International Journal of **Advanced Multidisciplinary Research Reports**
Volume I Number 1 Nov-Dec 2015 Maiden Edition

ONLINE SOCIAL ENGINEERS AND CYBER THREATS: AN EVALUATION OF YOUNG NIGERIAN FACEBOOK USERS

Charles Chukwuemeka Okika
Department of Mass Communication
Nnamdi Azikiwe University Awka
Anambra State,Nigeria
cc.okika@unizik.edu.ng

Allen Nnanwuba Adum
Department of Mass Communication
Nnamdi Azikiwe University, Awka,
Anambra State, Nigeria.
allenadum@gmail.com
08037585067

Uchenna Patricia Ekwugha
Department of Mass Communication,
Nnamdi Azikiwe University, Awka
Anambra State
ucheekwugha@yahoo.com
+2348035962584

ABSTRACT

Facebook social networking has forever changed the face of communication and socialization in Nigeria because of the interactivity it affords users. According to Facebook Reports, (2015), the highest population of Facebook users which constitutes 30.9% of the entire 1.4 billion subscribers are young adults within the age range of 18 to 25 years and also form the average age range of undergraduate students in various universities in Nigeria according to the United States Diplomatic Mission to Nigeria (2015). The Federal Bureau of Investigation (2015) describes social engineers as those who specialize in exploiting personal connections through social networks and are sometimes referred to as "human hackers,". It is argued that these social engineers manipulate the young facebook users through social interactions and other facebook communication platforms. It is also established that all manner of cybercriminals especially social engineers prowl this new information super highway with nefarious intentions.This study is therefore an attempt to assess the threats posed by the online engineers to young facebook users as regards to the violation of their personal security. Survey method was employed in this study and a sample size of 400 Facebook users were randomly selected through multi-stage sampling technique. Findings of the study indicate that most of these subscribers perceive Facebook as a relatively safe website despite the unguarded posts recorded on facebook. The findings further revealed that the young facebook users percieve facebook sites as a platform for valuable sales, public relations, advertising, marketing and diversions.

Keywords: *human hacker, social engineer, psychological manipulation, facebook, cyberthreat*

INTRODUCTION

This study is titled: *Online Social Engineers and Cyber Threats: An Evaluation of Young Nigerian Facebook Users*. The popularity of the social media has opened up lots of opportunities and changed how personal information is communicated to the audience whom greater percentage of them are strangers to account owners or subscribers. There are many studies that indicate that there is an increase in security issues founded on social media activity globally. As a result of this, there is a high threat level of what online social engineers who sometimes are referred to as "human hackers," who hide behind the cloak of disindividualization and anonimity to exploit personal connections which sometimes results in violation of privacy, cyberbullying, cyberstalking and even in the worst case scenario, violent and despicable crimes (Cluley, 2010; Daily Mail UK, 2015; Zimbardo,1969). According to Facebook Reports, (2015), the highest population of Facebook users which constitutes 30.9% of the entire 1.4 billion subscribers are young adults within the age range of 18 to 25 years and also form the average age range of undergraduate students in various universities in Nigeria according to the United States Diplomatic Mission to Nigeria (2015). It is argued that these online social engineers manipulate the young facebook users through social interactions and other facebook communication platforms. It is also established that all manner of cybercriminals especially online social engineers prowl this new information super highway with nefarious intentions. This study therefore will investigate what is applicable in Nigeria by assessing the threats posed by the online social engineers to young facebook users and to establish if the crimes commited by these online social engineers in developed countries are the same in Nigeria.

BACKGROUND OF THE STUDY

According to the Federal Bureau of Investigation(FBI), Internet-based social networking sites have created a revolution in social connectivity(FBI, 2015). However, con artists, criminals, and other dishonest members of the society are exploiting this capability for nefarious purposes. The shocking and gruesome murder of Facebook lover Cynthia Osukogu by her male Facebook friends in Lagos

in 2012,(The Sun September 2, 2012) has revealed that it is undoubtedly obvious that this so beloved product of the new media has opened up new avenues for disindividualization and anonimity which encourages social manipulation or social engineering, violation of privacy, cyberbullying, cyberstalking and even in the worst case scenario, facilitate violent and despicable crimes against an individual.

There are primarily two tactics used to exploit online social networks. In practice, they are often combined. Firstly, there are computer savvy hackers who specialize in writing and manipulating computer code to gain access or install unwanted software on your computer or phone. Secondly, social engineers or human hackers who specialize in exploiting personal connections through social networks. Social hackers, sometimes referred to as "social engineers," manipulate people through social interactions (in person, over the phone, or in writing). Humans are a weak link in cyber security, and hackers and social manipulators know this. They try to trick people into getting past security walls. They design their actions to appear harmless and legitimate. Falling for an online scam or computer hack could be damaging for an individual victim as well as the organization the victim works for.

According to Cluely(2010), once information is posted to a social networking site, it is no longer private. The more information a user posts, the more vulnerable the user may become. Even when using high security settings, friends or websites may inadvertently leak a user's information. Personal information a user shares could be used to conduct attacks against him or her or associates. The more information shared, the more likely someone could impersonate a user and trick one of the user's friends into sharing personal information, downloading malware, or providing access to restricted sites. Online predators, hackers, business competitors, and foreign state actors troll social networking sites looking for information or people to target for exploitation. Information gleaned from social networking sites may be used to design a specific attack that does not come by way of the social networking site.

STATEMENT OF THE PROBLEM

It has been established that there are many crimes committed globally which violates an indvidual's security and privacy with laser-sharp precision and they are

perpetuated by social engineers or social human hackers. These social engineers manipulate the young facebook users through social interactions and other facebook communication platforms.Also many researches established a link between these crimes and the victim's Facebook activity in developed countries.The question here is what is applicable in Nigeria besides the notoriety of the 2012 Cynthia Osukogu murder case which was an isolated event? Could online social engineers be a major threat to young facebook users in Nigeria? Could it be that the crimes commited by these online social engineers in developed countries are the same in Nigeria? All these questions form the concern of this study.

PURPOSE OF THE STUDY

In the light of the aforementioned research problem, this study is set out to establish the extent Facebook activity by young Facebook users made them vulnerable to social human hackers who directly posed a threat to individual security. Against this backdrop, the specific objectives are as follows:

1. To ascertain if the online social engineers manipulate young facebook users in Nigeria.
2. To know if the nature of crimes commited by these online social engineers in developed countries are obtainable in Nigeria.
3. To ascertain what these crimes are.
4. To measure how vunerable these young Facebook users perceive themselves to online social human hackers.

RESEARCH QUESTIONS

This study sought to answer the following questions:

1. To what extent do the online social engineers manipulate young facebook users in Nigeria**?**

2. Are the nature of crimes commited by these online social engineers in developed countries obtainable in Nigeria?

3. What are these crimes?

4. How vunerable do these young Facebook users perceive themselves to online social human hackers?

SCOPE

The threat to an individual's security as a Facebook user is quite broad as it encompasses cyber security, financial security, family security, workplace security, security of property and possesions etc. This study focused on the threat posed by social engineers on individual or personal security of young Facebook users in Nigeria with a focus on the undergraduates of two universities in Nigeria namely: Nnamdi Azikiwe University Awka Anambra State and Enugu State University of Science and Technology.

LITERATURE REVIEW: FACEBOOK SOCIAL NETWORKING

According to Carlson (2010), Facebook is an online social networking service headquartered in Menlo Park, California ,United States and offices. Its website was launched on February 4, 2004, by Mark Zuckerberg with his college roommates and fellow Harvard University students Eduardo Saverin, Andrew McCollum, Dustin Moskovitz and Chris Hughes. According to Facebook First Quarter Reports (2015) as at March 2015 Facebook has about 1.4 billion active monthly subscribers making it the most visited social network and an advertizers haven with a market value of $212 billion and a revenue of $12 billion in 2014. Researchers observe that undergraduate students are among the major Facebook users on a daily and use the platform to support their academic, as well as social goals (Ellison,2008;Ellison,2007).

iStrategylabs, (2015) also noted that these college students use the site in diverse ways to perform a wide range of social tasks (such as keeping in touch with high school friends or coordinating activities like sorority social events as well as registering users, creating a user profile, adding other users as "friends", exchanging messages, posting status updates and photos, sharing videos and receiving notifications when others update their profiles. Additionally, users may join common-interest user groups, organized by workplace, school or college, or other characteristics, and categorize their friends into lists such as "People from work" or "Close friends" (IBT Media Inc., 2015).

PERSONAL SECURITY

According to Tyska et al (2000) personal security can be defined as actions meant to protect people from physical violence, whether from the state or external states, from violent individuals and sub-state actors, from domestic abuse, or from predatory adults. For many people, the greatest source of anxiety is crime, particularly violent crime.

Talbot and Jakeman (2011) defined personal security as a general condition that occurs after adequate efforts are taken to deter, delay, and provide warning before possible crime, if such warning occurs, to summon assistance, and prepare for the possibility of crime in a constructive manner. Personal security aims to protect people from physical violence, domestic abuse, or from predatory adults. According to the US bureau of Diplomatic Security (2014), personal security can be analysed on various levels such as: residential security, security while travelling, security while lodged in a hotel, security for children, suspicious letters and parcels, carjacking, surveliance, sexual assault prevention. Social networking sites have been observed to pose certain threats.

Furthermore, Cluely (2010) observed that once information is posted to a social networking site like Facebook, it is no longer private and that the more information a user posts, the more vulnerable the user may become. The researcher further note that even when using high security settings, friends or websites may inadvertently leak a user's information and such personal information a user shares could be used to conduct attacks against him, her or their associates. The shows that the more information shared, the more likely someone could impersonate a user and trick one of the user's friends into sharing personal information, downloading malware, providing access to restricted sites or information to personal location or property (Talbot & Jakeman, 2011).

SOCIAL ENGINEERING

According to Anderson(2008) social engineeering in the context of information security though originally associated with the social sciences is the systemic

psychological manipulation of people into performing actions or divulging confidential information. It usually involves confidence tricks employed for the purpose of information gathering, fraud, or system access, it varies from a traditional "con" because it is often one of many steps in a more complex fraud scheme.

Jaco (2004) is of the opinion that most social engineering techniques are based on specific attributes of human decision-making known as cognitive biases. These biases, sometimes called "bugs in the human hardware", are exploited in various combinations to create attack techniques. The attacks used in social engineering can be used to steal employees' confidential information. The most common type of social engineering happens over the phone and lately via the Internet medium. Other examples of social engineering attacks are criminals posing as exterminators, fire marshals and technicians to go unnoticed as they steal company secrets. According to Kashyap, (2014) another example of social engineering would be that the hacker contacts the target on a social networking site and starts a conversation with the target. Slowly and gradually, the hacker gains trust of the target and then uses it to get access to sensitive information like password or bank account details. Cyberbullies, cyberstalkers, rapist and scam artists all adopt this strategy in varying degrees. (Mitnik and Simon, 2005).

According to the Federal Bureau of Investigation (2015) social engineers who specialize in exploiting personal connections through social networks and are sometimes referred to as "human hackers," manipulate people through social interactions either in person, over the phone, in writing or via the various online or Internet-based media. Humans are a weak link in cyber security and these hackers and social manipulators know this. They try to trick people into getting past security walls and private information. They design their actions to appear harmless and legitimate (FBI, 2015).

According to the Daily Mail UK (2015), a crime linked to Facebook is reported to police every 40 minutes. Last year, police officers logged 12,300 alleged offences

involving the vastly popular social networking site. Facebook was referenced in investigations of murder, rape, child sex offences, assault, kidnap, death threats, witness intimidation and fraud. For example, British teenager Ashleigh Hall was murdered by serial rapist Peter Chapman after he groomed her on Facebook. Chapman, 35, posed as a handsome teenager called Peter Cartwright to lure 17-year-old trainee nurse Ashleigh into his trap in September 2009. He sent her a series of text messages and arranged to meet some weeks later, claiming to be 'Peter's dad' to explain why he looked nothing like his photo. Chapman drove Ashleigh to a secluded area called Thorpe Larches, near Sedgefield in County Durham. Once there, he forced her to perform a sex act before binding and gagging her with duct tape, wrapping so much around her head that she suffocated to death. He then dumped her body in a ditch and drove off. In March 2010, Chapman was sentenced to a minimum of 35 years in jail for Ashleigh's kidnap, rape and murder.

The case cited by BBC News (2010) of the serial rapist Chapman shows that Facebook is a platform with clear and present danger associated with several crimes obtainable in the society thereby raising concern about how vulnerable these young and impressionable Facebook users can be to online social engineers which necessitates the evaluation of online social engineers and its cyberthreats among young Nigerian Facebook users.

SOCIAL ENGINEERING TECHNIQUES

Pretexting: According to the Federal Trade Commission (2012) ,pretexting also known as *blagging* or *bohoing*, is the act of creating and using an invented scenario or a pretext to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances.As in the case of an elaborate lie, it most often involves some prior research or setup and the use of this information for impersonation (*e.g.*, date of birth, Social Security number, last bill amount) to establish legitimacy in the mind of the target. Pretexting can also be used to impersonate co-workers, police, bank, tax authorities, clergy, insurance investigators or any other individual who

could have perceived authority or right-to-know in the mind of the targeted victim. The pretexter must simply prepare answers to questions that might be asked by the victim. In some cases, all that is needed is a voice that sounds authoritative, an earnest tone, and an ability to think on one's feet to create a pretextual scenario.

Diversion theft: Also known as the "Corner Game" or "Round the Corner Game", is a confidence trick originated in the East End of London. In summary, diversion theft is a "con" exercised by professional thieves, normally against a transport or courier company. The objective is to persuade the persons responsible for a legitimate delivery that the consignment is requested elsewhere hence, "round the corner"(Richmond Day & Wilson, 2010).

Phishing: is a technique of fraudulently obtaining private information. Typically, the phisher sends an e-mail that appears to come from a legitimate business a bank, or credit card company requesting "verification" of information and warning of some dire consequence if it is not provided. The e-mail usually contains a link to a fraudulent web page that seems legitimate with company logos and content and has a form requesting everything from a home address to an ATM card's PIN.

Confidence tricksters and fraudsters involved in Information Technology fraud by deliberately deceiving and manipulating people, exploiting human weaknesses to obtain personal benefit. Are also regarded as social engineers

Upcoming social engineering technique includes spoofing or hacking online indentity (IDs) of people having popular e-mail IDs such as Yahoo, Gmail, Hotmail, etc. and spoofing facebook profile names and pictures. Among the many motivations for human hacking by online social engineers are:

- Phishing debit/credit-card account numbers and their passwords.
- Cracking corporate/private e-mails and chat histories, and manipulating them by using common editing techniques before using them to extort money and creating distrust among individuals.
- Cracking websites of individuals, companies or organizations and destroying their reputation, including Facebook accounts.
- Malware,spyware and virus hoaxes

- Tricking users to run malicious code within the web browser via self-XSS attack to allow access to their Facebook or web account.

THEORETICAL FRAMEWORK

This study which its fulcrum is on the loss of self and disinhibition of individuals in a crowd to anti-social behaviour as a result of anonimity created by computer-mediated communication (CMC) is best built on two theories: The social identity model of deindividuation effects theory and Social Network Theory. The social identity model of deindividuation effects abbreviated as SIDE model is a theory developed in social psychology and communication studies. SIDE explains the effects of anonymity and identifiability on group behavior (Diener,1980). It has become one of several theories of technology that describe social effects of computer-mediated communication. Several works used the theory in describing computer-mediated communication for instance Van Swol, Braun, and Kolb's (2015) in their study titled *Deception, Detection, Demeanor, and Truth Bias in Face-to-Face (FtF) and Computer-Mediated Communication* tried to establish a relationship in detection of deception in Face-to-Face and Computer-Mediated Communication and found out that there was more deceptive omission used in FtF and more deceptive commission (bald-faced lies) used in CMC. In this instance what the researchers are trying to maintan is that individuals are prone to deceptive and manipulative behaviour when using anonimity created by computer-mediated communication as is obtainable in social networks.

According to Zimbardo (1969) the SIDE model provides an alternative explanation for effects of anonymity and other "deindividuating" factors that classic deindividuation theory cannot adequately explain. The model suggests that anonymity changes the relative salience of personal vs. social identity, and thereby can have a profound effect on group behavior. SIDE developed as a critique of deindividuation theory. Deindividuation theory was developed to explain the phenomenon that in crowds, people become capable of acts that rational individuals would not normally endorse. According to Chan (2010) in the crowd, so it would seem, humans become disinhibited and behave anti-normatively. Early versions of

deindividuation theory saw this as a consequence of reduced self-awareness and accountability.

Several studies have used this model to analyze how individuals in groups become disinhibited and anti-normative for instance, Kwon, Stefanone, and Barnett, (2015)in their study titled: *Social Network Influence on Online Behavioral Choices: Exploring Group Formation on Social Network Sites*, the study which was built on social influence literature to explore social network and gender effects on online behavior found out that network-related variables and gender are significantly associated with online behavior and that perceived social environment, measured by personal network exposure rate, is more significant than objective reality, measured by frequency of received social messages in determining behavior. This study is trying to maintain that online behaviour in this case Facebook users being manipulated by online social engineers can be associated personal network exposure rate, frequency of received social messages and perceived social environment.

RESEARCH METHODOLOGY

Survey method was employed for this research. The questionnaire was used as the survey instrument. Consequently, 400 copies of questionnaire were distributed to young people between the ages of 18 and 25 in two different universities in Nigeria –Nnamdi Azikiwe University, Awka (UNIZIK) in Anambra State and Enugu State University of Technology (ESUT). The choice of two universities located at different states of the country is to possibly generate more diversity of thoughts and responses. In Nnamdi Azikiwe University Awka, seven faculties were randomly selected from the total 14 faculties on the campus.

These include Faculties of Arts, Agriculture, Biosciences, Education, Engineering, Management Sciences and Social Sciences. From each of the seven faculties, a department was also randomly selected and these are: African and Asian Studies, Agric Economics and Extension, Parasitology and Entomology, Guidance and Counselling, Mechanical Engineering, Business Administration and Mass Communication.

In Enugu State University of Technology (ESUT) which has eight faculties and one college (which was treated as a faculty because it had departments), four faculties were randomly selected namely: Applied Natural Sciences, Education, Management Sciences, Law and College of Medicine in each of the following departments: Computer Science, Physical and Health Education, Marketing, Anatomy and Corporate Law.

Nnamdi Azikiwe university has a total population of 30, 038 undergraduate students while Enugu State University of Technology has a total population of 23, 125 undegraduate students surveyed from the registry departments of the various universities.

The next stage will involve determinig the sample size from the varied population of the universities.

Table 1. Breakdown of the Population by the Universities

S/N	Universities	Students Population
1.	UNIZIK	30,038
2.	ESUT	23,125
	Total	**53,163**

Drawing from the caculations, the total number of the population according to the universities population is 53,163. The next stage will be determinig the sample size from the calculations of Meyer (1973) as shown in Table 2 below which suggests that a population ranging from 1000 to infinity at 95% confidence level, a sample of 384 would be alright therefore the sample size for this study is 400 respondents from the population of the study.

Table 2: Population and Sample Size as determined by Meyer

Population Size	Sample Size
500,000+	384
100,000	383
50,000	381
10,000	370
5,000	357
3,000	341
2,000	278
1,000	278

Having determined the sample size, the next stage is to get the number of respondents from each of the universities because of the variation in the population of the undergraduate students. This is to enable the researcher to sample rare extremes of the given population and to avoid skewed results. Thus the ratio of each university will be used to get at the number of respondents alloted for each university using proportional startification method with the formular:

n_h = the startum sample size of each university

N_h = the individual population of each university

N = the overall total of all the universities

Therefor the calculated proportional allocation for the universities is as follows:

$$\textbf{UNIZIK} = \frac{400 \times 30{,}038}{53{,}163} = 226$$

$$\textbf{ESUT} = \frac{400 \times 23{,}125}{53{,}163} = 174$$

Summary of the distribution list is as follows:

UNIZIK = 226

ESUT = 174

Total = 400

Therefore the respondents will be emerge from the selected faculties and departments according to the ratio of the various universities:

UNIZIK = 226 (Ratio Number) /7 Departments

226/7 = 32.285

ESUT= 174 (Ratio Number) /4 Departments

174/4 = 43.5

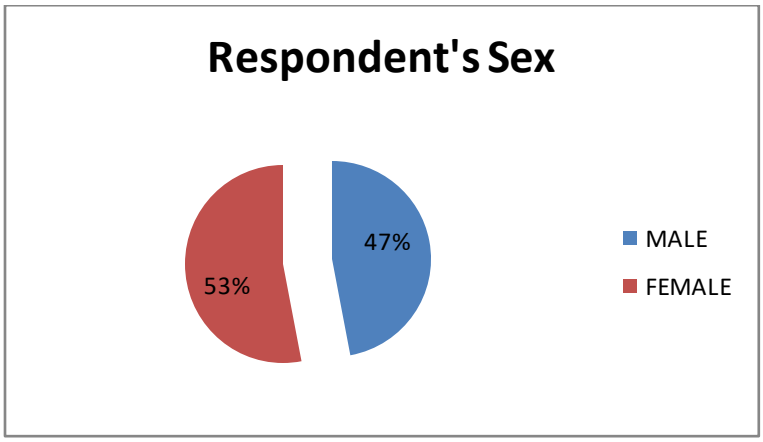
Thus 32 respondents will emerge in each of the selected departments in UNIZIK while 44 respondents will emerge in ESUT. The homogeneous purposive sampling technique at this point will be used to get at the active Facebook accounts. This is to enable the researchers to achieve a homogeneous sample; that is, a sample whose units (e.g., people, cases, etc.) share the same (or very similar) characteristics or traits (e.g., a group of people that are similar in terms of age, gender, background, occupation, etc.). A homogeneous purposive sample is often chosen when the research question that is being addressed is specific to the characteristics of the particular group of interest (active facebook subscribers).

For analyzing the data generated from the survey, the IBM's Statistical Package for Social Sciences (SPSS) version 17 was used. Data are presented in tables and charts.

ANALYSIS AND DISCUSSION OF FINDINGS

A total of 400 copies of the questionnaire that were distributed to respondents from Nnamdi Azikiwe University and Enugu State University of Technology Analysis was done with IBM's Statistical Package for Social Sciences (SPSS) Version 17. Below are the details of analysis based on prominent answers to the research questions explored in the study.

Chart 1: Respondents Sex



The chart above shows that majority of the respondents who are active facebook users are female undergraduates at 53 percent while 47 percent of the repondents are male showing a representation of the gender distribution of undergraduate students of the universities in South-East Nigeria which indicates that more females are enrolled in the universities than the male though with a slight margin.

Table 3. Respondents Facebook Activity Level

Respondents Facebook Activity Level	**No of Respondent**	**Percentage(%)**
Addictive	268	67%
Moderate	124	31%
Casual	8	2%
Total	400	100

The table above measured the respondents Facebook activity levels, majority of the respondents at 67% were addictive in their activity on Facebook, 31% were Moderate while 2% were casually active . The activity levels were characterized into three categories : Addictive level implied Facebook users who were always online and interacted intermittently on Facebook especially via mobile device Internet , moderate level implied users who subscribed to Facebook with moderation while casual were those who use facebook occassionally. That most of these subscribers were addicted to Facebook activity implies easy and affordable access to mobile Internet, lots of free time and an extended online presence. This also indicates that

Facebook could be a fruitful platform for valuable sales, public relations, advertising, marketing targeted at young Nigerians.

Table 4. Respondents posting of private information on Facebook

Responses	**No of respondenst**	**Percentage(%)**
Yes	286	71
No	114	29
Total	400	100

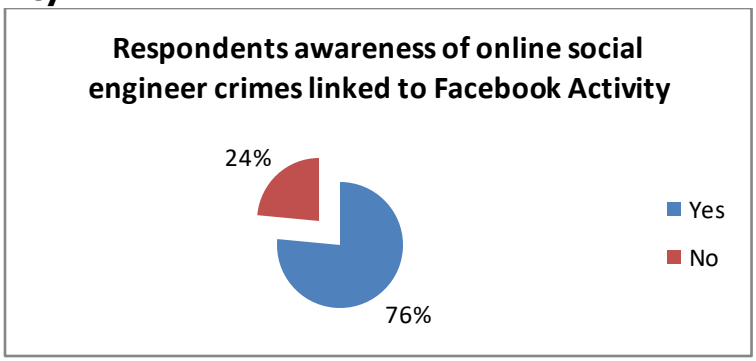
Respondents were exposed to questions meant to know if they post private information on Facebook, 71% admitted that they post private information on Facebook while 29% said they do not post private information showing that most respondents were not security conscious and this indication could pose a greater threat to the young impressionable minds who are the vunlnearble group.

Table 5. Respondents experience with invasion of privacy and breach of personal security link to Facebook activity?

Responses to Invasion of Privacy or breach of personal security	**No of respondent's**	**Percentage(%)**
Yes	12	3
No	388	97
Total	400	100

Respondents were also asked questions meant to find out if they have suffered invasion of privacy or breach of personal security directly linked to their Facebook activity, the table above shows that 3 % of the respondents said yes while 97% said no indicating that most of them have never suffered invasion of privacy or breach of security linked to their Facebook activity. This shows that in Nigeria, even though Cluely (2010) observe that once information is posted to a social networking site like Facebook, it is no longer private, most respondents think that they are not vulnerable to the cybertcriminals.

Table 6. Respondents awareness of online social engineer crimes linked to Facebook Activity



The respondents were further exposed to questions to inquire if they were aware of online social engineer crimes linked to Facebook activity. The table above showed that majority of the respondents at 76% were aware of crimes committed by online social engineers that were linked to facebook activity while 24% of them were not aware of such.Even though they are aware of these crimes, there are other indications that they think they are not vulnerable to such crimes.

Table 7: Respondents perception of obtainable crimes linked to Facebook online social engineer in Nigeria.

S/N	Nature Of Crimes	Strongly Agree	Agree	Strongly Disagree	Disagree	Undecided	Total Percentage
1	Kidnapping	10%	15%	45%	25%	5%	100%
2	Cyberbullying	16%	11%	35%	35%	3%	100%
3	Cyberstalking	17%	11%	37%	33%	2%	100%
4	Burglary	11%	2%	46%	38%	3%	100%
5	Financial scam	11%	14%	43%	27%	3%	100%
6	Rape	10%	4%	40%	45%	1%	100%
7	Murder	11%	3%	45%	40%	1%	100%

The respondents were also exposed to questions meant to determine what they thought about the obtainable crimes linked to Facebook online social engineers in

Nigeria. In the Table above, 45% of the respondents strongly disgreed that kindnapping was one of the crimes while 10% of the respondents strongly agreed. On the crime of cyberbully 35% of the respondents strongly disagreed while 16% strongly agreed. On the issue of cyberstalking, 17% strongly agreed while 37% strongly disagreed, on the crime of burglary 11% of respondents strongly agreed while 46% strongly disagreed. On financial scam 11% strongly agreed while 43% strongly disagreed, on the crime of rape, 10% strongly agreed, 40% strongly disagreed, while 1% is undecided. On the case of Murder 45% strongly while 11% strongly agreed its obtainability in Nigeria. These statistics indicated a generalized acknowledgement of non-significant presence of Facebook online social engineer crimes in Nigeria.

Table 8: Respondents perception of self as potential victims to crimes by Facebook online social engineers

Responses to perception of self as potential victims of Facebook online social engineer crimes	**No of respondent's**	**Percentage(%)**
Yes	27	7
No	373	93
Total	400	100

The respondents were also exposed to questions meant to determine how vunerable they percieved themselves to being potential victims of crimes by Facebook online social engineers and the Table above one can observe that 93% of respondents which is an obvious majority do not consider themselves potential victims of Facebook online social engineer crimes, while 7% have a contrary perception. Implying a sense of safety and security of this social network though this defer with the experience in developed countries where the Daily Mail UK (2015) reports that crimes such as rape, murder, cyberstalking, phishing etc that are linked to Facebook are reported to police every 40 minutes per day in the United Kingdom.

Table 9: Respondents overall perception of safety of Facebook activity

S/N	Perception of Facebook Activity	Strongly Agree	Agree	Strongly Disagree	Disagree	Undecided	Total Percentage
1	Safe	52%	30%	10%	6%	2%	100%
2	Unsafe	10%	6%	52%	30%	2%	100%

From the Table 9 above one can infer that 52% strongly agree that their Facebook activity is safe while 10% strongly disagree while 2% are undecided. In order to measure outrightly respondents perception of safety on Facebook, they were exposed to a conditional question dependent on affirmative to the questions meant to determine how vunerable they percieved themselves to being potential victims of crimes by Facebook online social engineers. This indicates that the majority of the respondents percieve Facebook activity as safe though there is an indication that with the rising use of mobile Internet among young impressionable minds, there might be a future danger because of their being exposed to the explosion of cyber criminals.

CONCLUSION

The findings answered the research questions of this study and suggested that for now online social engineers are not a threat to young Nigerian Facebook users. Social networking sites like Facebook can be a platform for valuable sales, public relations, advertising and marketing tools, as well as fun diversions. Inherent in these applications are security risks that can put the individual or a company in a compromising position or at serious risk. Aside from not using these sites at all, end-user education, alongside documented policies and procedures, is the most fundamental protection that exists. A well-informed user will not only help to maintain security, but will also educate others on these issues and establish best practices which can be standardized and updated as applications mature or as new applications come along.

Furthermore, the findings of the work indicates that the respondents are not vulnerable to cybercrimes perpetrated by online social engineers, however, the increase in use of mobile Internet in our society will create future danger for

facebook users with reagards to the menace of online social engineers and all manner of Internet predators.

REFERENCES

Anderson, R, J. (2008). Security engineering: A guide to building dependable distributed systems (2nd ed.). Indianapolis, IN: Wiley. p. 1040.

Carlson, N. (2010). "At Last – The full story of How Facebook was founded". Business Insider. March 5, 2010.

Chan, M. (2010). The impact of email on collective action: A field application of the SIDE model. New Media & Society, 12(8), 1313-1330.

Cluley, G. (2010) "Revealed: Which social networks pose the biggest risk?". Sophos. Retrieved July 12, 2010.

Daily Mail UK (2015). 400% of UK crimes linked to facebook: Retrieved from http://dailymail.co.uk.

Diener, E. (1980). Deindividuation: The absence of self-awareness and self-regulation in group members. In P. B. Paulus (Ed.), *The psychology of group influence* (pp. 209–242). Hillsdale, NJ: Lawrence Erlbaum.

Ellison, N. (2008). Introduction: Reshaping campus communication and community through social network sites. In G. Salaway, J. B. Caruso, & M. R. Nelson, The ECAR Study of Undergraduate Students and Information Technology, Research Study, Vol. 8. Boulder, CO: EDUCAUSE Center for Applied Research.Availableonline athttp://connect.educause.edu/Library/ECAR/TheECARStudyofUndergradua/47485.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. Journal of Computer- Mediated Communication, 12, pp.1143– 1168. Available online at http://jcmc.indiana.edu/vol12/issue4/ellison.html.

Facebook Reports (2015). First Quarter 2015 Results. April 22, 2015. Retrieved April 26, 2015

Federal Bureau of Investigation(2015). Internet Social Networking Risks. Retrived from www.fbi.gov/ InternetSocialNetworkingRisks.htm.

Federal Trade Commission (2012). How to keep your personal information secure. Retrieved from http://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure.

Kashyap, S (2014). Hack a Facebook Account with Social Engineering (Easiest Way) : Amazing Hacking Tricks. Retrieved from http://www.amazinghackingtricks.com/2014/06/hack-facebook-account-with-social.html.

Kwon, K.H., Stefanone, M.A. and Barnett, G.A. (2014).*Social Network Influence on Online Behavioral Choices: Exploring Group Formation on Social Network Sites.* American Behavioral Scientist September 2014 vol. 58 no. 10 1345-1360

IBT Media Inc. (2015). Facebook Gets Older: Demographic Report Shows 3 Million Teens Left Social Network In 3 Years. Retrived from www.ibtmediainc/ Facebook Gets Older: Demographic Report Shows 3 Million Teens Left Social Network In 3 Years.htm.

iStrategylabs. (2015). 2014 Facebook Demographic Report. Retrieved from www.istrategylabs.com/facebooksocialadsplatform.htm.

Jaco, K: (2004)"CSEPS Course Workbook", unit 3, Jaco Security Publishing.

Meyer, P. (1973). *Precision Journalism*. Bloomington: Indiana University Press.

Mitnick, K., & Simon, W. (2005). "The Art of Intrusion". Indianapolis, IN: Wiley Publishing.

Pew Research Center (2015). Social Networking Fact Sheet. Retrievement from http://www.pewinternet.org/Reports/2011/Technology-and-social-networks.aspx.

Reicher, S., Spears, R., & Postmes, T. (1995). A social identity model of deindividuation phenomena. European Review of Social Psychology, 6, pp.161–198.

Richmond Day & Wilson. (2010): Train for life Retrieved from http://web.archive.org/web/ 20100105024813/ http: //www.trainforlife.co.uk/onlinecourses.php.

Talbot, J. & Jakeman, M. (2011). *Security Risk Management Body of Knowledge*. John Wiley & Sons. pp. 72–73.

Tom Postmes, Russell Spears and Martin Lea's SIDE-Effects of computer-Mediated Communication.

Tyska, L, A. & Fennelly, L. J. (2000). *Physical Security: 150 Things You Should Know*. Butterworth-Heinemann. pp. 3.

The Sun September 2, 2012. The Police and Cynthia Osokogu. Retrieved from http://www.sunnewsonline.com/home/opinion/thepoliceandcynthiaosukogu.htm.

United States Bureau of Diplomatic Security(2014): Personal Security--At Home, On the Street, While Traveling. Retrieved from http://bds.gov.

United States Diplomatic Mission to Nigeria (2015). Nigerian education profile. Retrived from http://www.nigeria.usembassy.gov/resources/aboutNigeria/education.htm.

Van Swol,L.M, Braun,M.T. and Kolb,M.R. (2015). *Deception, Detection, Demeanor, and Truth Bias in Face-to-Face(FtF) and Computer-Mediated Communication (CMC).* Communication Research December 2015 vol. 42 no. 8 1116-1142

Zimbardo, P. G. (1969). The human choice: Individuation, reason, and order vs. Deindividuation, impulse and chaos. In W. J. Arnold & D. Levine (Eds.), *Nebraska symposium on motivation* ,Vol.17, pp. 237–307. Lincoln, NE: University of Nebraska Press.