as well

have a social system approach. The findings on the attitudes of the participants while implementing the model is also supported by the findings of Thomas et al (1998) found that transfer of knowledge is best effective in SL situation. Thus security experiences and encountered can best be transferred among users if a system of collaborative security is established.

One other fundamental implication in the findings of this study is that the social media of FB is the most ideal platform for countermeasures on SE based collaborations among workforce. FB platform is full of SE threats and attacks. If it was not on the FB the SNS model was implemented, the nature of the context posted, shared and commented by the members would not have been on SE issues, or might be less and very few. This is supported by the findings of Wang (2010) that web-based learning is ideal for learning system that promotes sharing of knowledge and resources. It is the aim of the SNS model to update users' knowledge base on the social system of security through sharing of experiences, encounters, and learned security issues. Another implication in the findings is that the SNS model is live platform for knowledge acquisition and application. Unlike the training programs proposed by previous research that make user security habit seasonal and reactive, the findings in the attitudes of the users while implementing the model has demonstrated the ability of the model in transforming the user into proactive habit to security, with a revolving platform for knowledge acquisition and application. This is supported by the findings of Stefan (2008) that a social media learning system is not a reservoir of knowledge for the instructor to his subjects but rather an opportunity for the subjects to interact, collaborate and share resources among themselves. The findings of this study is also in line with the findings of Fredericksen et al (2000) that effectiveness of learning depends on learners' interactions, participations on the subject matter, and feedback process. Previous

262

studies proposed training the user. This is not enough without providing the user with an ongoing, up-to-date, live, and continues learning process, which the SNS model has proved effective in the findings. This is supported by the study of Hiltz et al (2000) who found that participants on collaborative group perform better than those on instructional group. it is also in conformity with the findings is the study of Astin (1996) who confirmed that the more learners interact with one another on a subject matter, the more the learning outcome and the better the performance of the learners in the application of the knowledge acquired, or experience gained. Thus, the finding of this study has implications on issuance of instructional policy or user security awareness by confirming the insufficiency of such approach to counteract the social systems of intrusion.

6.12 Conclusion

The approach of this research to security solutions for intrusion into Wireless LAN differs from other non-technical approach that focused on administrative, managerial, and policies for user control and applications. While training the user was the main focus of most scholastic approach to non-technical system of securing the network and information resources, this research not only provided a unique system of training that is real-time and online through the platform of social networking on Facebook, which is popular and prone to rampant social engineering threats and attacks; but also provides a Bi-forminal structure of interactions that enable users to participate and collaborate freely for security issues.

Moreover this approach is unique in the system of imparting knowledge and developing Intrusion prevention competencies, by the use of Blooms taxonomy of learning. Security issues must be on-real time and a continuous process. If the user is to be turned into such condition, then the teaching-learning contents must be blended with three domains of psychomotor, motor and affective (knowledge, skills, and applications). Blooms taxonomy

of learning is effective and appropriate in achieving the system of training aimed to blend the leaning materials with the three domains. Previous studies focused on only one of the domains, while the current research went further and used all the domains for building SUCU (security unconscious competence user).

Moreover, while previous approaches to network and information security limit user monitoring obscured, this research provides real-time monitoring system on user contribution and participation to security issues. The model of this research made user participation transparent, accountable and responsible. The social networking platform reveals the user through post, comments, discussions, likes, and sharing on security issues.

The pre-post test of this research, therefore, showed that the model of the research was effective in providing a security system that is collaborative, participatory, on real-time with continuous learning process on social engineering threats and attacks that are rampant on social networking sites of Facebook. The control group mainly remained unchanged in the pre-post test. Thus the effect of the SNS model has created a socio-social system of security that complements the technical system of security for intrusion prevention on Wireless LAN.

A number of reasons account for the use of social engineering to attacks information and network resources. One of such reasons is the increasing sophistications in the technical solutions to security that a hacker takes longer time and efforts to crack a system. Secondly, security professionals and practitioners have engineering background and approach security solutions with technical bias.

Thirdly, scholars in information and network security pay less attention to the social system of security, thereby leaving a wider gap that turns the user as the weakest link in the security system. The SNS model has proved effective in providing a socio-technical system

of security that address the escalating social engineering threats and attacks on our Wireless LAN, which is used as gateway to web sites and internet resources of workforce of an organization.

6.13 Summary

This chapter has presented the empirical findings from both the quantitative data and the qualitative data. The quantitative findings were presented in tables as t-test results of the findings. The statistical results implicitly interpret the findings. Bar Graphs were used to further show the extent of the differences between the two groups, as revealed by the statistical analysis. The qualitative findings were presented in tables and analyzed by diagrams. The analysis of the qualitative findings runs concurrently with the discussions on findings; and linking the findings of the current research with similar empirical findings in the literature. The discussions on findings on the quantitative findings were done separately and similar empirical findings in the literature review were referred to for validating the findings in the current study. The overall quantitative findings of the study revealed that there is significant difference between Wireless LAN users exposed to the SNS based model and those who were not exposed to the model in the prevention of SE based intrusion on Wireless LAN. This revealed that the model is effective in contributing to wireless security in a real-time proactive security approach. The qualitative findings revealed the dominance of security based contexts and interactions in the implementation of the model by the participants on the social networking platform of FB.

The findings revealed that both formal tie connections and the informal tie connections were able to interact collaboratively for the security of the Wireless LAN. This implies that structural pattern of interactions is significant in collaborations for security matters. Thus generally the findings have contributed in complementing the technical system

of security in an approach that designs security for the users, by the users, and for the users, in real-time, proactive, and pragmatic controls.

CHAPTER 7:   Summary, Conclusion, and Recommendations

7.1   Summary

The subsequent sections under 7.1 give the summary of this research. The summary contains the background of the research, problems statement and the research question addressed in this research. The section also summarized the methodology used with brief summary of the findings, and the implications of the study. Thus, while using the Wireless LAN of an organization to visit web sites and the internet, users encounter unknown social engineering threats and attacks that compromise their network and information resources. The SNS model imparted the knowledge of social engineering threats and attack only to the experimental group of the study. They were tested together with their counterparts – the control group, on how to identify and prevent social engineering based threats and attacks. The test covered both online real-time activities and offline environmental activities.

The subjects were also tested on how they use the social media of Facebook as a platform for counteracting the threats and attacks, through noncompliance to the social engineering threats. Similarly, the subjects were tested on using the social network platform to report, discuss, share and inform the social network about suspicious events and threats experiences. The test scores were computed statistically to test the hypotheses of the research. The activity of the users on the social media platform of Facebook was also analyzed qualitatively and interpreted so as to give meaning to the implication of the activities the SNS model has been found to be effective for the purpose it was proposed. The subjects displayed security skills while collaborating for security on the platform social media of Facebook.

7.2 The background of the study and the Research Question

The main philosophy of undertaking this research is to provide a complementary solution to the existing automated software solution to Intrusion Prevention on Wireless LAN. The state-of-the-art in the field of this research revealed that much research has been done in the implementation of technical system of security, but little has been done in the area of non-technical system. The few studies on the non-technical system differ with this research in approach and methodology. The too much reliance on automated and encrypted system for Intrusion Prevention (IP) on Wireless network and coupled with a liaises-faire attitude on the user aspect of network security, resulted to an escalating attacks on WLAN through social engineering. Social engineering is the use of Human ingenuity to manipulate, deceive, or persuade the user of network and computing services to give out vital information or perform certain actions that are indirectly of benefit and advantage to the hacker. The main research question this research attempted to address was: *What is the effect of the SNS based model in the identification and prevention of social engineering based intrusion on Wireless LAN in an organization?; and what is the attitude of the users of the model on the social media platform of Facebook?*

In a rapidly changing world of technology, the life cycle of security devices/technology is becoming shorter and shorter, that today's innovation (or security solution) will be tomorrow's clone. Furthermore, increasing styles in social engineering is putting enterprise to a position of weaker opponent in the fight for threats and attacks. The traditional way of securing the WLAN is the formation and implementation of policies by the head of Network security or network administrator; or procuring and installing the necessary software and technologies to ensure that the network is safe and secured. The expansion of office activities and the digitalization of office functions raised the demand for

more hardware devices used in the office. This adds up to the existing numerous, and tedious work of security on network administrators.

WLAN (Wireless Local Area Network) uses radio signals to send and receive data within short distance between and among devices enabled with wireless communication. The flexibility, mobility and the numerous advantages associated with Wireless network, and coupled with the deployments of e-of-things in financial, health, and business sectors have led to the proliferations of wireless network in Africa and Nigerian society in particular. This development has in turn resulted to escalating rate of attacks on WLAN. Proliferations of Wireless networks have come with increasing need for security. Despite the fact that there are more security technologies for protecting WLAN, yet attacks on Wireless LAN continue to increase. Today's workforce uses the Wireless LAN to access web sites and the internet. There are regular reported cases of network attacks on the web, through media stations and personal experience. Some organizations may not even notice that their network is attacked, until some period of times, perhaps two or more years. Security vendors, universities, academicians, and researchers are daily bringing new solutions for counteracting attacks. The solutions are so powerful and sophisticated enough that attackers find it difficult and tedious to break them and gain access to the network and information resources. This frustrated attackers to find easy and less tedious ways to carry nervous activities. Social engineering is the new and common way attackers are using nowadays. Network is meant to be used by people as such attempts to provide security to the network must as well be approached both with the technical and social systems.

The tasks of security administration require performance of numerous tasks ranging from daily monitoring, software updates, patches, to planning and decision making. Qualified and experienced security personnel are scarce in most organizations thereby relin-

quishing the job of security administration to the network administrator who may find it tedious and difficult to combine the two jobs satisfactorily. The organizations that have qualified security personnel also face the challenges of effective security administration. This opens more gaps for attacks through non-technical vectors or through the user. The concentration of security measures are more on technical and software solutions with little or no attention to non-technical or social system thereby creating a gap to the security of network and information resources.

This research addressed the gap created by previous studies with bias to the technical system of network security. The non-technical system of security is the favourite attack channel by hackers. In the non-technical system of security, the user is an important component of Wireless LAN, yet less attention is given to user thereby making the user the weakest link in the fences of network and information security. Technical and automated software solutions dominated or outweighed the non-technical systems of security solutions. This research proposed, implemented and tested the SNS (Social Network Security) based model in the attempt to fill the gap created by the state-of-the-art approaches to security in favour of technical security, which over shadows the non-technical system of security. The subsequent section summarizes the methodology used to implement the model. The model provides a balanced system of security, in a way that has not been done before, so as to complements the technical and automated software solutions to security on Wireless LAN.

7.3 Methodology

A combination of quantitative and qualitative research methods were used in this research. In the quantitative method, between groups experimental design was used; and in the qualitative method, content analysis was used. This research consists up of three stages.

The first stage was the implementation of the SNS model through imparting knowledge and skills of social engineering based threats and attacks. The population of the research was the users of Wireless LAN in UMYU (Umary Musa Yaradua University) main campus. The subjects of the experiments were statistically chosen through random sampling, and they made up of eighty participants. The participants were then randomly assigned to experimental and control groups. Blooms taxonomy of learning was applied in disseminating the knowledge and building the skills and competencies of social engineering threats and attacks in the experimental group of the research. The second stage of the research was the administration of pretest and posttest to both the experimental and the control groups. Test of validity and reliability were carried out to achieve both internal and external validity. The test consists up of fifty questions in sixty responses which were answered through multiple choice and fill in the blank. Most questions refer the subjects to a website, their emails, or their Wireless devices, and surroundings before an answer is chosen or provided. Thus, the data collection method was the tests administered to the subjects of the research. T-test for independent sample was used to analyze the data. The third stage in the implementation of the SNS model was content analysis on the activities of the subjects on the social network platform of Facebook. Facebook functionalities were used as existing themes. Five man coders were used to assign the activities of the subjects into categories. Test of reliability was used to establish the consensus of the coders on assigning the activities into their respective categories.

The university environment of UMYU (Umary Musa Yarasua Katsina state, Nigeria) was chosen to conduct the experiment of implementing the proposed SNS based model of the research. University environment is ideal for the research because the environment consists up of various organizational structures and settings common to many organisations

and enterprises. Moreover, the environment consists up of various calibers of people from different background, experience and orientation, thereby provided the enabling social settings appropriate for the conduct of the research.

Many studies have used social network for sort of things, but this pattern of study to wireless security is new and a promising one. This research used experimental study to test the proposed model by exposing the model to the experimental group only for a period of 18 weeks. In order to achieve internal validity between the two groups, a pre-test was given to the two groups to ascertain their level of ICT proficiency. The results of the pre-test revealed the two groups were equal in terms of ICT proficiency. To further establish external validity, random assignment software was used to assign the participants to either the experimental or the control groups. After the exposure of the model to the experimental group was completed, the two groups sat for a post test. The results of the posttest were used to answer the research question of this research and tested the research hypotheses. An existing social network platform (the Facebook) was used to operate and apply the model in the identification and prevention of threats and attacks that are social engineering based. Content analysis was used to assess the behaviour of the participants on the platform of the model.

The training was given in the form of lectures, simulations, demonstrations, and role plays. Teaching aids, network and web resources were used in imparting the required knowledge, skills, and competencies to the experimental group. The Socio-technical theory was used as a theoretical framework for this research. The theory served dual purpose in the formulation of the research question, in one hand, and the construction of the SNS model, on the other hand. The theory purported that organizational problem exist either from the technical system or the social system, and solutions to organizational problems

272

could be approached and solved where both the technical and the social systems support and complement each other. Against this background, the research modified the theory and substituted some constructs existing in the socio-technical theory with formal and informal ties. This research came up with Bi-forminal ties as a structure and pattern of interactions users can engage for social networking to share knowledge, experience and encounters on both online and offline social engineering threats and attacks.

7.4   Conclusion

This research implemented SNS based model for the identification and prevention of social engineering based threats and attacks in Wireless LAN of an organization. This research has not only provided a socio-technical system of security that complements the technical security but as well has turned users into shield against compromising the security objectives of CIA (Confidentiality, Integrity, and Availability). Thus, this research has presented a socio-technical system for Wireless LAN security opening possibilities for further work.   The major findings of this research were two folds: in one hand the online and offline threats and attacks were identifiable and recognizable by users after exposure to the SNS model. Prior to the exposure of the model, the participants, both the experimental and the control groups could not identify or recognize the least threat both online and offline. However, after the exposure of the model to the experimental group, the group was smarter in recognizing threats; while their counterparts – the control group still remained the same as they were at the pretest level with the experimental group. The findings were from the performance of the posttest as well as the activities of the experimental group on the social network platform of the model. On the other hand, the training given to the users on the various online and offline social engineering tricks and threats, have facilitated and encouraged users to be alert and vigilant on their online activities as well as offline interactions.

The conventional way of protecting the network and the information resources against threats and attack is to buy the most advanced technology or the latest threats detection systems. This research has found that effective security system could be achieved with the involvement of the users. Technology and policies are only useful and effective when users of the technology are involved in the security of the network and the information resources. If users are given the right training and users collaborate on social networking platform, then the threats and attacks that bypass the technical system can be detected and mitigated. Thus, the research serves as a complementary solution to the technical system of security. The model tested in this research established that implementation of the model give users spiral learning platform that develops their skills and competencies to counteract social engineering threats and attacks. The findings of this research have been supported by professional and scholars in the field of network and information security. Notably, Diana (2013) asserts that just like driving a car requires multiple parts working together, "driving" a corporate IT network safely requires a blend of the traditional triumvirate: people, process and technology. Similarly, Keibler (2013) says it is too late an action to rely on the endpoint to stop all the malware. A more effective approach is to start with employee awareness, partner with employees and help them to be another arm of the security program. Keibler (2013) added that there are some social engineering components in 70 to 80 percent of attacks. This research does not only impart the knowledge and skills of social engineering threats and attacks, but also provides a structure in social network platform that bring users to interact and collaborate irrespective of their social tie connections.

The approach of this research to security solutions for intrusion into Wireless LAN differs from other non-technical approach that focused on administrative, managerial, and policies for user control and applications. User training was the main focus of most scho-

lastic approach to non-technical system of securing the network and information resources; and the training approach in the previous studies focused on the does and don'ts, likewise training in organizations follow the same pattern. This research not only provides a unique system of training that is on real-time, practical and online, but as well provides a Bi-forminal structure of interactions that enable users to participate and collaborate freely for security issues. This achieved through the platform of social networking on Facebook, which is popular and prone to rampant social engineering threats and attacks. Thus the model proposed in this research integrated security theory and practice. Users learn faster and are enthusiastic to put into practice the knowledge they acquired so far the knowledge presented is logical, coherent and on a platform that provides opportunities for further learning.

Therefore the SNS model is unique in the system of imparting knowledge and developing Intrusion prevention competencies, by the use of Blooms taxonomy of learning. Security issues must be on-real time and a continuous process. If the user is to be turned into such condition, then the teaching-learning contents must be blended with three domains of psychomotor, motor and affective (knowledge, skills, and applications). Blooms taxonomy of learning is effective and appropriate in achieving the system of training aimed to blend the leaning materials with the three domains. Previous studies focused on only one of the domains, while the current research went further and used all the domains for building SUCU (security unconscious competence user). The need for ongoing training for users to identify and mitigate the ever evolving social engineering threats and attacks is possible through the model of this research. The structure of the SNS model provides the platform for regular learning opportunities. While previous approaches to network and information security limit user monitoring obscured, this research provides real-time monitoring system

on user contribution and participation to security issues. The model of this research made user participation transparent, accountable and responsible. The social networking platform reveals the user through post, comments, discussions, likes, and sharing on security issues. ***Thus, by the model of this research, this research has contributed to knowledge by approaching security issues that other researches in the state-of-the-art have not considered; and this research has added to knowledge in a way that has not been done before.***

7.5 Limitation and Recommendation for further Study

Although social engineering threats and attacks are common phenomenon in any organization, implementing the proposed SNS model on different informal connections can widen the resourcefulness of the diversity of informal connections and achieve more user competencies.. The resources and the time limit, within which this research has to be completed, could not be sufficient to create more groups so as to achieve wider collaborations and gain more resources that build user competencies. ***Thus, it is recommended that future research should focus on wider application of the model among different groups and under different platforms of social medial or intranet system; with informal connections, thereby opening opportunities for further work.***

7.6 Recommendations

The subsequent sections under 7.3 offer recommendations both for further research and applications of the findings of this study in security implementations. The section also offers recommendation on academic curricula in the teaching-learning system of cyber and information security in Universities and tertiary institutions.

7.7   Equal priority to Human Component on security matters

An organization is a socio-technical system that comprises up of people and technology. The driving force of organizational functions in today's internet-of-things is ICT (Information and Communication Technology). The technology exists for the people, by the people and of the people. Thus the social system and the technical system must blend together to provide a system that is complementary and supportive to each of the system. The user has a great role and responsibility to play in the confidentiality, integrity and availability of the network and information resources of his/her organization. The attainment of these three fundamental pillars of security could not be actualized by partial or documentary policies. The user must be recognized as an indispensable component of the Wireless LAN that is prone to threats and attacks at any point.

7.8   A balanced Socio-technical system of Security

A balance should always be maintained between the technical and non-technical systems of security. If the social system is neglected and more priority is given to the technical system as highlighted in background of this research, then any or all of the security objectives of CIA can be compromised through the user; likewise if priority is given more to the social system, the technical system of attacks will compromise the network and information security of an organization.

The technical-automated software solutions monitor programs running on a system or network, incapable of detecting human tricks and threats. The modern way of attacking a network is by using the legitimate user to execute malicious programs. The user must not only participate in the security matters, but as well must interact actively and on real time to see, detect, act and share encounters and experience with colleagues and associates. Users are the producers, processors, and consumers of network and information resources and

any security attempt that sidelined them could not succeed entirely. Success to security solutions can only be realized where users feel a sense of ownership in the security affairs. The technical system should not overshadow the non-technical issues and each one should complement the other. All those concern with security issues in organizations should consider this recommendation, uphold and implement it.

7.9   A course on social engineering for IT and Computer science Programs

The security topics taught to students in Universities and tertiary institution should have dedicated core course on social engineering. Social engineering is maturing and is becoming more sophisticated. Social engineering threats and attacks remain hidden and unknown to many IT and computer science professionals. Keibler (2013) found that in every ten threats and attacks, 80% of them are from social engineering. Therefore in order to tackle the problem of social engineering from the grass roots, dedicated and core course on social engineering is not only desirable but highly essential in the curriculum of cyber security and IT security, in our Universities and tertiary institutions.

7.10   Social Network Security based Model for Network and Information security

Social networking is revolutionizing all aspects of human and enterprise activities. In an increasingly globalized and digitalized world, social relations is becoming a day affair in bringing people closer for communication, transactions, awareness, and collaboration on matters of interest. Embracing social networking in the work place is not just a nice frill, but a necessity. As more and more office workers are joining various social networking, enterprise must turn such trend to opportunity and advantage. In an increasingly globalized and digitalized world, social relations is becoming a day affair in bringing people closer for communication, transactions, awareness, and collaboration on matters of inter-

est. Embracing social networking in the work place is not just a nice frill, but a necessity. As more and more office workers are joining various social networking, enterprise must turn such trend to opportunity and advantage. Attackers and hackers are now using social engineering to gain access to information and network facilities and/or devices. Paying scrupulous attention to turning social networking to an opportunity will be a significant way for enterprise to fight the escalating attacks on WLAN. As a result of rapid proliferation of mobile technology devices coupled with rapid spread of social media, every office worker is said to be on the average as far as ICT (Information and Communication Technology) is concerned. This brings home the need for the office worker to be integrated in the issue of security of WLAN. Thus with the level of ICT literacy among office workers (the users of network and IT resources), the need for active collaboration among the work force is desirable and appropriate.

Social networking is revolutionizing all aspects of human and enterprise activities. In an increasingly globalized and digitalized world, social relations is becoming a day affair in bringing people closer for communication, transactions, awareness, and collaboration on matters of interest. Embracing social networking in the work place is not just a nice frill, but a necessity. As more and more office workers are joining various social networking, enterprise must turn such trend to opportunity and advantage.

Attackers and hackers are now using social engineering to gain access to information and network facilities and/or devices. Paying scrupulous attention to turning social networking to an opportunity will be a significant way for enterprise to fight the escalating attacks on WLAN. Attackers and hackers are now using social engineering to gain access to information and network facilities and/or devices.

CHAPTER 8:   References

The followings are the various authors and scholars consulted in their literature for proper understanding of the research problem and identification of a gap in literature.

References:

Abraham, S. & I. Chengalur-Smith (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, 2010. **32**(3)

Abu-Nimeh, S. (2008), "Phishing detection using distributed Bayesian additive regression trees", unpublished doctoral dissertation, Southern Methodist University, Dallas, TX.

Adman, P., & Warren, L. (2000). Participatory sociotechnical design of organizations and information systems - an adaptation of ethics methodology. *Journal of Information Technology,* 15(1): 39-51.

Alessandro A. & Ralph G. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. Privacy Enhancing Technologies Lecture Notes in Computer Science *Volume* 4258, 2006, pp 36-58.

Al-Mudimigh, A., Zairi, M., & Al-Mashari, M. 2001. ERP software implementation: An integrative framework. , 10(4): 216.

Anderson, K.B., Durbin, E. and Salinger, M.A. (2008), "Identity theft", *Journal of EconomicPerspectives,* Vol. 22 No. 2, pp. 171-92.

Anderson RH. (1999). Research and development initiatives focused on preventing, detecting, and responding to insider misuse of critical defense information systems. In: *Paper presented at the results of a three-day workshop,* RAND, Santa Monica, CA.

Arjan, H., & Harshrne, R. (2008). Investigating faculty decisions to adoptWeb 2.0 technology: Theory and empirical tests. *Internet and Higher Education*, *11*, 71–80.

Astin, A. W. (1996). Involvement in learning revisited: Lessons we have learned. *Journal of College Student Development*, 37(2), 123–134.

Audit Commission, (1994). *Opportunity Makes a Thief, An Analysis of Computer Abuse* Audit Commission, UK, London.

Avgerou, C. (2001). The significance of context in information systems and organizational change. *Information Systems Journal* 11 (1):43-63

Avgerou, C. (2002). The socio-technical nature of information systems innovation, In *Information systems and global diversity*, edited by C. Avgerou: Oxford University Press, USA.

Baker, W. E. (1992). The network organization in theory and practice. In N. Nohria, & R. G.Eccles (Eds*.), Networks and organizations: Structure, form, and action* (pp. 397–429).Boston: Harvard Business School Press.

Barsanti C. (1999). Modern network complexity needs comprehensive security. Security *1999;36(7):65–8*. http://www.bbc.co.uk/news/technology-10713199[Accessed: 14/02/2012].

Basgall, M. "Experimental Break-Ins Reveal Vulnerability in Internet, Unix Computer Security."http://www.dukenews.duke.edu/research/encrypt.html, January 1999.[Accessed: 14/05/2012].

Bargadiya, M., Chaudhari, V., Khan, M.I. and Verma, B. (2010), "The web identity prevention: factors to consider in the anti-phishing design", International Journal of Engineering Science and Technology, Vol. 2 No. 7, pp. 2807-12.

Beach, L.R. (1993). *Making the right decision. Organizational culture, vision and planning*Eaglewood Cliffs, New Jersey : Prentice Hall.

Belinda S. and Brandis P. (2013) Social Networks, Interactivity and Satisfaction: Assessing Socio-Technical Behavioral Factors as an Extension to Technology Acceptance: *Journal of Theoretical and Applied Electronic Commerce Research, Vol. 8, Issue 1, 35-52.*

Berghel H., (2003). Digital village — malware month. *Communications of the ACM*, 46(12), December 2003

BBC News. (2013) Adobe hack: Atleast 38 million accounts breached. http://news.bbc.co.uk/I//technology/-24740873. [Accessed: 30/10/2013].

BERR. (2008)Department for business Enterprise and regulatory Reform (BERR) information security breaches survey 2008, http://66. 102.9.132/search?q¼cache:LK4aPYKu4gcJ:www.berr.gov.uk/ files/file45714.pdfþberrþ2008þbreaches&;cd¼42&hl¼en&ct¼ clnk&gl¼uk; 2008 [Accessed: 11/07/2012].

Berti, J. and Rogers, M. (2004). *Social engineering: the forgotten risk.* Information security management handbook – fifth edition. Boca Raton : Auerbach Publications.

Bézivin, J. and Gerbé, O. (2001). *Towards a Precise Definition of the OMG/MDA Framework*, in *ASE, Automated Software Engineering*.

Blau, P. M. (1954). Patterns of interaction among a group of officials in a government agency. *Human Relations*, 7(3), 337–348.

Bloom, H.S., Kemple, J., Gamse, B. , and Jocob, R. (2005). Using Regression DiscontinuityAnalysis to Measure the impacts of Reading First. Paper presented at the annualConference of the American Educational Research Association held in Montreal, Canada.

Bezuidenhout, M., F. Mouton, and H.S. Venter. (2010*). Social engineering attack detection model: SEADM*. in *Information Security for South Africa (ISSA),*

Bogdan H. (2008). Phishing Attacks and Countermeasures: Implications for Enterprise Information Security. *Info-Science on Demand*.

Boshmaf, Y., Muslukhov, I., Beznosov, K., Ripeanu, M. (2011). The socialbot network: When bots socialize for fame and money. *ACSAC*.

Bostrom, R. and Heinen, S. (1977). MIS Problems and Failures: A Sociotechnical Perspective.*MIS Quarterly*, (September) 17-32.

Broderick JS. Information security risk management – when should it be manged? Information Security Technical Report2001;6(3):12–8.

Brody, R.G., Mulig, E. and Kimball, V. (2007), "Phishing, pharming and identity theft", Academy of Accounting and Financial Studies Journal, Vol. 11, pp. 43-56.

Brown, J.S., Collins, A. and Duguid, P. (1989), "Situated cognition and the culture of. learning", *Educational Researcher*, Vol. 18, pp. 32-42

Carayon P. and Karsh, B. (2000)Sociotechnical issues in the implementation of imaging technology, *Behavior & Information Technology* 19(4), 247–262.

Carayon, Pascale, & Karsh, Ben-Tzion. Jun2000. Sociotechnical issues in the implementation of imaging technology. *Behaviour & Information Technology, 19(4): p247-262.*

Carl C. (2009). Human factors in information security: The insider threat - Who can you trust these days?

Carlos, J., Bernardos, Ignacio, S., and Maria, C., (2010). IPv6 Network Mobility. *The Internet Protocol Journal – Volume 2, No.2*

Ceesay, E.N. (2008), "Mitigating phishing attacks: a detection, response and evaluation framework", unpublished doctoral dissertation, University of California, Berkeley, CA.

Charles D. (2010). Exploring the Potential of Social Network Analysis in Asset-based

Community Development Practice and Research*Australian Social Work* Vol. 63, No. 4, December 2010, pp. 404_417

Chai, S., & Kim, M. (2012). A socio-technical approach to knowledge contribution behavior: An empirical investigation of social networking sites users. *International Journal of Information Management*, 32(2), 118–126.

Chen, T.-C., Dick, S. and Miller, J. (2010), "Detecting visually similar web pages: application to phishing detection", ACM Transactions on Internet Technology, Vol. 10 No. 2, 38 pages (article 5).

Chetan, S., & Gurpreet S. W. (2013). Capturing HTTP Protocol Packets in a Wireless Network. International Journal of Wired and Wireless Communicaions, Vol.1, Issue 2.

Chidley, J. (1995). Cracking the Net *MacLean's,* May 22, pp 54-56

Chien-Kuo T & Buo-Han L. (2013). Applying Facebook as a Management Method for the Teachning Platform to develop product design.

Christine L. and Michel B. (2010)"Probabilistic localization and tracking of malicious insiders using hyperbolic position bounding in vehicular networks.*" EURASIP Journal on Wireless Communications and Networking,* Volume 2010.

Chu, S.-C. (2011). Virtual advertising in social media: Participation in Facebook groups and responses among college-aged users. *Journal of Interactive Advertising*, 12(1), 30–43.

Ciampa, M.D. (2008), "The impact of computer security policy content elements on mitigating phishing attacks", unpublished doctoral dissertation, Indiana State University, Terre Haute, IN.

Clifford M. (2008). Approaches to user education, *Network Security*, Volume 2008, Issue 9, September 2008, Pages 15-17, ISSN 1353-4858,

Coles-Kemp, L., & Theoharidou, M. (2010). Insider Threat and Information Security Management. In *Insider Threats in Cyber Security.* (pp. 45-71). Springer. doi: 10.1007/978-1-4419-7133-3_3

Cohen, L., Manion, L., Morrison, K., (2011). Research Methods in Education. Routledge Publishers, 7th ed.

Comesongsri, V. (2010), "Motivation for the avoidance of phishing threat", unpublished doctoral dissertation, The University of Memphis, Memphis, TN.

Conti, M. et al (2009), "Mobility and cooperation to thwart node capture attacks in MANETs"*URASIP Journal on Wireless Communications and Networking Volume 2009 (2009), Article ID 945943*

Contos, B. T. (2006). Enemy at the water cooler: Real-life stories of insider threats and enterprise security management countermeasures. Rockland, MA: Syngress.

Cooper J., Gencturk, N. and Lindley R.A. (1996). A sociotechnical approach to smart card systems design: an Australian case study, *Behavior & Information Technology* 15(1) (1996), 3–13

Cummings, T.G. and Worley, C.G. (1993) *Organizational Development and Change*, 5th ed., West Publishing Co., Minneapolis, MN, pp. 352-6.

Cummings, T. (1981) "Designing effective work groups", in Nystrom, P.C. and Starbuck, W.H (Eds), *Handbook of Organizational Design: Remodeling Organizations and Their Environments*, Vol. 2, Oxford University Press, Oxford, , pp. 250-71.

Czernowalow M. Lack of policy causes IT risks. Available from: ITWEB, http://www.itweb.co.za> [accessed 07.08.12].

Dlamini, M.T. Eloff, J.H.P. Eloff M.M. (2009). Information security: The moving target, *Computers & Security, Volume 28, Issues* 3–4, May–June 2009, Pages 189-198, ISSN 0167-

Dang H. (2008). The origins of social engineering. *McAfee Security Journal*; 2008. Fall.

Daniel, F., Stefan, F., & Lukas, L. (2013). Toward web-based information security knowledge sharing. *Information Security Technical Report*, Volume 17, Issue 4.

Darrell K., and Matthew C. E., (2003). Recent worms: A survey and trends. In *Proceedings of the 2003 ACM workshop on Rapid Malcode. Washington, DC, USA*, pages 1–10, 2003. ISBN: 1-58113-785-0.

Davenport, E. (2008). Social informatics and sociotechnical research--a view from. the UK. *Journal of Information Science* 34 (4):519

David, H., Toby, D., Chris W. (2003). *The New Workplace: A guide to the Human Impact of modern working practices*, John Wiley & Sons, Ltd.,

David, M. L. (1993). Online Statistics Textbook http://davidmlane.com/hyperstat/ [Accessed: 11/03/2012].

Davies, H., Leung, T.K.P., Luk, S.T.K., and Wong, Y.H. (1995). The Benefits of Guanxi: The Value of Relationships in Developing the Chinese Market, *Industrial Marketing Management* (24), 1995, pp. 207-214.

Davinson, N. and Sillence, E. (2010), "It won't happen to me: promoting secure behaviour among internet users", Computers in Human Behaviour, Vol. 26, pp. 1739-47.

Day, R. E. (2007). Kling and the critical: Social informatics and critical informatics. *Journal of the American Society for Information Science* 58 (4):575-582.

De Nooy, W., Mrvar, A., & Bategelj, V. (2005). *Exploratory social network analysis with Pajek: Structural analysis in the social sciences*. New York: Cambridge University Press.

Deloitte, Touche, Tohmatsu. Global security survey. Available at: www.deloitte.com. 2005.

Dhillon G, Backhouse J. (2000). Information system security management in the new millennium. Communications of the ACM 2000;43:125e8.

Dholakia, U.M., Bagozzi, R.P., Pearo, L.K. (2004). A social influence model of consumer participation in network- and small- group-based virtual communities. *International Journal of Research in Marketing* 21, 241–263

DiMicco JM, Millen D, Geyer W, Dugan C, Brownholtz B, Muller M (2008) Motivations.for social networking at work. *In Proceedings of CSCW 2008*, San Diego, CA, USA: 711-720

Dominic, S. (2011). What does it really mean to like something on Facebook? http://www.brandwatch.com/2011/10/what-does-it-really-mean-to-like-something-on-facebook/ [Accessed: 13/08/2013]

Dongsheng Yin; Kai Cui (2011) "A research into the latent danger of WLAN," *Computer Science & Education (ICCSE), 2011 6th International Conference on* , vol., no., pp.1085,1090, 3-5 Aug. 2011.

Dong L., Yu S., Xia T., Liao R. (2007), "WBIPS: A Lightweight WTLS-Based Intrusion Prevention Scheme", *In Proceedings of the International Conference on WirelessCommunications, Networking and Mobile Computing, IEEE Press.* pp. 2298-2301.

Doorley, J. and Garcia, H.F. (2011), *Reputation Management: The Key to Successful Public Relations and Corporate Communication*, CRC Press, Boca Raton, FL, pp. 113-33.

Dow, G. K. (1988). Configurational and coactivational views oforganizational structure. *Academy of Management Review*,13(1), 53–64.

Downs, J.S., Holbrook, M.B. and Cranor, L.F. (2007), "Behavioral response to phishing",Proceedings of the 2007 e-Crime Researchers Summit, ACM Press, New York, NY,pp. 37-44.

Duffy, T. M., & Jonassen, D. H. (1992). Constructivism: New implications for

instructionaltechnology. In T. M. Duffy & D. H. Jonassen (Eds.), *Constructivism and the technology of Instruction: A conversation*. New Jersey: Lawrence Erlbaum

Emery, R.E. and Trist, E.L. (1965) The causal texture of organizational environments", *Human Relations*, Vol. 18, , pp. 21-32.

Enid, M. (2006). The story of Socio-technical design: reflections on its successes, failures and   Potential. *Info Systems Journal, 26, 317 -342.*

Eisenstein, E.M. (2008), "Identity theft: an exploratory study with implications for marketers", Journal of Business Research, Vol. 61 No. 11, pp. 1160-72.

Eirik, A. & Jan, H. (2010). Improving Information Security awareness through dialogue: participation, and collective reflection: An innovation Study. *Computers & Security, Volume 29, Issue 4, June 2010, Pages 432-445, ISSN 0167-4048,*

Eloff, J.H.P., & Da Veiga A., (2009). A framework and assessment instrument for information security culture. Computer and Security, 29 (2010), 196-207.

Elodie, G. (2005). A Prime Target for Social engineering Malware: *McAfee Security Journal*; 2008. Fall.

Emm, D. (2006), "Phishing update, and how to avoid getting hooked", Network Security, Vol. 2006 No. 8, pp. 13-15.

Ernst, Young LLP. (2002). Global information security survey. UK: Presentation Services; 2002.

Evans, B. M.,Kairam, S.,&Pirolloi, P. (2010).Do your friends make you smarter?: An analysis of   social strategies in online information seeking. *Information Processing and Management*, *46*(6), 679–692.

Evans, T. (1994), Understanding Learners in Open and Distance Education, Kogan Page, London.

Everett C. J. (2006). Security awareness: switch to a better programme, *Network Security, Volume* 2006, Issue 2, February 2006, Pages 15-18, ISSN 1353-4858, http://dx.doi.org/10.1016/S1353-4858(06)70337-3.

Ferguson, A.J. (2005). Fostering e-mail security awareness: The West Point carronade. *Educause Quarterly* 28, 1 (2005).

Fergusen R. (2009). TrendLabs malware blog. Available from: <http://blog. trendmicro.com/new- variant-of-koobface-worm-spreading-onfacebook/>; [Accessed: 09/07/2013].

Finne T. Information systems risk management: key concepts and business processes. *Computers & Security* 2000;19(3): 234–42.

Florencio, D. and Herley, C. (2007), "A large-scale study of web password habits", Proceeding of the WWW 2007, Banff, Canada, ACM, New York, NY.

Freed, L., Ellison, C., Sarrel, M., Erlanger, L., & Kaven, O. (2013). What's Next. *PC Magazine,* 22,(16), 113.

Fredericksen, E., Picket, A., Shea, P., Pelz, W., & Swan, K. (2000). Student satisfaction and perceived learning with on-line courses: Principles and examples from the SUNYlearning network. *Journal of Asynchronous Learning Networks*, 4(2), 7–41.

Fu, A.Y. (2006), "Web identity security: advanced phishing attacks and counter measures",unpublished doctoral dissertation, City University of Hong Kong, Hong Kong.

Furnell, S.M. (2004b), "Getting caught in the phishing net", Network Security, No. 5, May,pp 14-18.

Furnell, S.M. (2007), "Phishing: can we spot the signs?", Computer Fraud & Security, No. 3,pp. 10-15.

Garretson C. (2007). Whaling: latest e-mail scam targets executives. Available from: <http://www.networkworld.com/news/2007/111407- whaling.html. [Accessed: 12/06/2013].

Gary, H., (2008). Social Engineering Techniques, Risks, and Controls. EDPACS *Journal, Vol. 37, Iss. 4-5, 2008*

Garner, R. (1995). The Growing Professional Menace: *Open Computing,* July, pp 33-42

Guanlin C., Hui Y., Zebing W. (2010), "An Intelligent WLAN Intrusion Prevention System Based on Signature Detection and Plan Recognition", *Second International Conference on Future Networks*.

Gaunt N. (2000). Practical approaches to creating a security culture. *International Journal of Medical Informatics* 2000;60(2):151–7.

Glazer, H. (2012). "Likes" are lovely, but do they lead to more logins?. *College & Research Libraries News, 73*(1), 18-21.

Gunter, O. (2013). The Phishing Guide: Understanding and preventing attacks. *IBM Internet Security Systems:* www-935.ibm.com/services/us/iss/pdf/phishing-guide-wp.pdf: [Accessed: 13/10/2013].

Gunter, O. (2013). Securing WLAN Technologies: Secure Configuration Advice on Wireless Network Setup. www.technicalinfo.net/papers/SecuringWLANTechnologi: [Accessed:11/10/2013].

Gilo, R., & Marius, M. (2009). Social Engineering: A serious underestimated Problem. *Computer and Society: Social Issues, Abuse and Crime involving computers.*

GMITS. GMITS: guidelines for the management of IT security, part 1: concepts and models for managing and planning IT security, ISO/IEC JTC1/SC27, PDTR 13335–1 (revision), version 28-11-2001. 2001.

Goodman S (2008). A Dirty Dozen: twelve p-value misconceptions. *Semin Hematol* 45(3):135–140.

Goring, S.P., Rabaiotti, J.R. and Jones, A.J. (2007), "Anti-keylogging measures for secure internet login: an example of the law of unintended consequences*", Computers & Security*, Vol. 26, pp. 421-6.

Gorling, S. (2007), "An overview of the sender policy framework (SPF) as an anti-phishing mechanism", *Internet Research*, Vol. 17 No. 2, pp. 169-79.

Gordon LA, Loeb MP, Lucyshyn W, Richardson R. (2004). CSI/FBI computer crime and security survey. Manhasset, NY: CMP Media; 2004.

Greene, Thomas C. (January 13, 2003). "Chapter One: Kevin Mitnick's story". The Register. Archived from the original on 2012-09-12

Gulati, R :The Threat of Social Engineering and Your Defence Against It. In SANS Institute Info Sec Reading Room 2003.

Hackman, R.J. and Oldham, G.R., (1980) W*ork Redesign*, Addison-Wesley, Reading, MA.

H˚agen H.,Yngve K., Ketil Ki., and Einar S. (2003). Measuring Resistance to Social Engineering.

Hahn, J., Todd, P., Van Der Klaauw, W. (2001). Identification and estimation of treatment effects with a regression discontinuity design. *Econometric*, 69, 201-209.

Hart, L. (2011), "Social media", in Doorley, J. and Garcia, H.F. (Eds), Reputation Management:

Hartman, R. L., & Johnson, J. D. (1990). Formal and informal grou communication structures: An examination of their relationship on role ambiguity. *Social Networks*, 12(2), 127–151.

Harvey, D.F. and Brown, R. (1992) *An Experiential Approach to Organization Development*, 4th ed., Prentice-Hall, Englewood Cliffs, NJ

Heather Fulford, Neil F. Doherty, (2003) "The application of information security

policies in large UK-based organizations: an exploratory investigation", Information Management & Computer Security, Vol. 11 Iss: 3, pp.106 – 114

Helen, J. L. (1996) "Managing information systems security: a soft approach," *Information Systems Conference of New Zealand, 1996. Proceedings* , vol., no., pp.10,20, 30-31 Oct 1996doi: 10.1109/ISCNZ.1996.554947

Henderson, C. R. (1901). The Scope of Social Technology. The American Journal of Sociology,6(4), 465-486

Hiltz, S. R., Coppola, N., Rotter, N., Turoff, M., & Benbunan-Fich, R. (2000). Measuring the importance of collaborative learning for the effectiveness of ALN: A multi-measure, multi-method approach. *Journal of Asynchronous Learning Networks*, 4(2), 103–125.

Hrastinski, S. (2009). A theory of online learning as online participation. *Computers &* Huber, M., et al. (2009). Towards Automating Social Engineering Using Social Networking Sites. In *Computational Science and Engineering, 2009. CSE '09. International Conference on*.

Hsu, C. L., & Lin, J. C. C. (2008). Acceptance of blog usage: The roles of technology acceptance, social influence and knowledge sharing motivation. *Information & Management*, 45, 65–74.

Ikujiro., N. (1994). A Dynamic Theory of Organizational Knowledge Creation, *Organization Science*, Vol. 5, No. 1. (Feb., 1994), pp. 14-37.

Ira S. W., Brian D. (1995) Information Security Technology?...Don't Rely on It A Case Study in Social Engineering. *Proceedings of the Fifth USENIX UNIX Security Symposium Salt Lake City, Utah, June 1995*

I. Nonaka, H. Takeuchi, The Knowledge-Creating Company, Oxford University Press, Oxford, United Kingdom, 1995.

Jack T, (2008), "Wireless Intrusion Prevention System", *Revista InformaticaEconomica*, vol. 47, March 2008

James C. (2012). Information systems user security: *A structured model of the knowing–doing gap, Computers in Human Behavior*, Volume 28, Issue 5, September 2012, Pages 1849-
Jagatic T., Johnson N., Jakobsson M., Menczer F. (2007). Social phishing. *Communications of the ACM* 2007;50:94–100.

Jakobsson, M. and Ratkiewicz, J. (2006), "Designing ethical phishing experiments: a study of (ROT13) rOnl query features", Proceedings of the 15th International Conference on World Wide Web, Edinburgh, Scotland, May 23-26.

Jefferey, M.S., Kathryn, R.S., Paul, M., Jefferey, J. (20050. Analyisi of end-user
    security behaviors . *Computer and Security*, 2005, 24.

Jeong-Jae W. et al (2009). Probabilistic Localization and Tracking ofMalicious Insiders
    Using Hyperbolic Position Bounding in Vehicular Networks.*EURASIP Journal
    onWireless Communications and Networking Volume 2009, Article.*

Johnson, R. B.(2009). Experimental Research. University of Alabama College of
    Education, Lecture Seires.
    http://www.southalabama.edu/coe/bset/johnson/lectures/lec9.htm [Ac-
    cessed:11/05/2012].

Jones A, Colwill C. (2008). Dealing with the malicious insider. *In: 9th Australian
    information and Warfare security Conference.*

John, A. (2003). Improving User Security behaviour. *Computers & Security Vol 22, No
    8.0167-*4048/0, Elsevier

John, H., Su, Z., Xinming, O., (2011): Effective Network Vulnerability assessment
    through DIMVA'11. *Proceedings of the 8th International Conference on Detection
    of Intrusion, Malware, and Vulnerability.*

John R., Gordon B., Dave C., David G., Natalie H., Adeel W. K., Justin K., Ian S.
    (2009). Social Networking and the Workplace. *The UK Large Scale Complex IT
    Systems Initiative*

Ka-Ping, Y. & Kragen, S. (2006). Passpet: Conveniet Password Management and Phishing
    Protection. ACM, Symposium On Usable Privacy and Security (SOUPS), Pitts-
    burg, PA, USA.

Kamay, V. & Adams, T. (1992). *The 1992 ACARB Profile of Computer Abuse in
    Australia* ACARB at RMIT, Melbourne

Kankanhalli A, Teo HK, Tan BCY, Wei KK. An integrative study of information
    systems security effectiveness. *International Journal of Information Management*
    2003;23:139–54.

Kelman, H.C. (1958). Compliance, identification, and internalization three processes of
    attitude change. *The Journal of Conflict Resolution* 2(1), 51–60

Kelley, D. (2003). The X factor: 802.1x may be just what you need to stop intruders
    from accessing your network. Information Security, 6(8), 60-69.

Kennedy, S. (2004). Best practices for wireless network security. *Information Systems
    Control Journal (*3).

Kenneth J. Knapp, R. Franklin Morris Jr., Thomas E. Marshall, Terry Anthony Byrd,

(2009). Information security policy: An organizational-level process model, *Computers & Security, Volume 28, Issue 7, October 2009, Pages 493-508, ISSN 0167-4048*,

Kent, M., Taylor, M., White, W. (2003). The relationship between web site design and organization responsiveness to stakeholders. *Public Relat. Rev.* Vol.29 No. 1,63–77.

Kling, R. (1987). Defining the boundaries of computing across complex organizations. In *Critical issues in information systems research*, edited by R. Boland and R. Hirschheim. London: John Wiley.

Kling, Rob, & Courtright, Christina. 2003. Group behaviour and learning in electronic forums: A sociotechnical approach. *Information Society*, Vol.19 No.3:221.

Kerry-Lynn, T., Rossouw, V.S., and Lynette, L. (2006). Cultivating an organizational information security culture. *Computer fraud and security*.

Knight, W. (2004), "Goin phishing", Infosecurity Today, Vol. 1 No. 4, pp. 36-8.

Knight, W. (2005), "Caught in the net", IEEE Review, Vol. 51 No. 7, pp. 26-30.

KPMG Corporate (1993). *Fraud Awareness Survey.* March, Sydney, Australia.

Kritzinger E., and Smith E.(2008). Information security management: An information security retrieval and awareness model for industry, Computers & Security, Volume 27, Issues 5–6, October 2008, Pages 224-231, ISSN 0167-4048.

Kritzinger E. & von Solms S.H.(2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computer & Security, 29, 846-847*

Kumaraguru, P. (2009), "PhishGuru: a system for educating users about semantic attacks",unpublished doctoral dissertation, Carnegie Mellon University, Pittsburgh, PA.

Kumaraguru, P., Sheng, S., Acuisti, A., Cranor, L.F. and Hong, J. (2010), "Teaching Johnny not to fall for phish", ACM Transactions on Internet Technology, Vol. 10 No. 2 (article 7).

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J. and Nunge, E. (2007a), "Protecting people from phishing: the design and evaluation of an embedded training email system", CHI'07: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 905-14.

Kumaraguru, P., Rhee, Y., Hasan, S., Acquisti, A., Cranor, L. and Hong, J. (2007b), "Getting users to pay attention to anti-phishing education: evaluation of retention and transfer", Proceedings of the APWG 2nd Annual eCrime Researchers Summit, Pittusburgh, PA, USA, pp. 70-81.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, A.B. and Pham, T. (2009),"School of phish: a real-world evaluation of anti-phishing training", Proceedings of the 5th Symposium on Usable Privacy and Security, Mountain View, CA, USA.

Kurt M. (2000) An Introduction to Social Engineering, *Information Systems Security*, 9:5, 1-7

Joon, S.P., & D.D. (2003). WLAN Security: Current and Future. *IEEE Computer Society*.

Kevin, B. & Peter, T.D., (2013). Understanding WEP Weaknesses. Hacking Wireless Networks for Dummies.

Kirsch, L. J.and Boss, S. R., (2007). "The Last Line of Defense: Motivating Employees to Follow Corporate Security Guideliness," in *Proceedings of the 28th International Conference on Information Systems*, Montreal, December 9-12.

Lambeth, J. (1996). Huge Increase in IT Crime. *Computer Weekly,* March 21, page 1

Lambeth, J. (1996). Time to Get Serious About Data Security. *Computer Weekly,* March 21, page 4.

Land, F. (2000). Evaluation in a socio-technical context. In *Organizational and Social Perspectives on Information Technology*, edited by R. Basskerville, J. Stage and J. DeGross. Boston: Kluwer Academic Publishers.

Land, F., and R. Hirschheim. (1983). Participative systems design: Rationale, tools and techniques. *Journal of Applied Systems Analysis* 10 (10):15-18.

Larson, A. (1992). Network dyads in entrepreneurial settings: A study of the governance of exchange relationships. *Administrative Science Quarterly*, 37, 76–104.

Lave, J. and Wenger, E. (1991), *Situated Learning: Legitimate Peripheral Participation*, Cambridge University Press, Cambridge.

Leary, M.R., Kowalski, R.M. (1995). *Social Anxiety*. Guilford Press, New York.

Leedy, P. & Ormrod, J. (2001). *Practical Research: Planning and design* (7th ed.). Upper Saddle River, NJ: Merrill Prentice Hall. Thousand Oaks: SAGE Pulbications.

Lewis, J.L. (2011), "Exploring the identity-theft prevention efforts of consumers in the United States", unpublished doctoral dissertation, Northcentral University, Prescott Valley, AZ.

Linda, Mc., Keith, W., & Denise, W. (2011). A *guide to Facebook Security, for yound, adults, parents and educators*. Your own space.

Maconachy, W.V., Schou, C.D., Ragsdale, D. and Welch, D. (2001), "A model for information assurance: an integrated approach", *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United State Military Academy, IEEE, West Point,*NY, pp. 306-10.

Mahi, D., (2009). Impact of the Human element on Information Security. *Social and Human Elements of Information Security, Premier Review, 2009.*

Mahi and Anup (2009). Impact of the human element of Information Security. *IGI Disseminator of Knowledge*

Manz, C. (1990) Beyond self-managing teams: towards self-leading teams in the workplace, in Pasmore, W. and Woodman, R. (Eds), *Research in Organizational Change and Development*, Vol. 4, JAI Press, Greenwich, CO, , pp. 273-99.

Marcus, J. (2008). Social Engineering 2.0: What's Netxt, Fall, *McAfee AvertLabs*, 2008.

Mardiana M. N., and Wan H. H. (2013). Wireless Networks: Developments, Threats and Countermeasures. *International Journal of Digital Information and Wireless Communications* (IJDIWC) 3(1): 119-134 *The Society of Digital Information and Wireless Communications.*

Mark C. (2011).A case study examining the implementation of social networking technologies to enhance student learning in a second language, Education, Business and Society: *Contemporary Middle Eastern Issues*, Vol. 4 Iss:1 pp. 80 – 90

Marek, S. "Identifying the Weakest Link." *Wireless Internet Magazine* www.wirelessinternetmag.com, [Accessed: 11/03/2012].

Martyn, S. (2009). Pretest-Posttest Designs. Retrieved June 09, 2013 from: Explorable.com http://explorable.com/pretest-posttest-designs

Martin, T.D. (2008), "Phishing for answers: exploring the factors that influence a participant's ability to correctly identify email", unpublished doctoral dissertation, Capella University, Minneapolis, MN.

Matthew, P. (2013). Spear Phsishing examples: how to stop phishing from compromising users *Technical Republic*.

McCumber, J. (1991), "Information systems security: a comprehensive model", *Proceedings of the 14th National Computer Security Conference, Baltimore, MD*

McDougall, P. (2004, March 25). Laptop theft puts GMAC customers'data at risk. Information Week Security Pipeline.

Mercuri, R.T. (2006), "Scoping identity theft", Communications of the ACM, Vol. 49 No. 5,pp. 17-21.

Marshall, A.M. and Tompsett, B.C. (2005), "Identity theft in an online world", Computer Law & Security Review, Vol. 21 No. 2, pp. 128-37.

Metzger, M. J. (2007). Making sense of credibility on the Web: Models for evaluating online information and recommendations for future research. *Journal of the American Society for Information Science and Technology*, 58, 2078-2091.

Michael W. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Systems Security Volume 16, Issue 6.*

Miles M.B, Huberman A.M. (1994). Qualitative data analysis: an expanded sourcebook. 2nd ed. Sage Publications

Min, W., Robert, C., Miller, G.L. (2006). Web Wallet: Preventing Phishing Attacks by Revealing User Intentions. *In Proceedings of the Symposium on Usable Privacy and Security (SOUPS),*

Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim (2008).Wireless Network Security: Vulnerabilities, Threats and Countermeasures. *International J ournal of Multimedia and Ubiquitous Engineering* Vol. 3, No. 3, July, 2008.

Mitnick, K., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. New York: John Wiley & Sons

Mohd Foozy, F., Ahmad, R., Abdollah, M. F., Yusof, R. and Mas'ud, M. Z. (2011) *Generic Taxonomy of Social Engineering Attack. In: Malaysian Technical Universities International Conference on Engineering & Technology* (MUiCET 2011), 13-15 November 2011, UTHM, Batu Pahat, Johor.

Mohammed, L.A.; Issac, B., "DoS attacks and defense mechanisms in wireless networks," *Mobile Technology, Applications and Systems, 2005 2nd International Conference on* , vol., no., pp.8 pp.,8, 15-17 Nov. 2005

Mosin H., Nilesh P. & Safvan V. (2010). Case study on Social engineering techniques for persuation. International journal *on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) Vol.2, No.2*.

Motorola (2010), The User Role in Information Security. www.motorola.com/services/government. [Accessed: 12/08/2012].

Mumford, E., and M. Weir. (1979). *Computer Systems in Work Design: the ETHICS Method*. New York: Wiley.

Murray B. (1991). Running corporate and national security awareness programs. In:

Proceedings of the IFIP TC11 seventh international conference on IS security 1991; p. 203–7.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study," *European Journal of Information Systems* (18), pp. 126-139.

Neumann, P. G. 1999. "Risks of Insiders," *Comunications of the ACM* (42:12), pp. 160.

Narain R. (2009). Rogue advertisement pushes scareware to NYTimes.com readers. Threat Post: KasperskyLab Security News Service; 2009.

Neil, Mc., M., and McCanny, J. (2004). "Reconfigurable Hardware Acceleration of WLAN Security," *IEEE Workshop on Signal Processing Systems (SiPS) Design & Implementation*

NCC, (1994). *IT Security Breaches Survey Summar.* National Computing Centre Limited, UK

Nicholas W., Vern P., Stuart S., and Robert C., (2003). A taxonomy of computer worms. In *Proceedings of the 2003 ACM workshop on Rapid Malcode*, pages 12–18. ACM Press, 2003. ISBN: 1- 58113-785-0 doi.acm.org/10.1145/948187.948190.

Nokia (2003). Man-in-the-middle attacks in tunneled authentication protocols.

Nohlberg, M. (2008), "Securing information assets: understanding, measuring and protecting against social engineering attacks", unpublished doctoral dissertation, Stockholm University, Stockholm

Nohria, N. (1992). Is a network perspective a useful way of studying organizations? In N. Nohria, & R. G. Eccles (Eds.), *Networks and organizations: Structure, form, and action* (pp. 1–22). Boston: Harvard Business School Press.

Noorderhaven, N. G. (1992). The problem of contract enforcement in economic. organization theory. *Organization Studies*, 13(2), 229–243

Nosworthy, J.D. (2000). Implementing Information security in the 21st Century – do you have the balancing factors? *Computers & Security* 19(4);337

Nyamsuren, E. and Ho-Jin C. (2007). Preventing Social Engineering in Ubiquitous Environment. in Future Generation *Communication and Networking (FGCN 2007)*.

Ong, T. H., Tan, C. P., Tan, Y. T., & Ting, C. (1999). SNMS – Shadow network management system, Symposium on Network Computing and Management, Singapore, May 21, 1-9.

Orlikowski, W. J. (2000). Using technology and constituting structures: A practice lens for studying technology in organizations. *Organization Science* 11 (4):404-428.

Painter, Christopher M.E. (March 2001). Supervised Release and Probation Restrictions in Hacker Cases"*United States Attorneys' USA Bulletin* (Executive Office for United States Attorneys).

Pahnila, S., Siponen, M., and Mahmood, A.(2007). "Employees' Behavior towards IS Security Policy Compliance," in *Proceedings of the 40th Hawaii International Conference on System Sciences,* Los Alamitos, CA: IEEE Computer Society Press, pp. 156-166.

Palvia, S.C., Sharma R.S. and Conrath, D.W. (2001). A socio-technical framework for quality assessment of computer information systems, *Industrial Management & Data Systems* 101(5) 237–251.

Parker, D.B. (1983), *Fighting Computer Crime*, Scribner, New York, NY.

Pasmore, W.; Francis, F,; Haldeman, J. and Shani, A. (1982). Sociotechnical Systems: A North American Reflection on Empirical Studies of the Seventies, *Human Relations*, 35(12) 1179-1204.

Patricia A.H.W. (2008). In a 'trusting' environment, everyone is responsible for information security. *Information Security Technical Report, 13, 2008, 207-215*

Peltier, T. R. (2001). Information security policies, procedures, and standards*: Guidelines for effective information security management.* Boca Raton, FL: Auerbach.

Penelopi A. (2012). Generating Social Awareness Through Social Network Sites. *Virtual Communities, Social Networks and Collaboration*, 181 Annals of Information Systems 15, DOI 10.1007/978-1-4614-3634-8_10,

Peter R. & Laddawan K. (2012). The Use of Facebook in an Introductory MIS Course: Social Constructivist Learning Environment. *Decision Sciences Journal of Innovative Education Volume 10 Number 2*

Peter G. (2013). Three Advantages of the Facebook Like Button You Should Know About.http://ezinearticles.com/?Three-Advantages-of-the-Facebook-Like-Button-You-Should-Know-About&id=4738806 [Accessed: 19/08/2013].

Polit, D.F., Beck, C.T. and Hungler, B.P. (2001), *Essentials of Nursing Research: Methods, Appraisal and Utilization*. 5th Ed., Philadelphia: Lippincott Williams & Wilkins.

Porterfield, A., Khare, P., & Vahl, A. (2011). "Chapter 3: Better Engagement with the

Help of Facebook Like Links and Buttons". *Facebook Marketing All-in-One for Dummies*. John Wiley and Sons. ISBN 0-470-94230-4.

Posthumus S, Von Solms R. A framework for the governance of information security. *Computers & Security* 2004;23(8): 638–46.

Power, K. (1994). Crooks Among Colleagues. *Informatics,* November, pp 22-26

Puhakainen P, A design theory for information security awareness. PhD thesis, University of Oulu; 2006.

Ractham, P.; Firpo, D. (2011). Using Social Networking Technology to Enhance Learning in Higher Education: A Case Study Using Facebook, *System Sciences (HICSS), 2011 44th Hawaii International Conference on* , vol., no., pp.1,10, 4-7 Jan. 2011

Ractham, P., Zhang, X. S.,&Firpo, D. (2010). Innovative web 2.0 implementation: Acase study of a web 2.0 technology proliferation within a university setting. *International Journal of Networking and Virtual Organisations (IJNVO)*, *7*(5), 479–496.

Radha, G. (2003). The Threat of Social Engineering and Your Defense against It. *SANS Institute 2003, As part of the Information Security Reading Room*.

Ravi, K.V. (2009). Towards a Theory of Socio-technical Interactions, lecture notes in Computer Science, Springer-Verlag Berlin Heidelberg, Vol. 5794, pp 694-699.

Robbins, S.P. (1994) *Essentials of Organizational Behavior*, 4th ed., Prentice-Hall Englewood Cliffs, NJ

Rocael H., Christian G., Hector R. A., (2012). Facebook for e-Moderation - A Latin-American Experience. Computer Uses in Education - *Collaborative Learning*.

Rogers, R. W. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," in *Social Psychology: A Source Book*, B. L. Cacioppo and L. L. Petty (eds.), London: Guildford Press, pp. 153-176.

Ronda R. H. (19990. Security service level agreements: Quantifiable security for the enterprise? In *Proceedings of the 1999 workshop on New security paradigms Caledon Hills, Ontario, Canada*, pages 54–60, 1999.ISBN: 1-58113-149-6 doi.acm.org/10.1145/335169.335194.

Ropohl,G. (1979). *Eine Systemtheorie der Technik: Zur Grundlegung der Allgemeinen Technologie*. Munich/Vienna: Hanser. 2nd ed., 1998

Roschelle, J. (1992). Learning by collaborating: Convergent conceptual change. *The Journal of the Learning Sciences* 2, 235–276

Rossouw von S. & Basie von Solms (2004). From Policies to Culture. *Computers &Security*

Rovai, A.P. (2000). Building and sustaining community in asynchronous learning networks. *TheInternet and Higher Education* 3, 285–297

Rubin D. A. (2001) Security considerations for remote electronic voting. In *29th Research Conference on Communication, Information and Internet Policy (TPRC2001)*, 2001.

RUsecure information security policies; 2002. Available from: http://www.information-security- policies.com/policies.htm . [Accessed 09 July 2013].

Rysavy, P. "Break Free With Wireless LANs." *Network Computing, Mobile and Wireless Technology Feature*, October 29, 2001.

Sangram, G., and Vetha, M., S., A., (2012). WLAN Security: Today and Tomorrow. Centre for Information and Network Security.

Sarel, D. and Marmorstein, H. (2006), "Addressing consumers concerns about online security: a conceptual and emperical analisys of banks actions", Journal of Financial Services Marketing, Vol. 11 No. 2, pp. 99-115.

Satidchoke P., & Mongkolchai W. (2011). Knowledge Management via Facebook: Building a Framework for Knowledge Management on a Social Network by Aligning Business, IT and Knowledge Management. *Proceedings of the World Congress on Engineering 2011 Vol III WCE 2011, July 6 - 8, 2011, London, U.K.*

Sheng, X. (2009), "A policy analysis of phishing countermeasures", unpublished doctoraldissertation, Carnegie Mellon University, Pittsburgh, PA.

Sherly A. & InduShobha C. (2010). An overview of social engineering malware: Trends,tactics, and implications, *Technology in Society, Volume 32, Issue 3*, August 2010, Pages 183-196, ISSN 0160-791X

Shi M., Shen, X. and Mark J. W. (2009) "IEEE802.11 roaming and authentication in wireless LAN/cellular mobile networks," *IEEEWireless Communications*, vol. 11, no. 4.

SCHNEIER, B. 2000. Semantic attacks: The third wave of network attacks. *Crypto-GramNewsletter*. http://www.schneier.com/crypto-gram-0010.html#1.

Schechter, S.E., Dhamija, R., Ozment, A. and Fischer, I. (2007), "The emperor's new security indicators", SP'07 Proceedings of the 2007 IEEE Symposium on Security and Privacy, pp. 51-65.

Schneier B. (2000). Secrets and Lies*: Digital Security in a Networked World*. John Wiley & Sons, 2000.

Sherif, J. S., Ayers, R., & Dearmond, T. G. (2003). Intrusion detection: The art and the practice, *Information Management and Computer Security*, 11(4): 175-186.

Shih, C. (2011), The Facebook Era: *Tapping Online Social Networks to Market, Sell and Innovate,* Pearson Higher Education, Boston, MA.

Shih, R.-C. (2011). Can Web 2.0 technology assist college students in learning English writing? Skeels M, Grudin J (2009) When social networks cross boundaries: A case study of workplace useof Facebook and LinkedIn. *In Proceedings of Group 2009, Sanibel Island,* FL, USA: 95-104.

Slavin, R.E. (1995). *Cooperative learning: Theory, research, and practice*. Allyn and Bacon,Needham Heights

Sorman, M.; Kovac, T.; Maurovic, D., "Implementing improved WLAN security," *Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium* , vol., no., pp.229,234, 18-18 June 2004

SpoofStick. 2004. http://www.spoofstick.com/. [Accessed: 18/07/2013].

Stamm, S.L. (2009), "Anticipating and hardening the web against socio-technical security attacks", unpublished doctoral dissertation, Indiana University, Bloomington, IN

Steinmüller, W. (1993) *Informationstechnologie und Gesellschaft: Einführung in dieAngewandte Informatik.*, Darmstadt: Wissenschaftliche Buchgesellschaft.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Newbury Park, CA: Sage Publications, Inc. http://www.tuc.org.uk/extras/facinguptofacebook.pdf. [Acessed: 12/07/2013].

Sandouka, H., A.J. Cullen, and I. Mann. *Social Engineering Detection Using Neural Networks*. in *CyberWorlds, 2009. CW '09. International Conference on*. 2009.

Selwyn, N.: Faceworking: exploring students' education-related use of Facebook. *Learning Media and Technology* 34, 157–174 (2009)

Selznick, P. (1948). Foundations of the theory of organization.*American Sociological Review*, 13(1), 25–35.

Schochet, P.Z. (2008). Statistical Power for regression discontinuity designs in educationalevaluations. Report submitted to Institute of Educational Sciences by Mathematica Policy Research, Inc., Princeton, NJ.: Mathematica Policy Research, Inc.

Schein, E.H. (1999). *The corporate culture survival guide.* San Francisco, California,

United States of America : Jossey-Bass Publishers.

Scott, W. R. (1998*). Organizations: Rational, natural, and opensystems* (4th ed.). Upper Saddle River: Prentice-Hall

Sharek D, Swofford C, Wogalter M. Failure to recognize fake Internet popup warning messages. *Human Factors and Ergonomics Society 52nd Annual Meeting*, New York; 2008.

Sherly A., & InduShobha C.(2010). An overview of social engineering malware: Trends, tactics, and implications, *Technology in Society*, Volume 32, Issue 3,

Shidhani A. Al and Leung V. (2009) Pre-authentication schemes for UMTS-WLAN

Shi-Ming P., Chen-Huei C., Hsiu-Li L. (2013). A study of Facebook members Knowledge Sharing. *Computers in Human behaviour,* 29 (2013)

Siponen, M.T. (2000). "A conceptual foundation for organizational Information Security Awareness," *Information Management & Computer Security*, Vol. 8. No. 1, pp. 31-41

Song S. et al (2009)."A secure and lightweight approach for routing optimization in mobile IPv6." *EURASIP Journal on Wireless Communications and Networking Volume 2009 (2009), Article ID 957690.*

Steven, F., & Kerry-Lynn, T. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud and Security, February, 2009*.

Steve, R. (2013). Social engineering and phishing attacks are getting smarter, but emplyees? *SNS, security the human*. www.cscoonline.com/article/739753. Accessed: 30/09/2013.

Steven, S. (2006). Social Engineering, the USB Way. http://www.darkreading.com/document.asp?doc_id=95556 [Accessed: 15/07/2012]
Sullivan, B. (2004). Consumers still falling for phish. MSNBC. http://www.msnbc.msn.com/id/5519990/: [Accessed: 13/07/2013].

Tavistock Institute (2011), The Socio-technology Design Approach. *Scandinavian Journal of Information System, Vol. 1* Terence Charlton , Marie Devlin & Sarah

Drummond (2009) Using Facebook to improve communication in undergraduate software development teams, *Computer Science Education*, 19:4, 273-292

Thach, L. and Woodman, R. (1994) Organizational change and information technology: managing on the edge of cyberspace", *Organizational Dynamics*, Vol. 23, summer 1994, pp. 30-46.

Thistlewaite, D.L., and Campbell, D.T. (1960). Regression-discontinuity analysis: An Alternative to the ex Post facto experiment. *Journal of Educational Psychology*, 51, 309-317.

Tim T. (2004). Social engineering: the "Dark Art". In *Proceedings of the 1st annual conference on Information security curriculum development* (InfoSecCD '04). ACM, New York, NY, USA, 133-135. DOI=10.1145/1059524.1059554 http://doi.acm.org/10.1145/1059524.1059554 [Accessed: 10/04/2012].

Thomas M. C., & Patrick J. W., Chapter 3 - Guarding Against Network Intrusions, In: John R. Vacca, Editor(s), Network and System Security (Second Edition), Syngress, Boston, 2014, Pages 57-82, Network and System Security (Second Edition), ISBN 97801241668   99,

Thomson, M.E.and Solms, R. (1998) "Information security awareness: educating your users effectively", *Information Management & Computer Security, Vol. 6 Iss: 4*, pp.167 – 173

Thomas, M. T. (2004). Wireless Security: Pearson *Education, Cisco Press, Indianapolis, Indiana.*

Tobias L., Veikko P., Davide B., & Engin K. (2012). Honeybot, Your Man in the Middle for Automated Social Engineering, *EURECOM Sophia-Antipolis, France.*

Trist, E. L. (1981). *The evolution of socio-technical systems: A conceptual framework and an action research program.* Ontario Quality of Working Life Center, Occasional Paper no. 2.

Trist, E. and Bamforth, K. (1951) Some Social and Psychological Consequences of the Longwall Method of Coal-Getting *Human Relations*, 4: 3-38.

Trochim, W.M.K (1984). Research Desigh for program Evaluation: The Regression – Discontinuity Design. Bererly Hills, CA: Sage Publications.

Turkle, S. (1984). *The second self: Computers and the human spirit*. New York: Simon & Schuster, 64–92.

TUC (2007) TUC briefing on online social networking and human resources. August 2007.
(Boundless Curates, 2013) – on the definition of the control group https://www.boundless.com/psychology/psychology-as-science/experimentation/explanation-of-random-assignment--38/ [Accessed: 13/01/2012].

Valentine J. A. (2006) Enhancing the employee security awareness model, Computer

Fraud & Security, Volume 2006, Issue 6, June 2006, Pages 17-19, ISSN 1361-3723,
http://dx.doi.org/10.1016/S1361-3723(06)70370-0.
(http://www.sciencedirect.com/science/article/pii/S1361372306703700) [Accessed:
07/06/2012].

Van de Ven, A., and Joyce, W. (1981) Overview of Perspectives on Organization
Design andBehavior. In *Perspectives on Organization Design and Behavior*, Van
de Ven and Joyce (Eds.), New York: John Wiley and Sons

Van Niekerk, J.F. Von Solms, R. (2009). Information security culture: A management
perspective, *Computers & Security, Volume 29*, Issue 4, June 2010, Pages 476-486,
ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2009.10.005.
(http://www.sciencedirect.com/science/article/pii/S0167404809001126) [Ac-
cessed:11/03/2012].

Vartak V., S. Ahmad, K N Gopinath (2007). "An Experimental Evaluation of Over-
The-Air (OTA) Wireless Intrusion Prevention Techniques", *In Proceedings of the
2nd International Conference on Communication Systems Software and Middle-
ware, IEEE Computer Society.*

Venkatesh, V., Davis, F.D. (2000) A theoretical extension of the technology acceptance
model: Four longitudinal field studies. *Management Science* 46(2), 186–204

Vernoy, M., & Kyle, D. (2002). *Behavioral statistics in action* (3rd ed.). Boston:
McGraw-Hill.

Verton D. (2002). Disaster recovery planning still lags. *Computer World*
2002;36(14):10.

Von Solms R, von Solms B. (2004). From policies to culture. *Computers and Security*
23(4):275e9.

Vroom C, von Solms R. (2004). Towards information security behavioural compliance.
Computers and Security 2004;23(3):191e8.

Vygotsky, L.S. (1978). *Mind in society: The development of higher psychological
processes*.Harvard University Press, Cambridge

Wang, M. J. (2009). Web based projects enhancing English language and generic skills
development for Asian hospitality industry students. *Australasian Journal of Edu-
cational Technology,* 25(5), 611-626.
http://www.ascilite.org.au/ajet/ajet25/wang.html [Acessed: 13/09/2013].
Watson, S., & Weaver, G. R. (2003). How internationalization affects corporate ethics:
Formal structures and informal management behavior. *Journal of International
Management*, 9(1), 75–93.

Webroot (2013). Phishing 2.0: Why phishing is back as the No. 1 Web threat, and how

web security can protect your company. www.webroot.com: [Accessed: 13/10/2013]

Wellman, B. and Haythornthwaite C.A. (2002). *The Internet in everyday life*: Wiley-Blackwell.

Wen-Chuan Hsieh, Chi-Chun Lo, Jing-Chi Lee, and Li-Tsung Huang (2004) 'The implementation of a proactive wireless intrusion detection system", *In Proceedings of the Fourth International Conference on Computer and Information Technology, IEEE Press, pp. 581- 586*

Wenger, E. (1998), *Communities of Practice: Learning, Meaning and Identity*, CambridgeUniversity Press, Cambridge.

Workman, M. (2008), "Theory-grounded investigation of phishing and pretext social engineering threats to information security", Journal of the American Society for Information Science and Technology, Vol. 59 No. 4, pp. 662-74.

Wright, R.T. and Marett, K. (2010), "The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived", Journal of Management Information Systems, Vol. 27 No. 1, pp. 273-303.

Wright, R.T., Chakraborty, S., Basoglu, A. and Marett, K. (2010), "Where did they go right?Understanding the deception in phishing communications", Group Decision and Negotiation, Vol. 19 No. 4, pp. 391-416.

Wu, M., Miller, R.C. and Little, G. (2006), "Web wallet: preventing phishing attacks by revealing user intentions", SOUPS'06: Proceedings of the Second Symposium on Usable Privacy and Security, Pittsburgh, PA, USA, pp. 102-13.

Wu, M., Miller, R.C. and Garfinkel, S.L. (2006), "Do security toolbars actually prevent phishing attacks?", CHI'06: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM Press, New York, NY, pp. 601-10.

Xin L and Qinyu L. (2007) Awareness Education as the Key to Ransomware Prevention, *Information Systems Security,* 16:4, 195-202, DOI: 10.1080/10658980701576412

Xun, D. (2009), Depending against Phishing attacks: PhD Dissertation, The University of Yourk.

Yacine R., & Adam M. (2008). Information security awareness in higher education: An exploratory study, *Computers & Security* 2 7 (2 0 0 8) 2 4 1 – 2 5 3

Yan Z., Dan H., & Yoonmo S. (2013). Facebook as a Platform for Health Information and Communication: A Case Study of a Diabetes Group. Springer *Science+Business Media New* York 2013

Yazan B., Ildar M., Konstantin B., Matei R. (2013). Design and analysis of a social botnet*Compuer and Network*, 57(2013) 566-578.

Yang X., Hui C., Shuhui Y.,Yi-bing L., Ding-zhu D.,(2009). Wireless Network Security. *EURASIP Journal on Wireless Communications and Networking*

Zhang, J, Reithel, B.J., and Li, H. (2009). Impact of Perceived technical protection on security behaviors. Information Management and Computer Security, 17(4), pp. 330-340.

Extract of some Figures from Chapter 2, for proper view.

Figure 2.12: MISSTEV Model
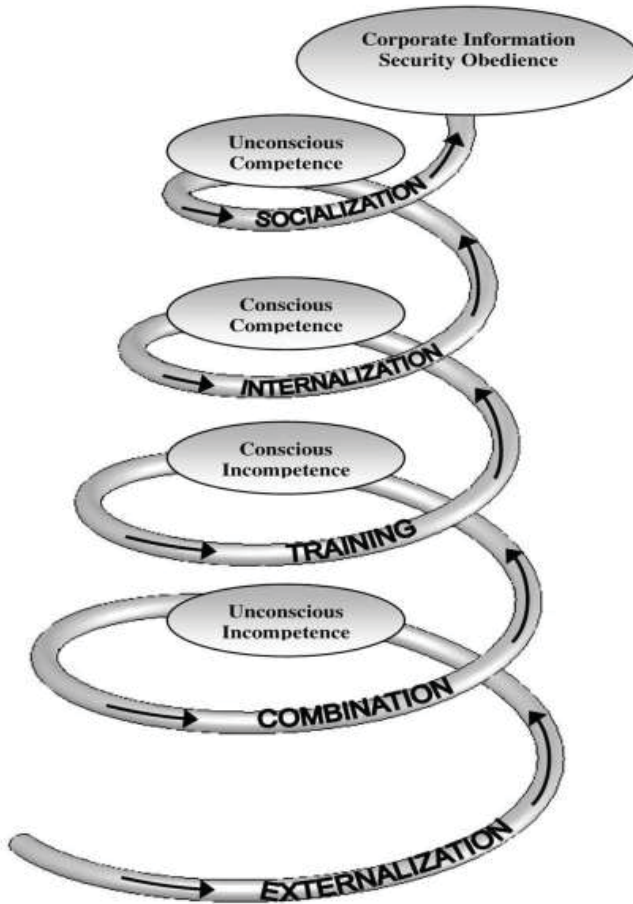
Source: Ikujiro, N. (1994) *Dynamic nature of organizational knowledge creation*

Figure 2.13:

The ISCF: Influencing information security behaviour and cultivating an information security culture.
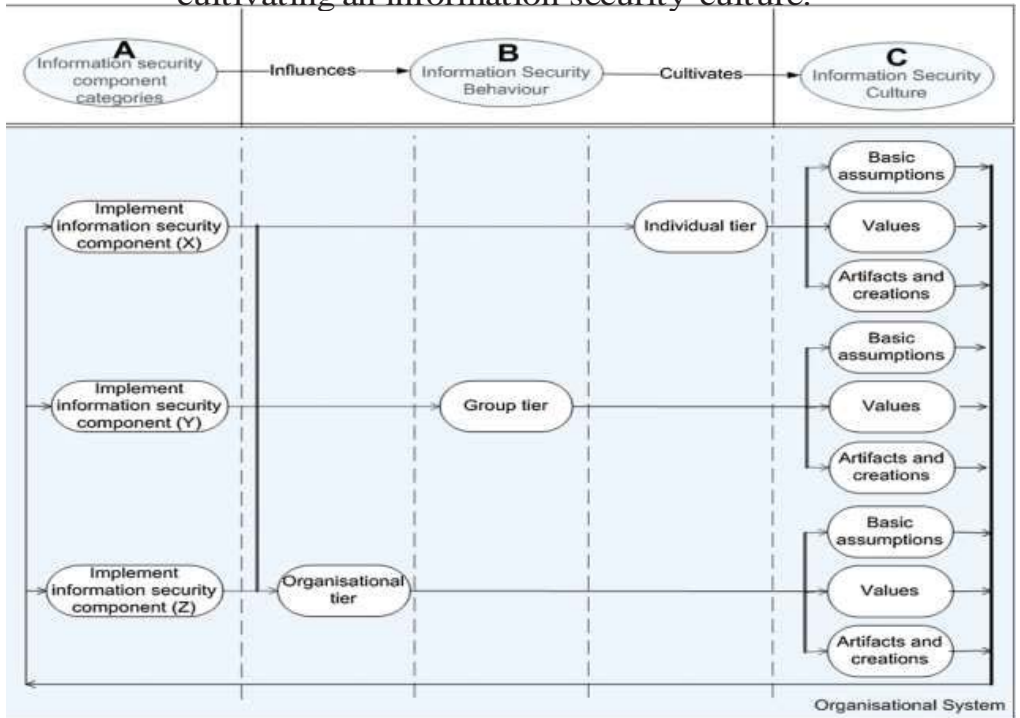
Source: *Eloff et al (2010). A framework and assessment instrument for information security culture*

Figure 2.16: **Managerial Information security Model**
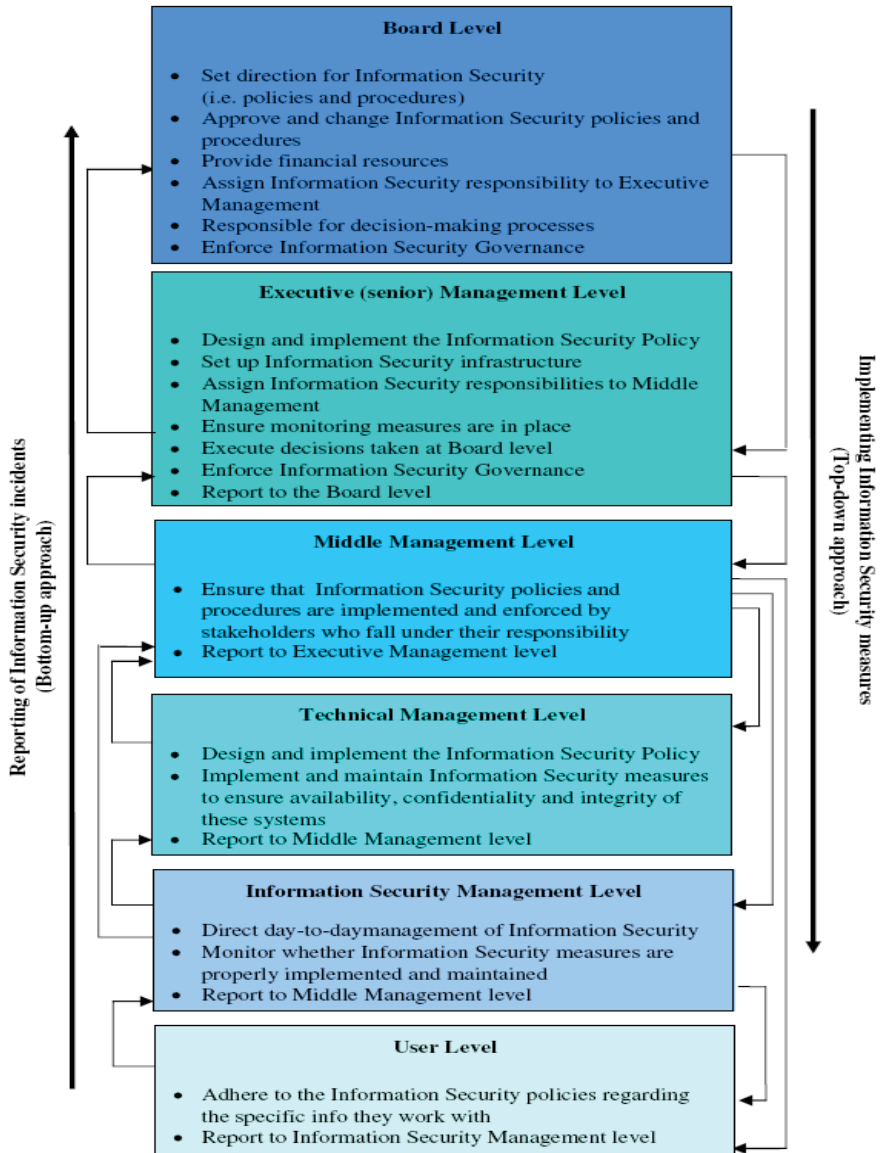
Source: Kritzinger et al (2006): Information Security Management

Figure 2.17: Tactical Information Governance Security Model

Source: Patricia (2008). Tactical information governance for security model (TIGS).
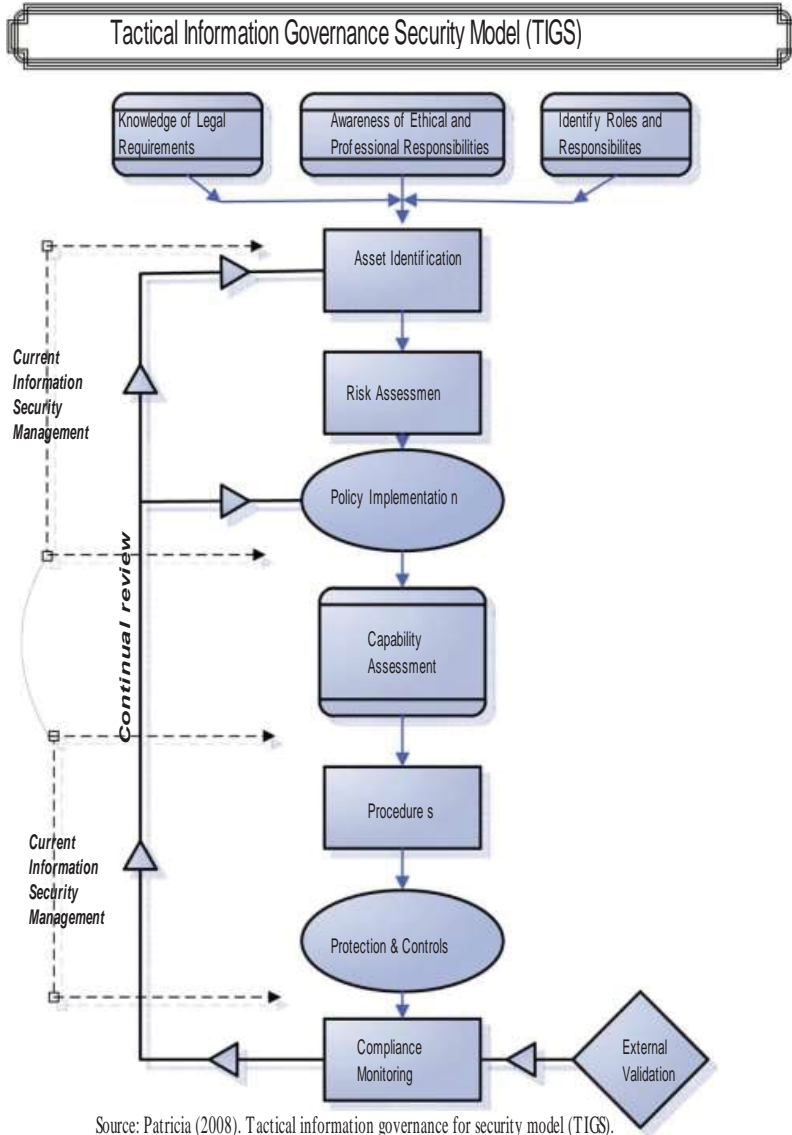
Figure 2.18: Information security process model
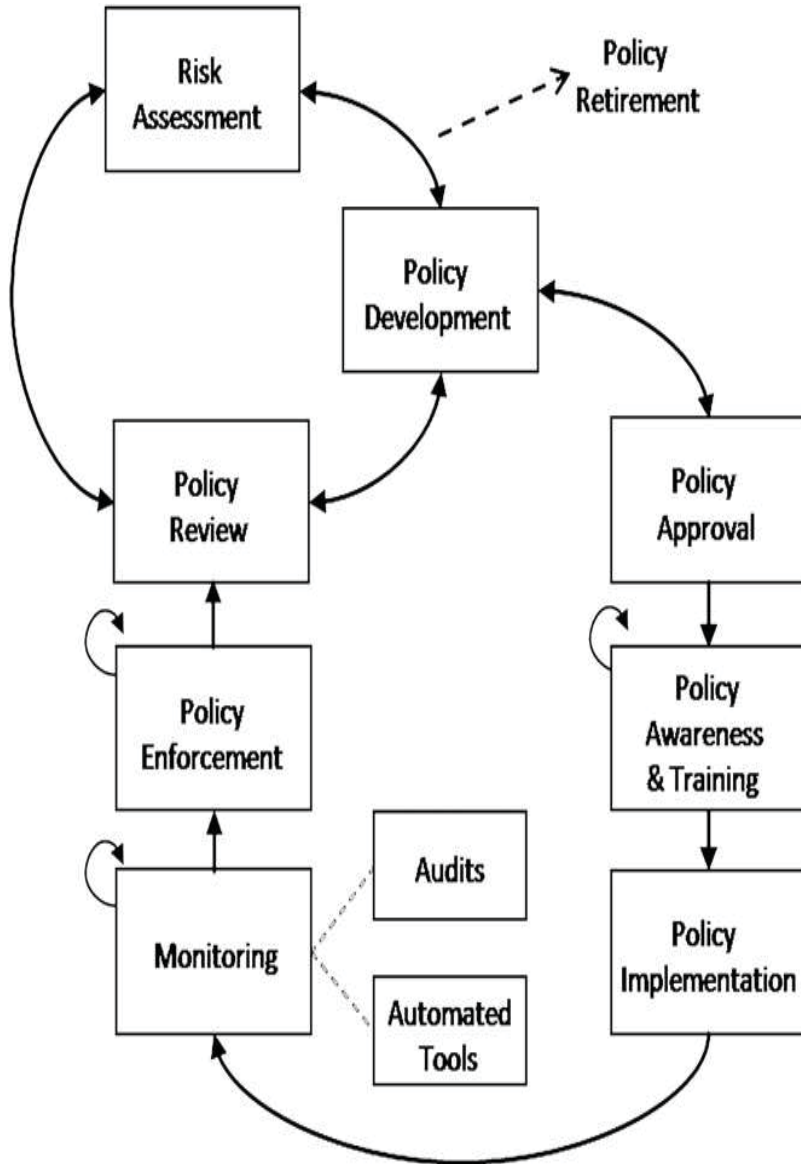
Figure 2.19: Content and processes of an information security workshop
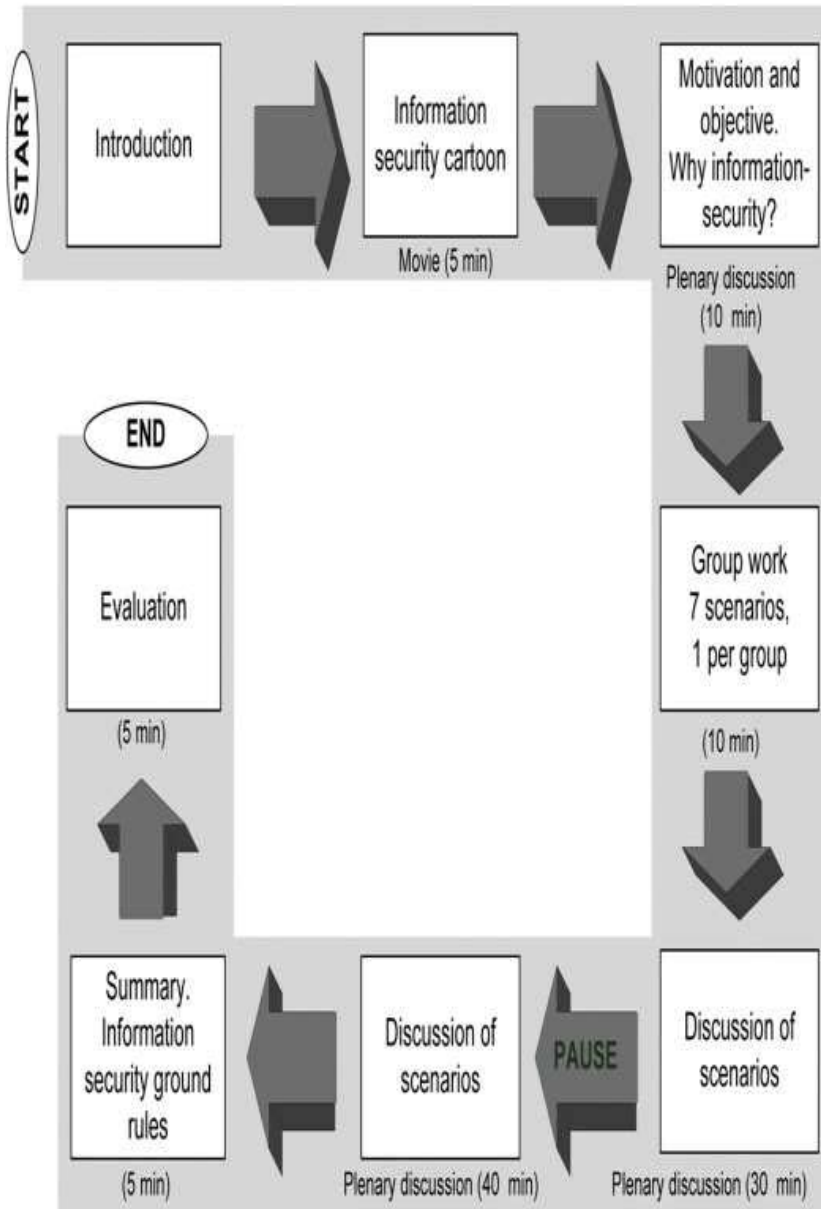
Source: Eirik, et al (2010): Improving Information Security awareness…

Figure 2.20: Comic Strip intervention: Teaching Johnny not falls for Phish.
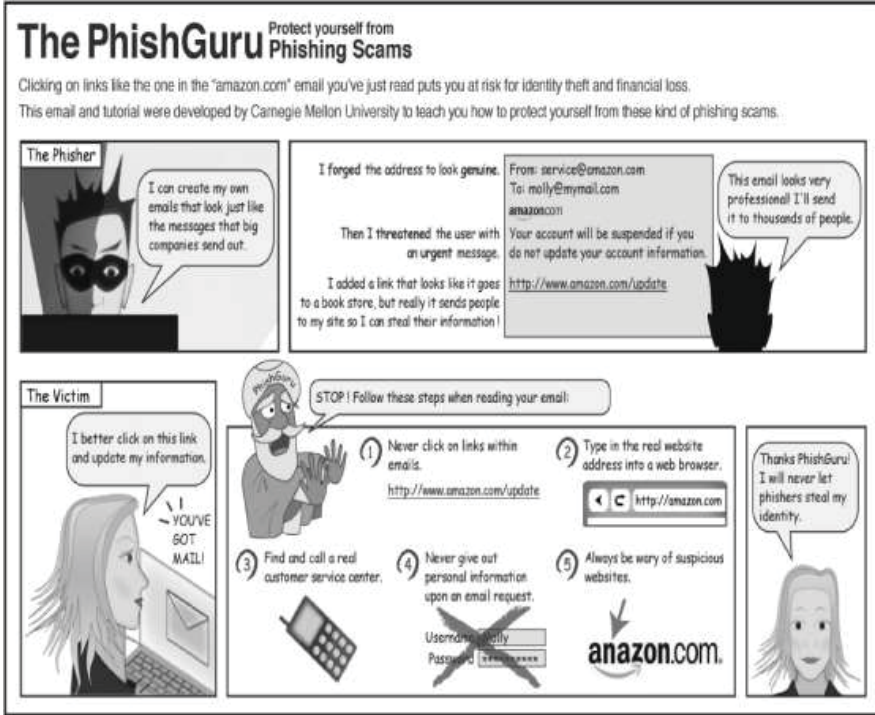
Figure 2.21: Social responsibility to combat malwa re
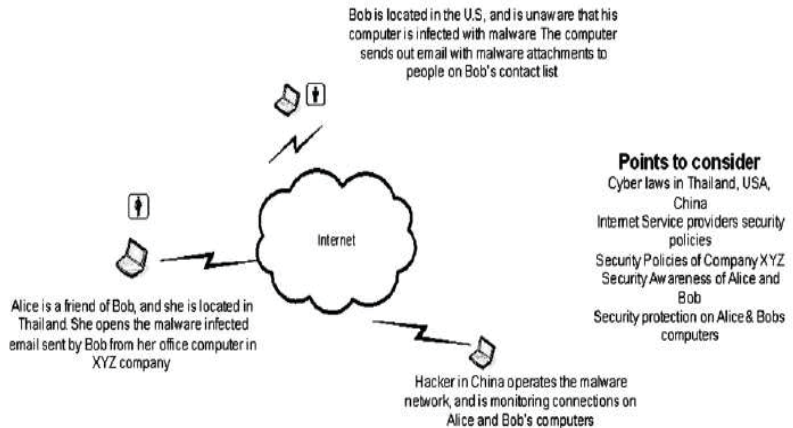
Appendix I

Source: Sherley et al (2006): Overview of Social engineering malware.

Appendix II
The Research Raw Data: Test scores

Below is the ***Raw Data*** collected from both the Experimental and Control groups of the research – performance scores of the subjects of the research. The participants attempted 50 questions of different actions and responses.

Experimental Group (Pre-test) **Control Group**

S/n	O1	02	03	04	05	06	07	S/n	O1	02	03	04	05	06	07
1	1	2	1	1	3	1	9	1	1	2	1	1	2	2	9
2	2	1	3	0	1	2	9	2	1	1	2	4	3	1	12
3	2	2	2	2	2	3	13	3	1	1	2	2	1	0	7
4	2	2	1	1	3	1	10	4	2	2	1	1	2	1	9
5	1	1	0	2	1	2	7	5	1	0	1	1	3	2	8
6	2	1	1	3	1	1	9	6	3	3	2	3	1	1	13
7	3	2	2	1	2	1	11	7	0	2	1	1	1	2	7
8	1	1	1	0	1	2	6	8	1	3	2	2	3	0	11
9	2	2	2	1	2	1	10	9	2	1	1	1	1	1	7
10	1	1	0	2	1	0	5	10	1	1	1	1	2	2	8
11	2	1	1	1	2	1	8	11	3	3	2	2	2	3	15
12	1	2	2	0	3	2	10	12	1	2	2	2	1	1	9
13	0	3	2	2	1	0	8	13	2	0	2	2	2	2	10
14	3	1	3	1	2	0	10	14	1	1	1	4	1	3	11
15	2	2	3	3	3	1	14	15	2	1	1	1	2	1	8
16	1	1	1	1	2	2	8	16	1	1	3	3	1	2	11
17	2	2	2	1	2	3	12	17	1	2	1	1	1	3	9
18	1	1	3	2	1	1	9	18	3	3	2	2	2	2	14

19	0	2	1	1	2	2	8	19	3	2	3	3	1	3	15
20	1	1	3	2	1	1	9	20	1	1	1	1	2	2	8
21	2	0	0	3	1	2	8	21	2	2	2	0	1	3	10
22	1	1	1	2	2	2	9	22	2	1	1	3	1	1	9
23	1	2	2	1	1	2	9	23	1	2	1	1	2	1	8
24	2	1	1	4	2	2	12	24	2	1	2	2	3	2	12
25	1	1	0	1	1	1	5	25	3	1	2	2	2	2	12
26	1	2	1	2	2	2	10	26	2	1	2	1	3	2	11
27	2	1	2	4	1	2	12	27	3	2	2	2	3	1	13
28	1	1	1	1	2	3	9	28	2	2	1	1	2	0	8
29	1	2	3	0	1	1	8	29	0	3	2	2	1	1	9
30	2	2	2	2	2	1	11	30	1	1	1	1	1	2	7
31	1	1	1	1	0	0	4	31	0	2	1	1	1	1	6
32	3	2	1	2	1	2	11	32	1	0	2	2	2	2	9
33	1	1	2	2	0	3	9	33	3	2	1	1	1	3	11
34	1	3	1	1	2	2	12	34	3	1	3	0	1	1	9
35	2	1	3	0	1	1	6	35	1	2	1	1	1	2	8
36	2	1	2	2	2	1	10	36	0	0	2	2	1	3	8
37	1	2	1	3	1	2	10	37	1	1	1	1	1	1	6
38	2	1	2	1	0	1	7	38	2	2	2	1	2	2	11
39	1	2	1	1	1	1	7	39	1	1	2	2	1	1	8
40	3	1	2	2	2	2	12	40	2	2	2	1	2	1	10

Raw Data: Test scores

Experimental Group   **(Post-test)**   **Control Group**

S/n	O1	02	03	04	05	06	07	S/n	O1	02	03	04	05	06	07
1	7	8	6	6	5	8	40	1	2	2	2	1	2	2	11
2	8	5	7	4	4	5	33	2	1	1	1	2	1	1	7
3	5	7	5	7	5	7	36	3	1	1	1	2	1	1	7
4	5	6	6	8	4	6	35	4	2	0	1	2	2	2	9
5	6	7	4	4	5	7	33	5	2	1	2	1	0	2	8
6	8	5	7	6	6	5	37	6	1	3	2	2	2	0	10
7	5	7	6	7	4	7	36	7	0	1	2	2	2	2	9
8	7	6	5	8	5	6	37	8	2	0	2	1	1	3	9
9	5	8	8	6	4	8	39	9	1	0	3	1	3	2	10
10	7	6	6	4	3	6	32	10	2	1	2	1	1	1	8
11	6	4	5	6	5	4	30	11	1	2	3	2	2	1	11
12	6	8	7	7	6	8	42	12	1	0	3	2	2	3	11
13	6	6	8	5	4	6	35	13	2	1	1	2	1	2	9
14	7	6	4	8	5	6	36	14	1	2	2	2	2	1	10
15	5	5	7	6	4	5	32	15	2	1	0	2	2	3	10
16	7	7	5	7	6	7	39	16	2	2	2	2	3	2	13
17	6	5	7	8	5	5	36	17	1	1	1	1	1	1	6
18	8	8	5	5	4	8	38	18	1	1	2	3	3	2	12
19	5	6	5	7	3	6	32	19	2	2	1	2	1	1	9
20	6	4	6	5	5	4	30	20	3	1	2	1	2	1	10
21	5	8	7	4	6	8	38	21	2	1	1	1	3	2	10

22	6	6	5	7	5	6	35	22	1	0	2	2	2	2	9
23	5	7	4	5	6	7	34	23	2	3	2	1	2	1	11
24	5	5	7	7	4	5	33	24	1	2	3	3	1	3	13
25	7	7	6	5	3	7	35	25	1	3	1	1	2	2	10
26	6	8	5	6	3	8	36	26	2	1	2	2	1	1	9
27	7	6	7	6	5	6	37	27	2	1	1	2	2	3	11
28	8	5	4	8	6	5	36	28	1	2	2	1	3	0	9
29	6	8	6	4	3	8	35	29	2	1	0	2	2	3	10
30	7	6	5	7	6	6	37	30	1	2	2	1	1	2	9
31	5	7	7	6	5	7	37	31	2	1	2	2	1	2	10
32	6	5	6	7	5	5	34	32	1	3	2	3	2	1	12
33	7	6	5	5	5	6	34	33	2	1	2	1	3	1	10
34	6	7	6	6	3	7	35	34	1	2	3	1	2	2	11
35	5	5	7	5	4	5	31	35	1	1	2	2	1	1	8
36	6	6	5	6	3	6	32	36	2	2	0	3	2	2	11
37	8	5	6	6	5	5	35	37	1	1	3	1	1	1	8
38	6	6	4	4	3	6	29	38	1	2	1	2	1	1	8
39	7	5	7	6	4	5	34	39	3	1	1	1	2	2	10
40	6	7	6	5	4	7	35	40	1	2	2	2	1	2	10

SUMMARY OF THE STATISTICS, AS USED IN EXCELL

1. **How the Data was computed.** Using Excel in the following procedure, the raw data was computed to test the Null Hypothesis.

Sum =

N   =   10, number of observations, participants

A   =   which is sum of the differences

B   =   which is number of observations times the differences squared

C   =   which is squaring the differences with sum of the differences

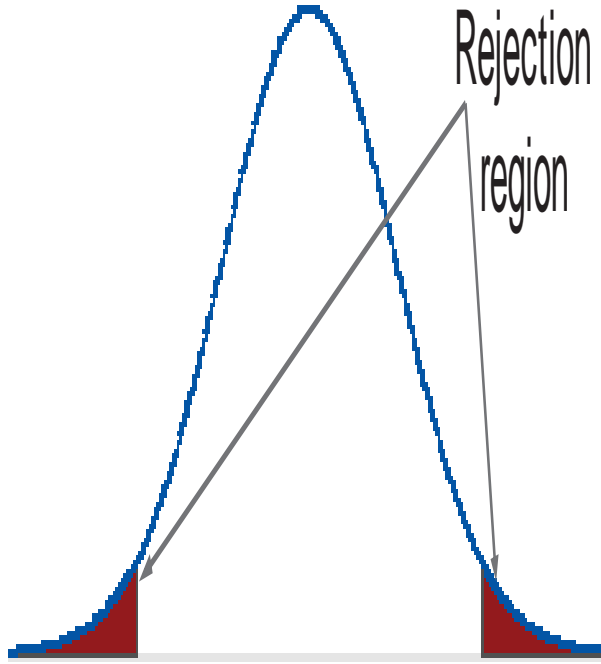D   =   which number of participants minus one

E   = which is B – C divided by D (B-C)/D

F   = which is Square root of E

t test = which is A divided by

2. **HOW THE RESULT WAS INTERPRETED**

- **Degree of Freedom n-1 (40 – 1)**
- **t value needed for rejection of null hypothesis 0.05 (95%) Confidence**

Rejection region

Pre-test Questionnaire for Experimental and Control Groups

January, 2014. **The underlined are the expected response** – *this appeared in appendix only*

Instructions: *Please attempt all the Questions. Tick your chosen response for questions with options. State the key words for questions requiring written answers.*

Hint: in the attempt to provide the correct answer, you are recommended to recall some instances within your environment, during or prior to the test; and also consider your online experiences and encounters both on websites and on social media.

Q1   My role as a worker is distinct from IT related issues

   a)   True   b) <u>False</u>

Q2   I respond to requests of visitors in my organization as far printing of documents or any online assistance either with their media devices or login through my device.

   a)   Yes   b) <u>No</u>

Q3   Whether your answer to Q2 is a or b, do you suspect any threat to such request?

   a)   Yes   b) <u>No</u>

Q4   A visitor to my organization with the news that our network is going for an upgrade for better performance, I jubilate with such news.

   a)   <u>Yes</u>   b) No

Q5   irrespective of your answer to Q4 is either Yes or No, do you feel like cooperating with the person for any assistance?

   a)   <u>Yes</u>   b) No

Q6   I am curious for any removable device I saw within my work place environment and make attempt to explore it on my system.

   a)   <u>Yes</u>   b) No

Q7   The posters and pamphlets I used to see around my work place environment calling me to visit some websites for some interesting things provoke my interest and I have the intention of visiting them.

   a)   <u>Yes</u>   b) No

Q8   As good employee, I can share my login details with official visitor to my work-place.

  a) <u>Yes</u>   b) No

Q9   I consider some mails in my scam box as genuine and I used to enable them as not scam mails.

  a) <u>Yes</u>   b) No

Q10   Before deleting any mail as in my junk file, I have to open it, view it and exhaust my curiosity of its contents

  a) <u>Yes</u>   b) No

Q11   A link sent to me in my email is important and failure to click and follow it may cause me to lose something important.

  a) <u>Yes</u>   b) No

Q12   reporting suspicious events encountered online or within my work place environment is not my concern and I keep off from doing that.

  a) <u>Yes</u>   b) No

Q13   I can detect a bogus email through its

  a. Contents
  b. <u>Link</u>
  c. Message
  d. None of the above

Q14   Through web browser, I can identify some anomalies.

  a) True   b) <u>False</u>

Q15   The URL indicates nothing as per as security is concerned

  a) <u>True</u>   b) False.

Q16   Pop-ups windows indicate warning of safety

  a) <u>True</u>   b) False

Q17   Blocking an email address or reporting it as spam is not a way of getting rid of such mail.

  a) True   b) <u>False</u>

Q18   Downloading Free version software is one of the ways to test the efficiency of the software.

   a) <u>True</u>   b) False

Q19   Suggestive game websites are helpful and I do not ignore them or one day I shall visit them.

   a) <u>Yes</u>   b) No

Q20   Video and Music download websites are helpful to refreshing my day's activities in my working place and as such interested in downloading them for my refreshments.

   a) <u>True</u>   b) False

Q21   The IT department or my superiors need to know about my online experiences.

   a) True   b) <u>False</u>

Q22   I consider sharing my online experience with my formal colleagues as waste of time.

   a) <u>True</u>   b) False

Q23   Disclosure of my online experiences with my formal colleagues is best done at an opportunity.

   a) <u>True</u>   b) False

Q24   My formal colleagues in my workplace receive the news of my online experiences immediately.

   a) True   b) <u>False</u>

Q25   My close friends and associate in my work place receive the news of my online experiences immediately.

   a) <u>True</u>   b) False.

Q26   Confiding with colleagues formally for any encounters within the environment of my work place may amount to infringement of others rights.

   a) <u>True</u>   b) False

Q27   Sharing some encounters in my workplace environment with my friends and close associates is a collaborative effort.

   a) <u>True</u>   b) False

Q28   Reporting my online experiences to the formal authority is the best way to counter-act viruses and malicious programs in my workplace.

  a) True   b) <u>False</u>

Q29   My close friends and associates are more resourceful in mitigating any form of online encounters of malicious programs and viruses in my workplace.

  a) <u>True</u>   b) False

Q30   State how you will take action against a virus or malicious program you encounter during your work day session…………………………………………………………………………..

<u>Reporting both to my formal authority and my close associates. (the answer should contained both two entities; or any experession that contain the two entities – formal authority and close associates).</u>

Q31   Social media of Facebook is appropriate only for friendship interactions

  a) <u>True</u>   b) False

Q32   The saying that online deception exist is

  a) True   b) <u>Not True</u>

Q33   There is Cyber bullying over the Facebook

  a) True   b) <u>Not True</u>

Q34   Privacy settings on Facebook do not contribute to network or information security.

  a) <u>True</u>   b) Not True

Q35   How do you check message in your Facebook ……..

        (<u>Direct from the Facebook profile).</u>

Q36   Adding Facebook applications add to enjoyment of Facebook functionalities.

  a) <u>True</u>   b) Not True

Q37   I frequently log into the Facebook than my email account or visiting some websites.

  a) <u>True</u>   b) Not True

Q38   State the most common Functionalities of Face-book…………………………………

Comment, Post, Like, Sharing, Tag (at least 4 of them)

Q39   Repeat the functions you stated in Q38 and against each function State its role in your Facebook interactions.

  Comment – say feelings, say opinion, thoughts, or initiate discussions (or any similar expression)
  Like – care about, reciprocity, association self,
  Share – disseminate Information, enlighten, or provoke action (or any similar expression).
  Post – information, announcement, enlightenment, provoke discussions.
  Tag – link, photo link (or any similar expression).

Q40   The term social engineering, mean to me:
  a) All kinds of civil and societal activities
  b) Means of deception

Q41   A stranger malingering over our workplace environment, should be
  a) Assisted
  b) Reported
  c) Questioned
  d) Monitored

Q42   Always escort visitors, do not make them wonder around and ask them to wait at a lobby and escort them back to the when the business is completed.
  a) Necessary   b) Not Necessary

Q43   When constructing your password, you should use easy to remember letters and always use the same password for different login profiles.
  a) True   b) False

Q44   Sending confidential information across the internet can be done through encryption or sent in a password protected zip file.
  a) Necessary   b) Not necessary

Q45   Internet is resourceful and informative; the free-of-things on the internet offered by individuals and groups should be accepted for knowledge dissemination.
  a) True   b) False

Q46   Disabling Firewall and browser settings, improves browsing experience
  a) True   b) False

Q47   If I encounter a security incident on my network or information resources, I
  a) Spread the message
  b) Contact the IT
  c) Tell a co-worker
  d) Tell a friend

e) Not my concern

Q48   Truly tick any or some of the terms below that you know their meanings and their implications to security.

a) Baiting
b) Click Jacking
c) Pharming
d) Elicitation
e) Cross-site Scripting
f) Phishing
g) Spoofing
h) Doxing
i) None of the above

Appendix IV

April 2014

POST TEST: **Experimental & the Control Groups**

SNS-based Model Test for Social Engineering based IP in Wireless LAN

Group:………………… No:…………………………………….

Instructions: Attempt all the questions. In answering the questions,

1. **Your system must be kept ON and connected to the internet.**
2. **You must be checking your email**
3. **You must be visiting the websites you were directed to**
4. **You must be online on the Facebook**

Check your email, and answer questions 1-20 using the messages and the websites you are directed to visit.

1. How do you react to the software you were asked to download for free trial?
   a) Download it
   b) Install it on the spot
   c) Send it to the social network
   d) <u>Ignore it</u>

2. How do you react to the email you received?
   a) Read it contents and abandoned it.
   b) Understand the subject matter and acted accordingly.
   c) <u>I have shared it for awareness</u>
   d) I deleted it.

3. The web links I received in my email or encountered while browsing, I
   a) Click it to get to know its contents
   b) Follow it to discover if it is real
   c) Ignore it
   d) <u>Throw it to social network</u>

4. The attachments I received in my mails, I
   a) Open it to read its contents
   b) Delete it immediately after reading it
   c) <u>Just send its link to the social network</u>
   d) a and b

5. The spasm or Junk mails I received in my emails, I
   a) Delete them periodically
   b) <u>Sent their links to social network</u>
   c) Report them as spam
   d) I do nothing

6. The alert flashing on my screen to scan my system for an infection, I handled it in the following way
   a) I immediately click to scan so as to be free from the infection
   b) <u>Share the link with my colleagues and friends</u>
   c) I ignore to scan
   d) Close the website

7. The mail I received congratulating me for a benefit, I consider it as
   a) Virus
   b) <u>Phishing</u>
   c) Malware
   d) Botnet   e) I don't know.

8. I distinguished the genuine and phishing URL by:
   a) <u>Letter/alphabet variations</u>
   b) Image appearance
   c) www followed by domain name
   d) presence of .com, .ng, .org

9. Describe what aids you to distinguish a bogus website often appear with
   a) <u>Anchor mismatch</u>
   b) Presence of external link
   c) Dynamic mismatch
   d) URL beginning with number
   e) None of the above

10. An IP in the URL indicates
    a) A genuine website
    b) Fake website
    c) <u>A suspicious site</u>
    d) Specific website

e) Connectivity is established

11. The Dot (.) in website indicates
    a) Genuinely of the website
    b) <u>Suspicious on the number of dots</u>
    c) Genuine URL do not have more than 5 dots
    d) Genuine URL don not have more than 3 dots
    e) None of the above

12. A phisher sends and email containing a phishing………. And if the receiver ………..the……….…………..is sent to the browser.

    <u>Link, click,</u>

13. Check your system, particularly attempt to open any website or click on any item, and then respond to the option below that you deem appropriate to you.

    a) I notice no anomalies
    b) I notice……<u>pop-up</u>…………as anomalies

14. Should your answer in Q6 is (a), then what indicators have you used to notice the absence of the anomalies. And should your answer in Q6 is (b), then precisely mention measures you can take to offset such anomalies.

    a. <u>is normal, window message</u>; (b) <u>ignore and share the experience</u>

15. With regard to email No. 15, to avoid being the victim of the…<u>phishing</u>……attacks, I avoid…<u>opening the attachment</u>

16. In response to the site asking me to sign up, I

    a) Signed up because the signing up is beneficial
    b) Avoid singing up, because?………<u>falling victim of social engineering</u>

17. While viewing the video I am directed on the YouTube, I notice
    a) <u>An Adware</u>
    b) Closing-Window
    c) Normal view
    d) Pop-up windows
    e) …………………….

18. The mails I received for winning prizes and other incentives,
    a) I kept them to myself
    b) I informed friends
    c) <u>I shared the Information</u>

d) I just deleted the mail
e) Respond to the senders

19. The unusual behaviour on my system and the Network,
    a) I decided to report to the IT personnel
    b) I attempted to diagnose and correct the problem
    c) I decided to share the experience on the network
    d) I complied with the displayed on my system
    e) I noticed no unusual system or network behaviour

20. I consider object that causes harm on my computer and our network, as
    a) Vulnerability
    b) Threat
    c) Attacks
    d) b and c
    e) Virus

21 **Use your Facebook page to answer questions 21-30.**

On your Facebook page spend some time exploring your profile, your friends and friends of your friends, and disclose your tour as (a) or (b) below:

a) I found no program attracting or requesting my intervention.
a) I found some programs appealing to me for my intervention (specify)
   A video to view, a site to view, a promotion to sign up,

22. Through …… I was able to understand more about online…..
    a) Education, tricks
    b) Group post, social engineering
    c) Seminar, attacks
    d) Newsletters, security measures
    e) Facebook, Social Media

23. I understand through ……….. I can receive reminders and useful information, vigilance to see, detect, and react to harmful objects on our WLAN.
    a) Newsletters
    b) Information handbook
    c) Security policy
    d) Social networking

24. The Facebook Platform tower has exposed me to:
    a) Malware, IP, and social networking
    b) Spyware, learning, and communication

327

c) Malware, Feedback, one-to-many
d) Phishing, forum, one-to-many
e) None of the above.

25. Through … the … I can able to recognize, detect, and prevent intrusion on our
WLAN through:
a) Feedback and comments
b) SE tricks and social networking
c) Posting and discussions
d) Alert and notifications
e) Phishing and virus

26. Through the … platform, I realize I can contribute to current issues.
a) Web
b) Emails
b) Training interaction
c) Social networking
d) Forums

27. If at all I am sharing my online experiences, I
a) Share it with my work group and friends
b) Share it with my work group
c) Share it with my fiends only
d) Share it publically

28. Consider your Facebook profile as initiative introduced by your workplace to make
you collaborate to protect your network and information security, which of the Fa-
cebook functionalities aid your contribution to the initiative:

Post, Comment, Like, Share, Tagging, Notification

29. wha impact does the initiatives of your workplace as in Q28 could have on you as a
user of the network and information resources?
Transparency, Accountability, Responsibility, and Participation.

30. Consider yourself in the Facebook platform introduced by your workplace, how do
you describe your role in the social network?
As a node, a Pc with Firewall, Intrusion prevention systems, as monitoring soft-
ware, and as anti-virus.
31. Describe (IF any), an incidence you noticed with your social networking

In the exam hall ………<u>ID theft</u>, <u>request from unknown friend</u>, <u>game suggestion</u>, and install <u>an application</u>

32. In the exam session, have you noticed any planted item within you?
 a) If yes, what does it implies: <u>removable media</u>, <u>needs my action to view</u>, <u>road apple</u> (only one answer surprises).

33. Should your workplace Facebook platform for security considers you as a firewall to the WLAN, briefly state what does that mean.
   <u>Prevention of threats and attacks</u>, <u>being proactive to security</u>, <u>stop anything   suspicious from accessing</u> or <u>getting into the network and the information system</u>.

34. You might have noticed some strangers in the exam hall; if so, briefly sate your observations regarding them.
   <u>Friendly</u>, <u>professional engagement</u>, <u>personal engagement</u>, <u>request for help</u>, <u>instructing to visit a website</u>, <u>fill online form</u>. *Any of the term or similar in meaning.*

   Answer questions 35-50 by:
   - Studying the websites you were directed to
   - Opening your email attachments from abdullah@es.aau.dk
   - Reading the suggested sites and pages on your Facebook

35. Using Google chrome browser, state your reaction visiting the following website:http://www.gameofwartune.com/motive1?entrypt=wt-aff_m1---@90--m1-56883-adv-ron

                           <u>asking me to sign up</u>

36. Using Google chrome browser, interpret your attempt to click on the *business information* link. http://www.lifewave.com/english-int/

                           <u>underlined links asking me to click "here"</u>

37. Using IE, visit the two below and describe your experience.
   (http://www.gameofwartune.com/motive1?entrypt=wt-aff_m1---@90--m1-56883-adv-ron, and http://www.lifewave.com/english-int/

   Attempt to deceive in rebooting my system, visiting a website, a form of social engineering attempt.

38. In the website below, interpret the message that appears:
   http://videnskab.dk/krop-sundhed/kalk-og-d-vitamin-gor-dig-til-en-overlever
      <u>you could win an   iPad, complete the survey, start here, and Click here.</u>

Collecting personal information, form of social engineering, deception,

39. Visit the following website and make a comment on the messages
http://www.hotnigerianjobs.com/hotjobs

Collect personal information, create log in details, attempt to cause malicious programs after clicking submit.

40. Study the following website address and attempt to visit the website, describe your experience.
http://www.hsbc.com-ids-onlineserv-ssl-login-secure-id-user.708210.12secure.com.tw-rock.org/credit card/

Deception, creating trust, reveal sensitive information, activate hidden malicioius software.

41. Study the following website address and attempt to visit the website, describe What is wrong with this address by visiting the website
http://www.ebay.cd.co.uk/eBayISAPI.dll?ViewItem&item=150258354848&id=6

Spoofing, redirected, flow up site, curiosity arousal to view an item

42. Among the websites, you visited so far, evaluate and comment on:
   a) HTTPS – portraying a secure web address
   b) Padlock – portraying secure website

43. Study the two websites below and chose a comment:
www.mybank.com and www.my-bank.com

   a) both a genuine website
   b) one is genuine and one is fake
   c) two different websites for two different organization

44. Should you happen to encounter a threat or attacks through your online activities, how do you mitigate the encounters? By:
   a) Assignment;
   b) Directness;
   c) Memorability;
   d) Communication channel;
   e) None of the above

45. The websites you were directed to visit might have some anomalies, what is true of such anomalies?

a) I noticed nothing
b) URL mismatch
c) Padlock indicator
d) HTTPs

46. The websites you were directed to visit might have some expressions or messages, briefly state the tone of such expressions or messages:

Attention, Interest, Desire, Action, Commitment.

47. Among the scam mails you received, study them and classify them into
Some kind of groups
a) Attachment
b) Clink links
c) Log in details
d) Offers and promotions

48. Through the reference to your Facebook and some websites, if you have come across any form of online deception, briefly state them.
Click jacking, Phishing, Spoofing, Pretexing, Baiting.

49. Should you have to share information on your workplace social media what facilitate the dissemination and sharing of the information on the social media?

Comment, Post, Like, share, groups, tag

50. Suppose your workplace Facebook Platform for security mentioned that the security system should be RIR (Real-time sharing, Identification and Reaction) what does that mean to you? *Any of the followings is correct response.*
a) Social system of security
b) User collaborations on security
c) Employee participations on security, d) proactive security measures