A LINGUISTIC ANALYSIS OF SCAM MAILS

BY

REKIYA DEDE HARUNA

ADMISSION NUMBER: 1011110078

A PROJECT SUBMITTED TO THE DEPARTMENT OF MODERN EUROPEAN LANGUAGES AND LINGUISTICS, FACULTY OF ARTS AND ISLAMIC STUDIES, USMANU DANFODIYO UNIVERSITY SOKOTO, IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF BACHELOR OF ARTS (HONS) ENGLISH.

OCTOBER, 2015.

APPROVAL PAGE

This project has been read and approved by the under signed of the department of Modern European Languages and Linguistics, Faculty of Arts and Islamic Studies, Usmanu Danfodiyo University Sokoto, as meeting part of the requirements for the award of Bachelor of Arts degree (B.A.Hons) in English.

....

Mansur Isah Buhari Date

Project Supervisor

....

Dr. Muhammad Aminu Mode Date

Head of Department

....

External Examiner Date

DEDICATION

This research work is dedicated to God Almighty and also to my Father Late Mr Haruna Adoga Mamud.

ACKNOWLEDGEMENTS

My profound gratitude goes to God who is my source and sustainer through the course of my course.

Special thanks to my project supervisor, Mallam Mansur Isah Buhari who was always available to put me through. God bless you sir, you are a mentor indeed.

I express my sincere gratitude to my uncle Engineer Onayesemi Tajinas Berida and his lovely wife Mrs Amina Berida, for their support morally, emotionally, spiritually, academically, and financially. May God rain down his blessings upon your family. I wish to convey my special appreciation to my Mother Mrs Nana Mamud, and my siblings Rahanat Haruna, Isiaka and Malik Mamud, for their support. Mr and Mrs Peter, Mr and Mrs Bakare, may God bless reward you all.

I cannot fail to express my sincere thanks to my fiancée Femi Olasupo Aransiola who has been a source of encouragement to me, I say thank you dear.

I appreciate my best friend, Anna Ishaya Lekwot who has been like a sister to me, thanks friend. I also express my thanks to my friends Ganiyat Kemi Agiringbadi, and Maureen Agbugba, you guys have been true friend indeed.

I wish to express my gratitude to Late Professor Abdulrahim Maruf Adekunle,the formal HOD of Geography, may his soul rest in peace. Amen

Finally, I must not forget the whole MELL family, I say a big thank you. May God bless you all in your various future endeavours.

TABLE OF CONTENTS

CHAPTER ONE

1.0 INTRODUCTION

This chapter presents the general overview of this research work as well as its significance and statement of problems,and also possible solution to those problems as this study is aimed to achieve.

1.1 BACKGROUND TO THE STUDY

Scam mails are a form of financial fraud in which huge offers of money are made to people provided they pass on bank details and other personal information to the perpetrator.This kind of message presents us with a typical instance of globalized communication,they are produced in the margins of the world and sent to other places;they are electronically mediated;and they are written in varieties of world languages,mostly English.

Patterns in content include similar narratives involving vast sums of money to be transferred from the scammer's home country with outside help and common persuasive strategies frequently involving apologies,flattery,attempts to intrigue,trust and religious feelings,while patterns in writing features include use

of attention inducing buzz words like “urgent’’ and “secret’’ in subject headings as well as in the letters themselves, and obvious nonnative English grammar,mechanics and vocabulary errors.Inspite of the cruder elements of these letters and worldwide efforts to fight the con artists sending them,recipients are still drawn into these scams in large numbers,losing huge sums of money every year.The best defense against them must still entail comprehensive public education about the nature of this scam.

For now,it still seems likely that for every antiscam measure someone develops,scammers will devise a counter measure.Perhaps,then,preventing scam from reaching personal computers might better be treated as a secondary concern,the primary goal should infact be the education of netizens to recognize deceptive content,specious persuasive strategies,inaccurate and unfair stereotypes of a scam when they see them,ensuring that they will avoid becoming its next victim.

1.2 STATEMENT OF THE PROBLEM

In scam messages,authors claim particular identities and relationships,and have

to do so using specific,generically regimented forms of communication.Investigating such forms yields a complex view of what it takes to communicate in a globalized environment,at least three different forms of communicative competence seem to be blended.first,authors require technological competence,the capacity to control,explore and exploit the communicative opportunities offered by global email systems.Second,they require cultural competence,they need some awareness of genres and genre expectations among their addresses inorder to stand a chance of success.And thirdly,they need linguistic competence,the capacity to actually produce linguistic messages that are congruent with the projected identities and relationships in the transaction.

We see that whereas the first two forms of competence appear to be well developed,the third is often problematic,yieldying rich indexical signals pointing towards fraud.The genre of mail scams thus yields insights into the changing nature of communication in the age of globalization.

Email scam is an unsolicited email that claims the prospect of a bargain or

something for nothing. Some scam messages ask for business,others invite victims to a website with a detailed pitch. Many individuals have lost their life savings due to this type of fraud.Email scam is a form of email fraud, this scam usually begins with a letter or email purportly sent to a selected recipient but actually sent to many, making an offer that would allegedly result in a large payoff for the victim. More recently, scammers have also used fake but plausible seeming accounts on social networks to make contact with potential victims.

1.3 JUSTIFICATION FOR THE STUDY

This research investigates scam mails as a means of defrauding individuals who are ignorant of their linguistic features.The study will try as much as possible to educate individuals and the society at large on how to identify the linguistic features of these scams.

1.4 AIMS AND OBJECTIVES OF THE STUDY

This study shows the linguistic relevance of the language of scam mails, and directed at the effect of language of scam mails. This research will examine the general nature of scam mails on emails,SMS and facebook chats. It will

analyse the pattern of scam mails generally and specifically stating its linguistic significance.

1.5 SIGNIFICANCE OF THE STUDY

This research work is significant in the sense that it investigates the use of language in scam mails. However, scam mails have become ubiquitous and are done worldwide since the world is now a global village, therefore this study is expected to educate the general public of the language of scam mails. The language involved however is an area where many people have not delved into, being a relatively new area much has not been said or written on it. This study adds to the body of literature in the subject and shows the transformations that have occured over time to English language as a medium of communication,particularly in Nigeria.

1.6 SCOPE AND LIMITATIONS OF THE STUDY

The scope of this research is restricted to emails,SMS and facebook chats,samples would be taken from these mails and the scam would be analysed. The unavailability of material, because not much have been written of this study. The study stretches its finding with a view to unveil the linguistic features of scam

mails and the extent of its formality or informality in various context of the scam but the study will limit the confines of its research to SMS,facebook chats, and Emails and also, the communicative function of this mails.

1.7 CONCLUSION

In conclusion,this chapter has successfully been able to review the background to the study,statement of the problem,justification for the study,aims and objectives of the study, significance of the study and the scope and limitations of the study.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

In this chapter, related literature on this topic will be explore and review. It will cover most aspects of linguistics and scam e-mails.

2.2 The Concept of Linguistics

Brashers (2005) observed that Linguistics is the scientific study of language. There are three aspects to this study: language form, language meaning, and language in context. In linguistics, human language is a system of sounds, symbols, and meaning. Phonetics is the study of acoustic, visual, and articulatory properties in the production and perception of speech and non-speech sounds. The study of language meaning, on the other hand, deals with how languages encode relations between entities, properties, and other aspects of the world to convey, process, and assign meaning, as well as to manage and resolve ambiguity. While the study of semantics typically concerns itself with truth conditions, pragmatics deals with how context influences meanings.

Baron [2005], sees Grammar as a system of rules which govern the language of a particular speech community. It encompasses of sound, meaning, and gestures, and

includes phonology (how sounds and gestures function together), morphology (the formation and composition of words), and syntax (the formation and composition of phrases and sentences from words).

In the early 20th century Ferdinand de Saussure distinguished between the notions of *langue* and *parole* in his formulation of structural linguistics. According to him, parole is the specific utterance of speech, whereas langue refers to an abstract phenomenon that theoretically defines the principles and system of rules that govern a language. This distinction resembles the one made by Noam Chomsky between competence and performance, where competence is individual's ideal knowledge of a language, while performance is the specific way in which it is used. In classical Indian philosophy of language, the Sanskrit philosophers like Patanjali and Katyayana had distinguished between sphota (light) and dhvani (sound). In the late 20th century, French philosopher Jacques Derrida distinguished between the notions of speech and writing.

The formal study of language has also led to the growth of fields like psycholinguistics, which explores the representation and function of language in the mind; neurolinguistics, which studies language processing in the brain; and language acquisition, which investigates how children and adults acquire a particular language.

According to Balswick (2006), Linguistics also includes the study of other aspects like the influence of social, cultural, historical and political factors on language. The study of such cultural discourses and dialects is the domain of sociolinguistics, which looks at the relation between linguistic variation and social structures, as well as that of discourse analysis, which examines the structure of texts and conversations. Research on language through historical and evolutionary linguistics focuses on how languages change, and on the origin and growth of languages, particularly over an extended period of time.

Corpus linguistics takes naturally occurring texts or films (in sign languages) as its primary object of analysis, and studies the variation of grammatical and other features based on such corpora. Stylistics involves the study of patterns of style: within written, signed, or spoken discourse.[14]Language documentation combines anthropological inquiry with linguistic inquiry to describe languages and their grammars. Lexicography covers the study and construction of dictionaries. Computational linguistics applies computer technology to address questions in theoretical linguistics, as well as to create applications for use in parsing, data retrieval, machine translation, and other areas. People can apply actual knowledge of a language in translation and interpreting, as well as in language education- the teaching of a second or foreign language. Policy makers work with governments to

implement new plans in education and teaching which are based on linguistic research.

Language is central to our human nature, and linguistics is the systematic study of human language. Although on the face of it there is huge variation among the world's languages, linguists not only describe the diverse characteristics of individual languages but also seek to discover the deeper properties which all languages share. These common properties may give us an insight into the structure of the human mind.

Part of the appeal of linguistics is that it draws on methods and knowledge from an unusually wide range of scholarship and transcends the usual subject boundaries. For instance, the study of meaning draws on work by philosophers, whereas the part of our course concentrating on the sounds of speech takes place in our Phonetics Laboratory. Here computers are used to display and analyse the speech signal using methods from physics and engineering. This variety is what makes linguistics fascinating: at one moment you might be poring over a medieval text for evidence of how the grammar of a language has changed, and the next, learning about how the larynx creates sound energy for speech.

To Chafe (2005), He said the flexibility of language as a tool for communication depends on combining smaller elements into larger structures. Language does this

at several 'levels', and the description of languages involves different levels of analysis. *Syntax* describes the combination of words to form sentences; *morphology* describes the building of words from components such as roots and suffixes; and *phonology* identifies the sound-units of a language and describes aspects of their combination. These levels of language constitute a system for associating structures with meaning, and the study of meaning in language belongs to the domain of *semantics*. *Phonetics* is concerned with how people speak and understand speech, and with speech sounds themselves.

Baym (2005), views other linguistic sub-disciplines as being directed towards language in action. *Pragmatics* deals with the ways in which the meaning of an utterance depends on the context of its use. *Sociolinguistics* studies the relation between language and all aspects of society, from the way social groups mark themselves linguistically, to the dynamics of conversations. *Psycholinguistics* is concerned with how language is represented and processed in the mind, and how it is acquired. *Historical linguistics* reconstructs earlier forms of a language, and seeks general trends in the ways languages change; explanations for changes may draw on social and psychological aspects of language use.

The investigation of language has a long history, which is a topic of study in its own right, and it draws on techniques and knowledge from disciplines as diverse as

philosophy, physics, biology, psychology, and sociology. For many people part of the attraction of linguistics is that it transcends disciplinary boundaries, including notably the traditional boundary between the arts and sciences.

2.2 Branches of Linguistics

According to Campbell (2002), It is generally agreed that linguistics should include at least five parameters, namely, phonologic, morphologic, syntactic, semantic, and pragmatic. The following are these main branches of linguistics

2.2.1 Phonetics

Phonetics studies speech sounds , including the production of speech ,that is how speech sounds are actually made , transmitted and received ,the sounds of speech ,the description and classification of speech sounds ,words and connected speech ,etc.

Once we decide to begin an analysis of speech, ewe can approach on various levels .At one level, speech is s mater of anatomy and physiology. We can study organs such as tongue and larynx and their function in the production of speech. At another level, we can focus on the speech sounds produced by these organs by identifying and classifying the individual sounds .This is the domain of articulatory

phonetics. We can also investigate the properties of the sound wave—acoustic phonetics .As speech is intended to be heard or perceived ,it is therefore possible to focus on the way in which a listener analyses or process a sound wave—auditory phonetics

2.2.2 Phonology

Cherny (2005), defines Phonology as the studies of the rules governing the structure, distribution, and sequencing of speech sounds and the shape of syllables .It deals with the sounds systems of a language by treating phoneme as the point of departure .A phoneme is the smallest linguistic unit of sound that can signal difference in meaning. English has approximately forty-five phonemes. If you repeat the /p/ sound ten times, each production will vary slightly for some physiological reasons. In addition, the /p/ sound differs from that in poor or soup because each is influence by the surrounding sounds. Even so, each /p/ is similar enough so as not to be confused with another phoneme.

Phonetics is the study of speech sounds that the human voice is capable of creating, whereas phonology is the study of a subset of those sounds that constitute language and meaning .The first focuses on chaos while the second focus on order .

2.2.3 Morphology

According to Balswick (2006), Morphology is concerned with the internal organization of words .It studies the minimal units of meaning, morphemes and wordformation process. Although many people think of words as the basic meaningful elements of a language, many words can be broken down into still smallest units, called morphemes. Morphemes serve different purposes. Some derive new words by changing the meaning or the part of the speech, others only refine and give extra grammatical information about the already existing meaning of a word with meaning, there are many complexities involved.

Language differ in their degrees of dependence on the morphological components .In Latin ,for example, meaning is changing through the use of many morphological endings .In contrast ,in English words order is used more than morphological addition to convey much of the meaning of the utterance .For instance ,The dog sees the rabbit. If we change the order of the words and get the rabbit sees the dog , the sentence meaning changes .But in ‘Latin and in Russian , dog and rabbit take on some morphological endings depending on whether they are subject of the sentences, and can therefore change places without affecting the meaning of the sentence.

2.2.4 Syntax

Baym (2005), states that Syntax is about principles of forming and understanding correct English sentences .The form or structure of a sentence is governed by the rules of syntax .These rules specify word order ,sentence organization, and the relationships between words ,word classes and other sentence elements .We know that words are organized into structures more than just word order .

2.2.5 Semantics

According to Chafe (2005), Semantics examines how meaning is encoded in a language. It is not only concerned with meanings of words as lexical items ,but also with levels of language below the word and above it ,e.g. meaning of morphemes and sentences ,The following are what the key concepts look like :semantics components, denotation of words ,sense relation between such as antonymy and synonymy ,sense relation between sentences such as entailment and presupposition.

2.2.6 Pragmatics

Campbell (2002), defines Pragmatics as the study of meaning in context .It deals with particular utterances in particular situations and is specially concerned with the various ways in which the many social contexts of language performances can

influence interpretation .In other words, pragmatics is concerned with the way language is used to communicate rather than with the way language is structured.

It regards speech performance as primary a social act ruled by various social conventions. Some key concepts such as reference , force , effect, and cooperative principles may appear commonsensical ,yet pragmatics is just about one of the most promising fields of linguistic studies .Take conversation for example ,since language is transmitted primarily via the speech mode ,pragmatics rules govern a number of conversational interactions , such as sequential organization, repair of errors role and speech acts . Organization of conversations includes taking turns, opening, maintaining and closing a conversation, establishing and maintaining a topic etc.

2.3 The Concept of Scam E-Mail

Baron (2005), sees Email scam as an unsolicited email that claims the prospect of a bargain or something for nothing. Some scam messages ask for businesses, others invite victims to a website with a detailed pitch. Many individuals have lost their life savings due to this type of fraud. Email scam is a form of email fraud. This scam usually begins with a letter or email purportedly sent to a selected recipient but actually sent to many, making an offer that would allegedly result in a large

payoff for the victim. More recently, scammers have also used fake but plausible-seeming accounts on social networks to make contact with potential victims.

The email's subject line often says something like "From the desk of barrister [Name]", "Your assistance is needed", and so on. The details vary, but the usual story is that a person, often a ‘government’ or a ‘bank employee’, knows of a large amount of unclaimed money or gold which he cannot access directly, usually because he has no right to it. Such people, who may be real but impersonated people or fictitious characters played by the con artist, could include, for example, the wife or son of a deposed African leader who has amassed a stolen fortune, a bank employee who knows of a terminally ill wealthy person with no relatives, or a wealthy foreigner who deposited money in the bank just before dying in a plane crash (leaving no will or known next of kin), a US soldier who has stumbled upon a hidden cache of gold in Iraq, a business being audited by the government, a disgruntled worker or corrupt government official who has embezzled funds, a refugee, and similar characters. The money could be in the form of gold bullion, gold dust, money in a bank account, blood diamonds, a series of checks or bank drafts, and so forth. The sums involved are usually in the millions of dollars, and the investor is promised a large share, typically ten to forty percent, in return for assisting the fraudster to retrieve or expatriate the money. Although the vast majority of recipients do not respond to these emails, a very small percentage do,

enough to make the fraud worthwhile, as many millions of messages can be sent daily.

Balswick (2006), states that to help persuade the victim to agree to the deal, the scammer often sends one or more false documents bearing official government stamps, and seals. 419 scammers often mention false addresses and use photographs taken from the Internet or from magazines to falsely represent themselves. Often a photograph used by a scammer is not a picture of any person involved in the scheme. Multiple "people" involved in schemes are fictitious; the author of the "West African Advance Fee Scams" article posted on the website of the Embassy of the United States in Abidjan, Ivory Coast believes that, in many cases, one person controls many fictitious personas used in scams.

Once the victim's confidence has been earned, the scammer then introduces a delay or monetary hurdle that prevents the deal from occurring as planned, such as "To transmit the money, we need to bribe a bank official. Could you help us with a loan?" or "For you to be a party to the transaction, you must have holdings at a Nigerian bank of $100,000 or more" or similar. This is the money being stolen from the victim; the victim willingly transfers the money, usually through some irreversible channel such as a wire transfer, and the scammer receives and pockets it. More delays and additional costs are added, always keeping the promise of an

imminent large transfer alive, convincing the victim that the money the victim is currently paying is covered several times over by the payoff. The implication that these payments will be used for "white-collar" crime such as bribery, and even that the money they are being promised is being stolen from a government or royal/wealthy family, often prevents the victim from telling others about the "transaction", as it would involve admitting that they intended to be complicit in an international crime. Sometimes psychological pressure is added by claiming that the Nigerian side, to pay certain fees, had to sell belongings and borrow money on a house, or by comparing the salary scale and living conditions in Africa to those in the West. Much of the time, however, the needed psychological pressure is self-applied; once the victims have provided money toward the payoff, they feel they have a vested interest in seeing the "deal" through. Some victims even believe they can cheat the other party, and walk away with all the money instead of just the percentage they were promised.

According to Chafe (2005), The essential fact in all advance-fee fraud operations is the promised money transfer to the victim which never happens, because the money does not exist. The perpetrators rely on the fact that, by the time the victim realizes this (often only after being confronted by a third party who has noticed the transactions or conversation and recognized the scam), the victim may have sent huge sum of their own money, and sometimes thousands more that have been

borrowed or stolen, to the scammer via an untraceable and/or irreversible means such as wire transfer. The scammer disappears, and the victim is left on the hook for the money sent to the scammer.

Baym (2005), states that during the course of many schemes, scammers ask victims to supply bank account information. Usually this is a "test" devised by the scammer to gauge the victim's gullibility; the bank account information is not used directly by the scammer, because a fraudulent withdrawal from the account is more easily detected, reversed, and traced. Scammers instead usually request that payments be made using a wire transfer service like Western Union and MoneyGram. The reason given by the scammer usually relates to the speed at which the payment can be received and processed, allowing quick release of the supposed payoff. The real reason is that wire transfers and similar methods of payment are irreversible, untraceable and, because identification beyond knowledge of the details of the transaction is often not required, completely anonymous. However, bank account information obtained by scammers is sometimes sold in bulk to other fraudsters, who wait a few months for the victim to repair the damage caused by the initial scam, before raiding any accounts which the victim did not close.

Telephone numbers used by scammers tend to come from mobile phones. In Ivory Coast a scammer may purchase an inexpensive mobile phone and a pre-paid SIM card without submitting any identifying information. If the scammers believe they are being traced, they discard their mobile phones and purchase new ones.

2.4 History of Scam e-mail

Campbell (2002),sees419 scam as a form of advance-fee fraud similar to the Spanish Prisoner scam dating back to the late 18th century. In that con, businessmen were contacted by individuals allegedly trying to smuggle someone connected to a wealthy family out of a prison in Spain. In exchange for assistance, the scammer would promise to share money with the victim in exchange for a small amount of money to bribe prison guards. One variant of the scam may date back to the 18th and 19th centuries, as a very similar letter, entitled "The Letter from Jerusalem", is seen in the memoirs of Eugène François Vidocq, a former French criminal and private investigator. Another variant of the scam, dating back to circa 1830, appears very similar to what is passed via email today: "Sir, you will doubtlessly be astonished to be receiving a letter from a person unknown to you, who is about to ask a favour from you...", and goes on to talk of a casket containing 16,000 francs in gold and the diamonds of a late marchioness.

The modern 419 scam became popular during the 1980s. There are many variants of the letters sent. One of these, sent via postal mail, was addressed to a woman's husband, and inquired about his health. It then asked what to do with profits from a $24.6 million investment, and ended with a telephone number. Other official-looking letters were sent from a writer who said he was a director of the state-owned Nigerian National Petroleum Corporation. He said he wanted to transfer $20 million to the recipient's bank account – money that was budgeted but never spent. In exchange for transferring the funds out of Nigeria, the recipient would keep 30% of the total. To get the process started, the scammer asked for a few sheets of the company's letterhead, bank account numbers, and other personal information. Yet other variants have involved mention of a Nigerian prince or other member of a royal family seeking to transfer large sums of money out of the country.

The spread of e-mail and email harvesting software significantly lowered the cost of sending scam letters by using the Internet. While Nigeria is most often the nation referred to in these scams, they may originate in other nations as well. For example, in 2006, 61% of Internet criminals were traced to locations in the United States, while 16% were traced to the United Kingdom and 6% to locations in Nigeria. Other nations known to have a high incidence of advance-fee fraud include Ivory Coast, Togo, South Africa, the Netherlands, and Spain.

According to Chafe (2005), One reason Nigeria may have been singled out is the apparently comical, almost ludicrous nature of the promise of West African riches from a Nigerian prince. According to Cormac Herley, a researcher for Microsoft, "By sending an email that repels all but the most gullible, the scammer gets the most promising marks to self-select." Nevertheless, Nigeria has earned a reputation as being at the center of email scammers, and the number 419 refers to the article of the Nigerian Criminal Code (part of Chapter 38: "Obtaining property by false pretenses; Cheating") dealing with fraud. In Nigeria, scammers use computers in Internet cafés to send mass emails promising potential victims riches or romance, and to trawl for replies. They refer to their targets as *Magas*, slang developed from a Yoruba word meaning "fool". Some scammers have accomplices in the United States and abroad that move in to finish the deal once the initial contact has been made.

According to Campbell (2002), In recent years, efforts have been made, by both governments and individuals, to combat scammers involved in advance-fee fraud and 419 scams. In 2004, the Nigerian government formed the Economic and Financial Crimes Commission (EFCC) to combat economic and financial crimes, such as advanced fee fraud. In 2009, Nigeria's EFCC announced that they had adopted smart technology developed by Microsoft to track down fraudulent emails. They hoped to have the service, dubbed "Eagle Claw", running at full capacity to

warn a quarter of a million potential victims. Some individuals may also participate in a practice known as scam baiting, in which they pose as potential targets and engage the scammers in lengthy dialogue so as to waste their time and decrease the time they have available for real victims. Details on the practice of scam baiting, and ideas, are chronicled on a website, 419eater.com, launched in 2003 by Michael Berry. One particularly notable case of scam baiting involved an American who identified himself to a Nigerian scammer as James T. Kirk. When the scammer — who apparently had never heard of the television series Star Trek — asked for his passport details, "Kirk" sent a copy of a fake passport with a photo of *Star Trek*'s Captain Kirk, hoping the scammer would attempt to use it and get arrested.

2.5 Types of scam e-mail

According to Balswick (2006), some of the earliest forms of cybercrime were email scams, which continue to this day. Here are five of the most common types:

2.5.1 Foreign Lottery Scam

The foreign lottery scam is one of the most common types of email scams, in which one receives what looks like an official email from a foreign lottery

corporation. The subject line offers a congratulatory announcement, and may include the supposed amount of money one has "won."

Here are the sure signs your winnings are false:

- **The Sender Is a Person**. If the sender is an individual – or is, at least, obviously not an official lottery email – then you know you have got a scam on your hands. For example, mikesmith1453@earthlink.com certainly is not going to be the guy to tell you that you have won several million dollars.
- **Your Name Is Not in the "To" Field**. If your name is not in the "To" section of the email, then this phishing email has likely been sent to thousands of people, all in the hopes of snagging a few bites.
- **The Lottery Does not Exist**. Do a simple Google search. Does the lottery even exist? You may find that not only is the lottery fake, but that it is a well-documented scam.
- **Request for Information**. Scammer emails routinely request your full name, date of birth, street address, and telephone number. This is known as a phishing scam, which is designed to get you to reveal sensitive personal information. Once you respond with this information, you have been hooked, and may ultimately end up with a stolen identity or, even worse, a drained bank account.

The best way to avoid the common email scam is to realize this one simple rule: If you did not enter the lottery, you will not win the lottery. And even if you do enter the lottery, you probably will not win.

2.5.2 Survey Scam

Baron (2005), states that this common email scam looks innocent enough. You have expressed interest in social issues, such as global warming or the war in the Middle East, and you have been sent a survey that requests your input. Why not participate? Unless you have specifically requested to be on a survey mailing list, what you are getting is nothing but spam.

When you click on the link to take the survey, malicious spyware or malware is installed on your computer. Once this occurs, cybercriminals can spy on every move you make on your computer, collecting passwords, bank account information, and more. Suddenly, you may see thousands of dollars worth of charges on your credit card bill for purchases you never made. This is result of identity theft, and it can ruin your life.

2.5.3 PayPal or Online Credit Card/Banking Scam

According to Baym (2005), At first, you may really believe there is something wrong with your PayPal account, as you will receive an email that appears to be

from PayPal with a warning message such as, “Act now, or your account will be deactivated,” or “Security breach on your account.” This can cause you to panic, open the email, click the link, and log in to your account.

The problem is that you’re not really on PayPal’s website, but rather a false website designed to look identical to PayPal. You’ve just given your email address and password to your actual PayPal account to a cybercriminal, who can now use that information to change your password and clean you out. They may even use this information to scam your friends and business associates.

2.5.4 Mystery Shopper Scam

According to Cho,T. (2006), The secret shopper (or mystery shopper) scam has several different variations, but all are designed to steal your money, your information, or both. This common work-from-home scam attempts to suck you in with an email featuring a subject line promising you a large income, simply by working as a mystery shopper. You need no experience or education, and you can make up to $200 to $300 a day doing just what you love: shopping! Sounds too good to be true, right?

It is indeed. Instead of being paid to shop, here are the two ways in which you can be swindled:

- **You Have to Pay Upfront**. The money looks good, but in order to get your "training materials," you must send the company money via PayPal or with a personal check. You send the money and wait for a package that never arrives.
- **You Receive a Fraudulent Check**. This one is even worse. You provide the false company your address, and are sent a fraudulent check in the mail as your first payment. However, you are requested to send some of the money back to cover your study materials. You cash the check, wire the requested amount of money, and then discover that the check you deposited has bounced. You are responsible for $1,000 or more worth of fraudulent check charges, plus overdraft fees.

If you did not apply for a job, you would not be offered a job. They do not just fall out of the sky. Furthermore, if you are ever asked to spend money upfront for materials, you are likely being scammed.

2.5.5 Nigerian Check Scam

According to Cherny (2005), Another one of the more common email scams is the Nigerian check scam. If you are subject to this scam, you receive an email from a royal-sounding person with the name of "Sir Arthur Von-Monsoon," or "Barrister Frank N. Stein" with a request to help recover large sums of money from an

overseas bank. As a reward, you will receive a handsome cut of the cash. Nice, huh?

Unfortunately, there is always a catch. It seems like a win-win situation, so you respond with your willingness to help. You are told the money will be transferred to your bank account; therefore, you must provide your bank account information. Also, there are transfer fees involved, and you have to pay those as well. Once you pay a couple hundred dollars, waiting for your huge windfall, you receive another email stating there has been some type of holdup, and you must send a bit more cash.

This continues until the unsuspecting victim, realizes that money is only going one way out of their bank account.

2.5.6 Job Scams

The victim is seeking a job and posts a resume on any internet job site. The scammer spots the resume and sends the victim an email claiming to be a legitimate job listing service, claiming to have a client who is looking for an employee with their skills and experience. The victim is invited to click on a link to apply for the job. Clicking the link takes the victim to a job description specifically written for the skills and experience on the victim's resume which provides a very high salary, and invites them to 'click here'' to apply for the job. If

the victim clicks on that ‘appy’’ link, they are taken to an ‘application’’ form that asks for the normal job application information, PLUS the victim’s social security number, date of birth, the name of the bank and account number where they will want their paycheck to be deposited to, a ‘relative’’ reference, etc. With this information,the scammer can open up a bank account in any on-line bank and utilize the victim’s credit to buy items on line and ship them to associates who are in the scam.

2.5.7 Quiz Scam

It may be in one’s best interests to delete all app requests, and never take social networking quizzes. Turns out those “Which Twilight Character Are You?” quizzes could end up costing you a monthly charge.

It starts out innocently enough: You see the quiz on your friend’s profile, click on it, and enter your cell phone number as instructed. The quiz pops up, you take it and find out you are more an Alice than a Bella, and promptly post it on your profile for all of your friends to see and participate in.

When next month rolls around, you are shocked to learn that a $9.95 fee has been added to your cell phone bill for some dubious “monthly service.” Remember that the quiz asked you for your cell phone number in order for you to take it? You

were so anxious to get the results that you did not even stop to wonder why they wanted it. Now you know.

2.5.8 Suspicious Photo Scam

According to Cho, T. (2006), This is one of the most common ways online con artists obtain login information to hijack an account. One of your friends, whose account has been hacked, posts a link on your page with a message such as, "OMG! Is this a naked picture of you?"

This causes you to panic and you click the link, only to find yourself back at the Facebook login page. You figure it is just one of Facebook's many glitches and login again.

By doing this, you have just disclosed your Facebook (or Twitter) account login information. Now, some cybercriminal is out there using your profile to attempt to scam your friends.

If you see a suspicious link, simply delete it and send a message via email or text message to your friend to warn them they have been hacked.

2.5.9 Hidden URL Scam

According to Cherny (2005), As a regular Twitter user, always use TinyURL.com to shorten your links. Plenty of legitimate businesspeople do this to get around Twitter's character limit. However, when clicking links, it's best to err on the side of caution.

When you receive a new follower on Twitter, check out their previous updates. Do they all look like spam? Do they follow thousands of people, yet have few followers of their own? Is their profile picture worthy of a Victoria Secret or Maxim catalog cover? If this is the case, beware. Clicking on their links could take you to a website where spyware or malware might be downloaded onto your computer without your knowledge.

2.5.10 Sick Baby Scam

Campbell (2002), states that the sick baby scam works like this: A "friend" posts a photograph of an ill baby or young child with a caption beneath it that reads, "Little Jimmy has cancer. Click this link to donate $1 to help him and his family. Every little bit counts!"

Your heart goes out to this helpless little baby, and you click on the link, whip out your bank card, and donate some money. What you do not realize is that the money

is not going to help some dying child – it is going straight to the bank account of a con artist.

Also, remember that shares do not equal donations. Often, instead of sending money to help the “sick baby,” you are asked to share the photo with everyone you know because each share supposedly earns $0.05. However, Facebook, nor any social networking website, will donate money based on how many times something is shared. This is almost always an attempt to phish for personal information.

2.6 The Nigerian E-Mail Scam

Nigeria also contains many businesses that provide false documents used in scams; after a scam involving a forged signature of Nigerian President Olusegun Obasanjo in summer 2005, Nigerian authorities raided a market in the Oluwole section of Lagos. The police seized thousands of Nigerian and non-Nigerian passports, 10,000 blank British Airways boarding passes, 10,000 United States Postal money orders, customs documents, false university certificates, 500 printing plates, and 500 computers.

The "success rate" of the scammers is also hard to gauge, since they are operating illegally and do not keep track of specific numbers. One individual estimated that

he sent 500 emails per day and received about seven replies, citing that when he received a reply, he was 70 percent certain he would get the money. If tens of thousands of emails are sent every day by thousands of individuals, it doesn't take a very high success rate to be worthwhile.

2.8 CONCLUSION

In conclusion, this chapterhas successfully been able to review linguistic concept and its branches and also the concept of scam emails, as well as its linguistic features.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

The purpose of this chapter is to discuss the methods of investigation used. This chapter contains relevant facts concerning the research design, population of the study as well as the analysis of the data and justification for research methods used.

3.1 Research Design

The study used historical research design. The historical research research deals with the determination, evaluation and explanation of past events essentially for the purpose of gaining a better understanding of the present and making a more reliable prediction of the future (Ade 1999).

3.2 Sample and Sampling Techniques

The sample size for this study consist of thirty(30) email messages. This can be shown in a clear manner in the table as follows;

S/N	NAMES OF SOCIAL MEDIA	NUMBER OF MESSAGES	PERCENTAGE

1	Facebook chats	10	50%
2	E-mail messages	10	50%
3	Text messages (SMSs)	10	50%

The above table shows the sample size of the population. The researcher considered ten(10) messages each from the selected electronic mail messages, the selection of the email messages is based on random sampling in consideration of the different electronic mail chats we have.

3.3 The research tools used in collecting data for this study are the social media (internet) newspapers, magazines and textbooks. This research tool was used in order to get the authentic data.

3.4 Validity and Reliability of Tools

In order to get the validity and reliability of the research tools, the researcher used the social media(internet) in sorting datas, that is, from individual facebook accounts, email accounts and text messages. These datas were the original messages sent to the individuals by the scammers. This is to ensure that the data to be obtained is reliable as no oral interview or questionnaire was administered. The

researcher used this research tools in order to get the adequate outcome the study is intended to measure, to a certain extent the study is valid and reliable.

3.5 Method of Data Collection

Taking into cognizance the nature and objective of the study, the use of data collection tools such as the questionnaire or interview is not considered necessary. The researcher used secondary source of data collection, such as documents from empirical studies, textbooks, internet articles and journals to establish the framework and arguments that are related to the study.

3.6 Method of Data Analysis

As regards the method of data analysis suitable for this research project, a non-statistical method of data analysis will be employed since no questionnaire was administered.

3.7 Conclusion

This chapter deals with the designs employed by the study and the methods and procedures used in conducting the research work. The sources from which data for the study was collected; and the techniques used for analyzing the data collected are also clearly spelt out in this chapter. The secondary method of data collection was used because of the fact that data collected have a unique peculiarity features to the researcher and the particular research.

CHAPTER FOUR

DATA PRESENTATION AND ANALYSIS, SUMMARY AND CONCLUSION

4.1 Introduction

This chapter contains data analysis and presentation according to secondary data analysis.

4.2 The Linguistic Features of Nigerian Scam E-mails

According to Baron (2005), in Nigeria with the emergence of greater computer/interest mediated communication systems, coupled with the readiness with which people adapt to meet the new demands of a more technological sophisticated world, it is expected that users will continue to remain under pressure to alter their language use to suit the new dimensions of communication.

As the number of internet users increases rapidly around the world, the cultural background, linguistic habits and language differences among users are brought into the Web at a much faster pace. These individual differences among Internet users are predicted to significantly impact the future of Internet linguistics, notably in the aspect of the multilingual Web. As seen from 2000 to 2010, Internet penetration experienced its greatest growth in non-English speaking countries such

as China, India and Africa, resulting in more languages apart from English penetrating the Web.

Also, the interaction between English and other languages is predicted to be an important area of study. As global users interact with each other, possible references to different languages may continue to increase, resulting in formation of new Internet stylistics that spans across languages. Chinese and Korean languages have already experienced English language's infiltration leading to the formation of their multilingual Internet lingo.

At current state, the Internet provides a form of education and promotion for minority languages. However, similar to how cross-language interaction has resulted in English language's infiltration into Chinese and Korean languages to form new slang, minority languages are also affected by the more common languages used on the Internet (such as English and Spanish). While languages interaction can cause a loss in the authentic standard of minority languages, familiarity of the majority language can also affect the minority languages in adverse ways. For example, users attempting to learn the minority language may opt to read and understand about it in a majority language and stop there, resulting in a loss instead of gain in the potential speakers of the majority language. Also, speakers of minority languages may be encouraged to learn the more common languages that are being used on the Web in order to gain access to more

resources, and in turn leading to a decline in their usage of their own language. The future of endangered minority languages in view of the spread of Internet remains to be observed.

Statistics concerning Internet use at any given time vary according to many factors, including disparities across regions of the world and other demographic characteristics of users such as age and socio-economic status (cf, Pew Internet and American Life Project, 2005). This variation not withstanding, statistics on Internet use generally point to a steady growth in the number of users. According to one source, the total world Internet population increased from 6,084,907,596 users in 2000 to 6,845,609,960 users in 2010 (Internet World Stats, 2010). Broadband usage is also increasing, with developing markets such as China and India predicted to drive further growth (European Travel Commission, 2010). Along with the increase in number of users, use of the Internet for interpersonal communication continues to grow.

Among the internet technologies used for interpersonal communication is *electronic mail (email),* one of the oldest forms of computer-mediated communication (CMC) (Hafner & Lyon, 1996). In 2000, it was estimated that 90% of Web users connected to Internet primary to view and send email (NUA, 200). Moreover, the number of worldwide email accounts is predicted to increase from over 2.9 billion in 2010 to over 3.8 billion in 2014 (Radicati, 2010). Evidence is

inconclusive as to whether social networking services compete with or facilitate email usage, an issue that is further complicated by the integration of email with social networking services (Carr, 2010; European Travel Commission, 2010). Yet despite the importance of email, language specialists have conducted relatively few studies of this form of communication, focusing more often on publicly-available multi-participant discourse in chat rooms, newsgroups, and discussion forums (e.g, Cherny, 1999; Grubner, 1996; Herring, 1996; Werry, 1996).

This item analyzes the linguistic features of email and written memoranda in an academic workplace setting. To date, no linguistic study has compared email and memoranda, despite the fact that the former is replacing many of the functions of the latter, as pointed out by Yates and Orlikowski (1993). At the same time, research suggests that email is structurally and stylistically different from other types of workplace communication. For instance, although email and memoranda are both forms of written communication that are typically composed on a keyboard, and both are *asynchronous* an addressee need not be present to receive messages (LaQuey & Ryer, 1993) email has been claimed to exhibit features of oral communication (see e.g, Murray, 1990; Uhlirova, 1994). Certainly email can be used for informal purposes such as suggesting a lunch date to a colleague for which it would be inappropriate to write a memorandum. This point is echoed by Yates and Orlikowski (1993), who claim that the “memo genre” was “elaborated”

in email in the 1970s to the 1990s. at the same time, they note that email can be used to convey messages that would not typically be handled through memoranda (e.g, a one-word response to a question). They suggest that email composition draws selectively on the memo genre and that some email messages resemble genres other than memoranda, and conclude with a call for empirical research.

Although some developments in the structural and linguistic features characterizing electronic mail have been noted, without further empirical study it is not clear whether these have become sufficiently widespread or stable within smaller or larger communities to be institutionalized as genres. (Yates & Orlikkwoski, p. 320)

Balswick (2006), states that in order to compare email and memoranda, the present study empirically analyzed a variety of structural linguistic features, including the use of contractions, abbreviations, ellipsis, features relating to grammatical complexity, and phatic communication in the form of greeting and leave-taking formulas. The results show that email and memoranda even when produced in the same workplace environment are linguistically different varieties of communication. Several factors are suggested to explain the differences, notably the tendency in email towards linguistic economy, expressivity, and attempts by users to imitate an informal ‘oral style’. Email style is also found to be more

variable than that for memoranda, a result which is proposed to relate to the relative lack of established norms for email communication.

Baym (2005), states that the remainder of this article is organized as follows. The next section provides theoretical background on linguistic research on CMC, with a focus on the notions of linguistic economy and social expressivity. This is followed by a description of the methods and procedures followed in the present study and a presentation of the results for the email and memoranda samples. The results are presented in three categories: structural features, phatic features as evidenced by greeting and leave-taking formulas, and linguistic innovation. These findings are then discussed and interpreted in light of competing forces at work in the email usage of professional colleagues who must also interact face-to-face.

4.2.1 Presentation of Data

This chapter dwells on the presentation of data of e-mail messages such as Facebook messages, e-mail messages and text messages.

4.2.2 Analysis of cases of Facebook Scam

Sample 1: free facebook credits scam

Get your FREE 5000 FACEBOOK CREDITS! NO SCAM NO SURVEYS no waste of time no task, its totally FREE! this promo is available for the first 1000 persons only…CHECK IT OUT ENJOY…i got mine and it works get yours

here

http://creditsoffers.blogspot.com.

In the sample above, the content was not specific “Get your FREE 5000 FACEBOOK CREDITS!” the scammer did not state the type of credit to be acquired. Too much emphasis was made on the acquisition of it “NO SCAM NO SURVEYS no waste of time no task, its totally free!” in order to convince or lure the victim. “I got mine and it works, get yours here” is an incomplete sentence, it was suppose to be “I got mine and it works; get yours here by clicking on the link below”. The scammer here used the third person singular instead of first person singular.

Sample 2: change your facebook color

Are you sick of that boring old blue theme? Well now you have the power to change your facebook color to anything your heart desires! By clicking “Change Your Color” botton above. I accept and agree by the terms of use.

In the above sample, “ you have the power to change your facebook colour to anything your heart desires! By clicking on the Change Your Color botton above” there is no button on any phone indicated as Change Your Color. “I accept and agree by the terms of use” the above message did not display any terms in order for the victim to accept or decline.

Sample 3: facebook profile view scam

This application allows you to check who visited your profile. Get a detailed report of profile, IDs and datas as well as total views count. To see your stats, please complete the following two steps.

There are grammatical errors in the sample above that qualifies the message to be a scam. “Get a detailed report of profile, IDs and datas”, instead of “Get a detailed report of your profile, IDs and data”. “please complete the following two steps” meanwhile no steps were outlined in the message.

Sample 4: free product Giveaway Posts

Hey I can’t believe it, I actually got a free ipad to test out and keep. They are only giving a limited supply, so I’m showing you this, they are still giving them away from the new year overstock I absolutely LOVE the ipad. Click Here!!! JANIKPOWERED32.TK let me know when you have yours too.

In the sample above, the language used is deceptive “I actually got a free ipad to test and keep”. They are only giving a limited supply” as if it is a demand placed by individuals in which the company is responding to such demands. “I am showing you this” meanwhile the above message is without evidence to proof the scammer right. “Let me know if you have yours too” the too is not required in the sentence.

Sample 5: facebook video

Hey Nina, look at you in this video… What are you doing? LOL! You have to love this …apps.facebook.com

The style of language used by the scammer is a deceptive form of language meant to entice the victim to log into the account. “Hey Nina, look at you in this video… What are you doing? Lol! You have to love this…the language used here is shocking, horrific and hilarious that would urge the recipient to eagerly click the link in order to get to see the video.

Sample 6: Facebook App or News

Ha ha check this out…she is soo busted. CLICK HERE to see the status update that got a girl expelled from school!!! You got to see this, she is in such trouble.

In the scam above the whole sentence is deceptive, the style of writing is not fluent ‘she is soo busted’ the soo is misspelt and not necessary for the sentence. ‘CLICK HERE to see the status updated that got a girl expelled from school’ the sentence does not correlate, ‘she is in such trouble’ they are all grammatical errors.

Sample 7: Facebook Amazing Weight Loss Offers

Heyy, for the past few weeks I have been trying this new weight loss product I saw on Oprah and CNN. You should check this out too I have lost some weight already on it, and I hear many others have too. Facebook Sponsored Weight

Loss Product app.facebook.com Living proof that it works.

The scam did not mention the name of the product; a product cannot be advertised without mentioning the name of the product. The scammer mentioned that he/she saw the product on Oprah and CNN and the weight loss product is sponsored by facebook; no unknown product can be sponsored by any organization or media. 'Having proof that it works' meanwhile there is no proof because no picture was shown to proof that the product is authentic and it works.

Sample 8: Facebook Phishing Schemes

You haven't been back to Facebook recently, you have received notifications while you were gone. Thanks, The Facebook Team. To login to Facebook, follow the link below: http://www.facebook.com/gentleny62%40yahoo.com

In the sample above, there are some grammatical errors that made the message obviously a scam. 'You haven't been back to facebook recently', which is actually supposed to be 'You have not logged into your facebook account recently'. 'following the link bellow' the bellow is misspelt instead of below. No Facebook Team would send anyone a message informing the facebook user he/she have not logged into his/her account and giving the individual the link with which to open the facebook account.

Sample 9: Facebook Fake Friend Request

Kaamil Mahmoud wants to be friends with you on facebook. Confirm Friend Request.

The scam says 'Kaamil Mahmud wants to be friends with you on facebook' a single person cannot be friends but friend with you, by seeing this grammatical error, it is known the message is a scam.

Sample 10: Facebook Job Scam

R.I.P Steve Jobs. In memory of Steve a company is giving 10 people employment this week. Click to apply.http:/bit.ly/restinpeace-steve-jobs.

In the sample above, the name of the company was not mentioned, the job specification was not given and also the qualification of the applicant was not stated. The above link is non-existent. The language used is not fluent and convincing.

4.2.3 Analysis of Cases of Email Scam

Sample 1: Email Scam

From: John Owens jmo69@yahoo.com Date: October 18, 2011 12:33:06 PM EDT To: undisclosed recipients: subject: Sad News……John Owens. Reply-To:

Jmo69@yahoo.com Hi, I'm writing this tears in my eyes. My family and I came down here to London, England for a short vacation and we were mugged at gun point last night at the park of the hotel where we lodged all cash, credit cards and cell phone were stolen off us. I've been to the US embassy and the Police here but they're not helping issues at all, My flight leaves in few hrs from now and am having problems settling the hotel bills. The hotel manager won't let me leave until I settle the hotel bills now. Well I really need your financial assistance…Please, let me know if you can help us out? Am freaked out the moment. John Owens…

In the sample above, the writer of the scam is suppose to be a native speaker who speaks standard English, but in the mail there are some features of Nigeria English in it. 'with tears in my eyes', 'stolen off us', 'not helping issues at all', 'am', 'well', 'my family and I', all this are element of Nigerian English not a native speaker. The scammer made mention of not having money to settle the hotel bills meanwhile hotel bills are paid before checking into an hotel. The message did not disclose to the recipient where he came from for the vacation in London, England. All this linguistic features constitute together to make the mail a scam.

Sample 2: Disease Scam

From: “Paul George” charles@g-photonics.com Date: January 1, 2000 5:28:53 PM EST subject: Greeting, Please acknowladge the receipt of this mail. Reply-To: paulgeorge01@yahoo.cn Hello, I am Paul George, I am ill and would die having been diagnosed with cancer disease. I want to distribute my funds to charities in your country through you. Please respond for more details respectfully, Paul George.

In this sample, there are grammatical errors and the whole sentence does not correlate to the sender’s problem. There is a spelling mistake ‘acknowladge’ which is not correct. The sender did not mention his country and also the home country of the receiver which he want him to distribute his fund. An individual from another country cannot email just an individual in another country to distribute his fund who he does not know. If the sender has any fund to distribute, he would channel it through his lawyer to the organization of his choice.

Sample 3: Custom Scam

From “Mr Jason Ahern” customofficeus@yahoo.com.hk Date: April 7, 2009 9:16:15 AM EDT Subject: Your Package/Funds at KJFK Airport. Reply-To: uscustoms5036@yahoo.co.jp We hereby bring to your notice that a consignment been delivered at your residence by two diplomats. They had been

stopped by us. There is a security measure put in place by United States of America, check terrorism and money laundry through the sale of illegal drugs locally and internationally. After examination, we found out that the consignment contained the sum of US $5.7 Million, which upon further investigation revealed that the fund was your inheritance. Consequently, the diplomats will deliver your consignment at your residence after all protocols have been observed. However, in order to proceed we need you to reconfirm the following information, Full Name:…Residential Address:… Date of Birth:… Occupation:… Telephone/Mobile Numbers:… We await your response. Regards, Jason Ahern.

When such mail is sent from a corporate body to an individual the name of the organization where the mail is sent from is suppose to be mentioned. The position held by Mr Jason Ahern in the organization and the address of the office the mail was sent from was not mentioned. The mail has a feature of Nigeria English in it, 'after protocols have been observed', also 'protocols' does not have pluralization.

Sample 4: Courier Scam

From: "UPS COURIER COMPANY" info@ups.net Date: April 21, 2009 9:14:38 AM EDT Subject: UPS PARCEL Reply-To: clairefisher_bl@live.com I am sorry to encroach into your privacy through this manner; we have a Certified

Cheque of $300,000 in your custody that belongs to you. This cheque was brought to my desk last week by a lady name Mrs Christiana Wood who gave us your e-mail address to contact you on the delivery. You are advice to send us the following: Name: Address: Contact phone number: We wait your response soonest. UPS COURIER COMPANY Email: clairefisher_bl@live.com Waiting anxiously for a swift response. Prof Charles Brown. Despatch Director. Tel, + 234-7089147754

In the sample, there is a problem of tense usage; the scammer used present tense 'a lady name Mrs Christiana Wood', the 'name' is supposed to be in past tense 'a lady named Mrs Christiana Wood'. There is also a substitution of preposition of 'of' to 'on '. The eagerness for the reply of the message was emphasized 'waiting anxiously for a shift response'. The courier company should not be anxious on waiting for a response of a client or even a courier company usually delivers their client's parcel in the designated address.

Sample 5: Asking For Assistance Scam

Hello My Friend,

This is a message from Hong Kong, my name is MrChing Wong. Credit Officer in a finance firm, I am contacting you because I need your assistance in moving the sum of Twenty Million Dollars from my country to yours. But I need you to

stand as the beneficiary of the funds in the means of this process. This business has steps and you will have 40% of the above sum at the end of the transaction. If you interested please reach me back via my private e-mail address chingwong20@hotmail.com I will introduce you to the next step. I want to hear from you soon. Thanks.

MrChing Wong.

The language used in this sample is obviously deceptive. One cannot go into business with such huge sum of money with an unknown individual. In the heading, the writer sounded as if he knows the person he is sending the mail to but in the beginning of the mail he introduced himself by stating where he is writing from and his name. In business, the type of transactions to be made is suppose to be discussed before the percentage of the interest to be shared.

Sample 6: Investment scam

NEWS WAS RELEASED AFTER THE MARKET CLOSE FRIDAY! WATCH SBRX LIKE A HAWK MONDAY!! THE ALERT IS ON!!!

TRADING ALERT!

Date: Monday, May 1, 2006

Stonebridge Resources Exploration, Ltd.

Acquisition and Development of Oil and Gas Assets

Symbol SBRX

Price: $1.13

IS THERE A HOTTER SECTOR TO TRADE?! IS SBRX ON THE VERGE OF A "MONSTER MOVE?" LOOK AT FRIDAY'S ACTION IN THE SHOCK? DO IT BREAK OUT?

THE NEWS: Go to Your Favourite Financial Website and Read The Full Story Right Now!!

In the sample, there is omission of preposition of 'on' in the heading of the mail 'WATCH SBRX LIKE A HAWK (ON) MONDAY'. A legitimate investment planner with legitimate stock advice does not use such choice of style in advertising their stock. They would rather deal with their own existing clients, not recruiting via random email.

Sample 7: Internet Phishing Scam

Dear Wamu Customer,

We regret to inform you that we had to lock your Wamu account access because we have reasons to believe that it may have been compromised by outside parties. In order to protect your sensitive information, we temporarily suspended

your account access.

CLICK HERE to verify and reactivate your account access by completing the secure form that will appear.

This is a security measure that will ensure that you are the only person with access to the account. Thank you for your time and consideration in this matter.

The salutation of the mail should have been the name of the recipient because the name of the customer should have been known by the bank and used when sending a mail to a customer's personal email address. Not using "Dear Wamu Customer". "By outside parties" is not also grammatical, instead of "By a third party". No legitimate online financial service will ask you to login this way.

Sample 8: Webmail Scam

From: avoth@cogeco.ca[mailo:avoth@cogeco.ca] On Behalf of Webmail.

Uchicago.edu@cogeco.ca

Sent: Thursday, July 24, 2008 6:46 PM

Subject: Quoting Uchicago.edu, Member. Service@ Uchicago.edu

Dear Uchicago.edu, email account user, We are currently verifying our subscribers email accounts in order to increase the efficiency of our webmail

futures. During this course you are required to provide the verification desk with the following details so that your account could be verified;

CNetID:……

Password:…….

Territory:……..

Kindly send these details so as to avoid the cancellation of your email account.

Thanks, Uchicago.edu, Team.

The style used in this mail shows that is a scam because no such mails come from such email address and ask for such information to verify an email account. The address from which this email was sent is obviously not a university email address.

Sample 9: Tax Refund Scam

From: Internal Revenue Service

[mailto:yourtaxrefund@InternalRevenueService.com]

Sent: Tuesday, July 22, 2008 9:47 AM

Subject: [SPAM.#] Get your tax refund now

Importance: Highly

After the last annual calculations of your account activity we have determined that you are eligible to receive a tax refund of $479.30.

Please submit the tax refund request and allow us 2-6 days in order to process it.

A refund can be delayed for variety of reasons.

For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please click here (http://edlogs.rta.mi.th:84/www.irs.gov/)

Note: Deliberate wrong inputs will be prosecuted by law.

Regards,

Internal Revenue Service.

In this sample, there is no such tax refund activities put in place to refund any tax collected by the tax fund Internal Revenue Service. The mail should carry the name of the recipient and also all the details the individual have used to pay the tax previously in order to make the mail authentic, but all this were absent in this spam mail. From the address of the mail it shows the address is not a government email address, and the link does not lead to the real IRS website.

Sample 10: Impersonation Scam

From: Senator David Mark

[mailto:info@atm.com]

Sent: Tuesday, April 14, 2009 9:49 PM

Subject: OUR REF:FRN/ATM/882

YOUR REF: CLAIM/ATM/882

This is to officially inform you that (ATM Card Number; (5179123456789120) has been accredited in your favour. Your Personal Identification Number is 882. The ATM Card Value is $6.8 MILLION USD. You are advice to contact Mr Jeffery Simpson via Email (firstflightservice@yahoo.com.hk) with the following information's;

Full Name:

Delivery Address:

Phone Number:

Country:

Occupation:

Sex:

Age:

Please Note that you are to pay the sum of $85 USD for the delivery of your ATM Card by FedEx Courier Express.

Best Regards,

Senator David Mark.

In the mail above, the language is more of a deceptive tone and not convincing at all, a mail with such content cannot be sent to an individual email address by just a single individual you do not know to give away credited ATM Card.

4.2.4 Analysis of cases of Text Messages

Sample 1: Bank Scam

I'm texting from the customer experience centre for Bank of America. Our records indicate that you had an interaction with the Card Service Department at Bank of America on September 3rd. please call 1-800-490-5065 and answer a few questions regarding the interaction. Thank you.

In this sample, there are some wrong arrangements of sentences. In regards to the senders' location, he/she is meant to be a native speaker of English but the content of the SMS is not that of a native speaker. ' I'm texting from the customer experience centre for bank of America', such SMS from a corporate company and

a native speaker is not suppose to start with ‘I’m texting’ and also ‘customer experience centre’. There is also a wrong arrangement of the date ‘on September 3rd’ instead of ‘on the 3rd of september’.

Sample 2: Card Block Scam

F.C.U (Card Blocked) Alert. For more information please call 1-866-972-7278. Thank you.

The sample above is vague, the style of writing is apparently a scam. An acronym was used which might not fully be understood by the recipient, and the next statement that follows it is “(Card Blocked) Alert”, no explanation was made on the message to give a better understanding of the content.

Sample 3: Puppy Scam

Hello, my name Stephen. I will like to know if the puppy is still for sale, if yes, how much and whats the sex?

The SMS sounds like the recipient had advertise the sales of a dog, and if such advert was made, the sex and the price of the puppy would have been mentioned in the detail.

Sample 4: Phishing Scam

Dear Costums,

Your Apple ID has been used to a open a session Icloud from an unauthorized phone.

It is imperative to conduct an audit of your information is present, otherwise your ID will be destroyed.

Just click the link below and log in with your Itunes ID and password. Check Now.

The salutation “Dear Custums’ is spelt wrongly. No authorize phone company would send such message to their customers they would not ask to click on any link before checking if it’s true or false.

Sample 5: Request Scam

How are you doing today? I will need you to take care of a bank wire transfer for me today. Let me know the required information needed for you to process the Wire transfer. I will appreciate swift response.

Thanks

The content of the SMS is ambiguous and imprecise, it did not specify if the money to be transferred will be sent to the bank account of the recipient or if the transfer will be carried out through the sender’s bank account, and if it is through

the sender's bank account, the recipient need not to send any information. Before such message would be attended to, both individuals have to be familiar with each other. The style of the text used is suspicious.

Sample 6: Share-A-Load Scams

Your postpaid account number has been charged P500 for LTE use. Is this a wrong charge? Text 500 sent to 292667674329 for REFUND.

In the above sample, "Your post-paid account number", the 'number' should not be present in the statement. If the message is coming from the network subscriber, they should know if the charge was wrong not asking the network user after deducting the account.

Sample 7:Report Scam

For all Globe postpaid users in if you did scam. How to report? And how to block the sim. Just text 300 and send to 29361323065 when send is finished. Show Help from the next received message

In the sample above, there are grammatical errors which cannot come from an authorized labelled agent, the grammar used in the above sample is not well structured which hinder the intended meaning of the sender.

Sample 8: Winning Alleged Raffle Prizes

Congratulations! You have just won the sum of Five Hundred Thousand Naira (500,000), in the raffle draw held today in Lagos. To claim this prize load a #1500 credit on your phone.

The sample above, the individual will first of all consider if he/she had played any game that demands a raffle draw. “To claim this prize load a #500 credit on your phone”, the reason for loading the credit on your phone was not told and no legitimate free prize would demand anything from the winner to claim the prize.

Sample 9: Cloning Scam

Dear subscriber, to update your phone send your unique serial number to this number 27490874371.

In the scam above, no network operator would ask you to send your serial number to update your phone rather they only ask you to update your phone if it needs an update.

Sample 10: Vote with Your Phone Scam

You can actually cast your phone for the candidate of your choice by pressing the “YES” button on your phone. Voting is FREE.

The content of this SMS in the above sample does not sound convincing enough, it is not possible to cast a vote on your mobile phone, one would actually imagine if

after pressing the YES button, the names of the candidates contesting for the election would be shown and then you cast your vote accordingly.

4.3 Summary of the Findings

4.3.1 The data reveals that scam email can be in form of Facebook, email and text messages. Email scam is an unsolicited email that claims the prospect of a bargain or something for nothing. Some scam messages ask for business, others invite victims to a website with a detailed pitch. Many individuals have lost their life savings due to this type of fraud. Email scam is a form of email fraud. The linguistics analysis of scam e-mails is important.

4.3.2 The findings from the respondents reveal that there is genuine motive behind the linguistic analysis of scam e-mail.

4.3.3 The relationship between linguistic analysis and scam e-mails is very favourable.

4.3.4 Linguistic analysis of scam e-mails proves that scam e-mail in Nigeria is very high.

4.4 CONCLUSION

Many Nigeria scams emails are very similar except for the names used in the message and various details such as place, names, dates, amounts and contact

details. However, citizens still fall victims to these scams because they do not know the linguistic features of these mails. They are carried away by pity for the message or by the huge sums of money promised them.

This study is to educate individuals and the society at large on how to identify these scams linguistically which seems to be best solution to scam mails for now. From the data's shown in chapter four (4), they are real example of scams. The sum of money they mention does not exist. Recipients who initiate a dialogue with the scammers by replying to these messages will eventually be asked for advance fees supposedly required to allow the deal to proceed.

Bibliography

Adkins, M. & Brashers, D.E. (2005). The Power of Language in Computer-Mediated Groups. *Management Communication Quarter*,8(3), 289-322.

Balswick, J. & Avertt, C. (2006). Differences in Expressiveness: Gender,Interpersonal Orientation, and Parental Expressiveness as Contributing Factors. *Journal of Marriage and the Family,* 38,121-127.

Baron, N.S. (2005). Letters by Phone or Speech by other Means: The Linguistics of email. *Language and Communication,* 18 (2), 133-170.

Baym, N. (2005). The Emergence of Community in Computer-mediated Communication. In S. Jones (Ed.), *Cybersociety: Computer-mediated Communication and Community* (pp. 138-163). Thousand Oaks, CA: Sage.

Campbell, K. (2002). Power, Voice and Democratization: Feminist Pedagogy and Assessment in CMC. *Educational Technology and Society*,5(3), 27-39.

Carr, A.(2010). Open Thread: The end of email? Retrived September 28, 2010, From http://www.fastcompany.com/1661288/the-end-of-email.

Chafe, W. L. (2005). Linguistic Differences Produced by Differences Between Speaking and Writing. In D. Olsen, N. Torrance & A. Hildyard (Eds.),*Literacy, Language and Learning: The Nature and Consequences of Reading and Writing* (pp.105-123). New York: Cambridge University Press.

Chafe, W., & Danielewicz, J. (2007). Properties of Spoken and Written Language. In R. Horowitz & S. J. Samuels (Eds.), *Comprehending Oral and Written Language* (pp. 83-116). San Diego: Academic Press.

Cherny, L. (2005), *Conversation and Community: Chat in a virtual world*.Stanford, CA: CSLI Publications.

Cho, T.(2006). *The Use of Computer-generated Concordances in Languages: How Technology Redefines Research.* Unpublished Manuscript.

Condon, S. L. & Cech, C. G.(2005). Functional Comparison of Face-to-Face and Computer-mediated Decision making Interactions. In S. Herring (Ed.) *Computer-mediated communication: Linguistic,social and cros- Cultural perspectives* (pp.65-80). Amsterdam: John Benjamins.

Condon, S. L., & Cech, C. G. (2006). Discourse Management Strategies in Face-to-Face and Computer-mediated Decision making Interactions. *Special Issue of the Electronic Journal of Communication* [On-lineserial],6 Available from comserve@rpitsvm.bitnet.

Coulmas, F. (2002). *Language and Economy.* Oxford: Blackwell.

Coupland, J., Coupland, N., & Robinson, J. (2002). "How are you?": Negotiating Phatic Communion. *Language in Society, 21,* 207-230.

Crystal, D. (2001). *Language and the Internet.* Cambridge: Cambridge University Press.

Cumming, J. D. (1995). The Internet and the English Language. *English Today*,11(1), 3-8.

NUA. (2000). *Email: The IdealMarketing Tool.* Dec 19. Retrieved June 7, 2004, from

http://www.nua.com/surveys/index.cgi?f=VS&art_id=905356261&rel=true.Pew Internet & American Life Project (2005).*Trends 2005. The Internet:The Mainstreaming of Online Life.*Retrieved June 7, 2004, from http://www.pewinternet.org/PPF/r/148/report_display.asp

Spam Filter Review (2004).*Spam Statistics 2004.* Retrieved June 7 2004, fromhttp://spam-filter-review.toptenreviews.com/spam-statistics.html

Wandvogel, J.(2001). Email and Workplace Communication: A Literature Review. *Language in the Workplace Occasional Papers,* 3.Retrieved June 7, 2004,From http://www.vuw.ac.nz/lals/research/lwp/docs/ops/op3.htm

Yahoo! (2010). *The Yahoo! Style Guide: The Ultimate Source Book for Writing, Editing,and Creating Content for the Digital World.* New York: St Martins'

http://en.wikipedia.org/wiki/ List_of_Email_Scams#Cite_note-3

http://www.onguardonline.gov/articles/0003-Phishing